NICOLA LUGARESI

INTERNET E DIRITTO:
CASI E MATERIALI

SOMMARIO

INTRODUZIONE: IL DIRITTO PUBBLICO DI INTERNET

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 online, 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 autonoma 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 branche 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 della 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 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

EASTERBROOK, F., *Cyberspace and the Law of the Horse*, 1996 *U. Chi. Legal F.* 207

HUNTER, D., *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91, Cal. L. Rev. 439 (2003)

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

LESSIG, L., *The Law of the Horse: What Cyberlaw Might Teach*, 113 *Harv. L. Rev.* 501 (1999)

LEMLEY, M., *Place and Cyberspace*, 91 *Cal. L. Rev*. 521 (2003)

REIDENBERG, J., *Lex Informatica: The Formulation of Information Policy Rules through Technology* 76 Texas L. Rev. 553 (1998)

1. INTERNET, DIRITTO, GIURISDIZIONE

1.1. Tecnologia e diritto

Corte Suprema degli Stati Uniti, 11 giugno 2001, no.99-8508 (*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* […]. 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.

1.2. *Cyberspace*, ed altri luoghi

Corte di Appello degli Stati Uniti, Eleventh Circuit, 21 settembre 2001, no. 00-16346

[…]

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. Section 27-523 defines adult entertainment 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 distinguished by their display or depiction of specified anatomical areas or specified anatomical activities, as defined in this section."

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.

2. Whether the District Court properly relied on the negative secondary effects doctrine in determining the constitutionality of Tampa's zoning restrictions as applied to 2312 West Farwell Drive.

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.

III. Standard of review

This Court reviews the District Court's grant of a motion for summary judgment *de novo*, applying the same legal standards used by the District Court. *Sammy's of Mobile, Ltd. v. City of Mobile* […] (11th Cir., 1998).

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 City 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*, No. 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

[…]

1.3. *Cyberspace*, luoghi e comunicazioni

Corte di Cassazione, sez.II penale, 18 ottobre 2010, n.37151

[…]

In fatto

Il G.I.P. del Tribunale di ..., con ordinanza in data 10 maggio 2010, rigettava la richiesta del P.M. di sostituzione, nei confronti di ... e ..., della misura degli arresti domiciliari con la custodia in carcere per avere gli stessi violato la prescrizione loro imposta di non comunicare con persone diverse dai familiari conviventi, comunicando via Internet, sul sito "*Facebook*", con altre persone.

Proponeva ricorso per Cassazione il Procuratore della Repubblica presso il Tribunale di ... ritenendo integrata la violazione della prescrizione di non comunicare con altre persone, imposte in sede di concessione della misura cautelare, stante i contatti intrattenuti con altre persone dagli imputati attraverso la rete.

Motivi della decisione

Il ricorso è fondato.

La generica prescrizione di "non comunicare con persone diverse dai familiari conviventi" prevista dall'art.276, comma 1, c.p.p., va intesa nell'accezione di divieto non solo di parlare con persone non della famiglia e non conviventi, ma anche di entrare in contatto con altri soggetti, dovendosi ritenere estesa, pur in assenza di prescrizioni dettagliate e specifiche, anche alle comunicazioni, sia vocali che scritte attraverso Internet. L'uso di Internet non può essere vietato *tout court* ove non si risolva in una comunicazione con terzi, comunque, attuata, ma abbia solamente funzione conoscitiva o di ricerca, senza di entrare in contatto, tramite il *web*, con altre persone.

La moderna tecnologia consente oggi un agevole scambio di informazioni anche con mezzi diversi dalla parola, tramite *web*, e anche tale trasmissione di informazioni deve ritenersi ricompresa nel concetto di "comunicazione", pur se non espressamente vietata dal giudice, dovendo ritenersi previsto nel generico "divieto di comunicare", il divieto non solo di parlare direttamente, ma anche di comunicare, attraverso altri strumenti, compresi quelli informatici, sia in forma verbale che scritta o con qualsiasi altra modalità che ponga in contatto l'indagato con terzi ("pizzini", gesti, comunicazioni televisive anche mediate, etc.).

L'eventuale violazione di tale divieto va, comunque, provato dall'accusa e non può ritenersi presunto, nella fattispecie, dall'uso dello strumento informatico.

Non risulta, nella specie, alcuna motivazione da parte del G.I.P., in ordine all'eventuale comunicazione con terzi, posta in essere dall'indagato attraverso *Facebook*.

Va, quindi, annullato il provvedimento impugnato con rinvio […].

[…]

1.4. Giurisdizione e valori

Tribunal de Grande Instance di Parigi, ord. 22 maggio 2000

(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 *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 sul suo servizio *Geocities.com* due monumenti della letteratura contemporanea antisemita, il *Mein Kampf* di Adolf Hitler e i Protocolli dei Savi 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 cui 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 correlativamente 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 evochino 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 Savi 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, dai 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 "olocausto" 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 intenzionale 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 riveli 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 colleghi 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 offre all'utente 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 comprendente 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 *links* successivi, sia attraverso parole chiave lo porti verso a siti, pagine o *forum*, il cui titolo e/o i cui 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 *links* 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.

[…]

1.5. Giurisdizione e reati commessi in Rete

Corte di Cassazione, sez.V penale, 27 dicembre 2000, n.4741

[…]

D.M., con atto di querela datato 1 marzo 2000, esponeva al P.M. di Genova che su alcuni "siti" Internet erano stati pubblicati scritti ed immagini, lesivi della sua reputazione e della privacy sua e delle figlie minorenni, D. e Da.. Riferiva il D. che le due minori, nate dal suo matrimonio con T. P., erano state affidate ad entrambi i genitori al momento della separazione legale degli stessi. Successivamente, la madre aveva arbitrariamente portato con sé le due bambine in Israele, dove ella si era risposata con un rabbino, aderendo ad una "versione" particolarmente rigorosa ed "ultraortodossa" della religione ebraica. D. e Da., rintracciate dalle autorità israeliane, erano state affidate al solo padre (il D., appunto) che le aveva condotte con sé in Italia. A partire da tale momento, su alcuni "siti" Internet, erano stati immessi scritti ed immagini, che riferivano ed illustravano la vicenda appena esposta, formulando giudizi estremamente negativi e diffamatori sulla personalità e sul comportamento del D. (oltre che sull'operato dell'autorità giudiziaria italiana), nonché messaggi contenenti l'invito, rivolto agli aderenti alla religione ebraica, a "liberare" le due minori, "tenute prigioniere" dal padre, che impediva loro di professare i culti relativi alla predetta fede religiosa.

[…]

La Corte ritiene in diritto

Allo scopo di decidere correttamente una questione, quale quella prospettata, che presenta, senza dubbio, alcuni caratteri di novità, appare innanzitutto opportuno verificare come si caratterizzi il delitto di diffamazione consumato con quel nuovo mezzo di trasmissione-comunicazione che prende il nome di Internet.

Il legislatore, pur mostrando di aver preso in considerazione l'esistenza di nuovi strumenti di comunicazione, telematici ed informatici (si veda, ad esempio, l'art.623-*bis* c.p. in tema di reati contro l'inviolabilità dei segreti), non ha ritenuto di dover mutare o integrare la lettera della legge con riferimento a reati (e, tra questi, certamente quelli contro l'onore), la cui condotta consiste nella (o presuppone la) comunicazione dell'agente con terze persone. E, tuttavia, che i reati previsti dagli artt.594 e 595 c.p. possano essere commessi anche per via telematica o informatica, è addirittura intuitivo; basterebbe pensare alla cosiddetta trasmissione via *email*, per rendersi conto che è certamente possibile che un agente, inviando a più persone messaggi atti ad offendere un soggetto, realizzi la condotta tipica del delitto di ingiuria (se il destinatario è lo stesso soggetto offeso) o di diffamazione (se i destinatari sono persone diverse).

Se invece della comunicazione diretta, l'agente "immette" il messaggio "in rete", l'azione è, ovviamente, altrettanto idonea a ledere il bene giuridico dell'onore. Per quanto specificamente riguarda il reato di diffamazione, è infatti noto che esso si consuma anche se la comunicazione con più persone e/o la percezione da parte di costoro del messaggio non siano contemporanee (alla trasmissione) e contestuali (tra di loro), ben potendo i destinatari trovarsi persino a grande distanza gli uni dagli altri, ovvero dall'agente. Ma mentre nel caso di diffamazione commessa, ad esempio, a mezzo posta, telegramma o, appunto, *email*, è necessario che l'agente compili e spedisca una serie di messaggi a più destinatari, nel caso in cui egli crei o utilizzi uno spazio *web*, la comunicazione deve intendersi effettuata potenzialmente *erga omnes* (sia pure nel ristretto - ma non troppo - ambito di tutti coloro che abbiano gli strumenti, la capacità tecnica e, nel caso di siti a pagamento, la legittimazione, a "connettersi"). Partendo da tale - ovvia - premessa, si giunge agevolmente alla conclusione che, anzi, l'utilizzo di Internet integra una delle ipotesi aggravate di cui dell'art.595 c.p. (comma 3: "offesa recata ... con qualsiasi altro mezzo di pubblicità"). Anche in questo caso, infatti, con tutta evidenza, la particolare diffusività del mezzo usato per propagare il messaggio denigratorio rende l'agente meritevole di un più severo trattamento penale. Né l'eventualità che tra i fruitori del messaggio vi sia anche la persona nei cui confronti vengono formulate le espressioni offensive può indurre a ritenere che, in realtà, venga, in tale maniera, integrato il delitto di ingiuria (magari aggravata ai sensi del comma 4 dell'art.594 c.p.), piuttosto che quello di diffamazione. Infatti il mezzo di trasmissione-comunicazione adoperato (appunto Internet), certamente consente, in astratto, (anche) al soggetto vilipeso di percepire direttamente

l'offesa, ma il messaggio è diretto ad una cerchia talmente vasta di fruitori, che l'addebito lesivo si colloca in una dimensione ben più ampia di quella interpersonale tra offensore ed offeso. D'altronde, anche per altri media si verifica la medesima situazione. Un'offesa propagata dai giornali o dalla radio-televisione è sicuramente percepibile anche dal diretto interessato, ma la fattispecie criminosa che, in tal modo, si realizza è, pacificamente, quella *ex* art.595 c.p. e non quella *ex* art.594.

Peraltro, la diffusività e la pervasività di Internet sono solo lontanamente paragonabili a quelle della stampa ovvero delle trasmissioni radio-televisive. Internet è, senza alcun dubbio, un mezzo di comunicazione più "democratico" (chiunque, con costi relativamente contenuti e con un apparato tecnologico modesto, può creare un proprio "sito", ovvero utilizzarne uno altrui). Le informazioni e le immagini immesse "in Rete", relative a qualsiasi persona sono fruibili (potenzialmente) in qualsiasi parte del mondo. Ma proprio questo è il nodo che qui interessa sciogliere, dal momento che, in considerazione della caratterizzazione "transnazionale" dello strumento adoperato, può apparire, in un primo momento, problematica l'individuazione del luogo in cui deve ritenersi consumato il delitto commesso "a mezzo Internet". In realtà, un'espressione ingiuriosa, un'immagine denigratoria, una valutazione poco lusinghiera inserite in un "sito" *web* sono soggette ad una diffusione al di fuori di ogni controllo e di ogni ragionevole possibilità di "blocco", se non attraverso i mezzi coercitivi legalmente riservati alla pubblica autorità (e sempre che siano disponibili adeguati strumenti tecnici). Ma, va da sé, le procedure, appunto legali o tecniche, hanno bisogno di tempi lunghi, mentre il messaggio veicolato dal computer si propaga fulmineamente.

[…]

La diffamazione, contrariamente a quello che il Riesame e lo stesso P.M. ricorrente affermano, è un reato di evento, inteso quest'ultimo come avvenimento esterno all'agente e causalmente collegato al comportamento di costui. Si tratta di evento non fisico, ma, per così dire, psicologico, consistente nella percezione da parte del terzo (*rectius* dei terzi) dell'espressione offensiva. Pertanto è sicuramente in errore il ricorrente quando, a proposito, appunto, della percezione, scrive che essa è elemento costitutivo della condotta; in realtà la percezione è atto non certamente ascrivibile all'agente, ma a soggetto diverso, anche se - senza dubbio - essa è conseguenza dell'operato dell'agente.

Il reato, dunque, si consuma non al momento della diffusione del messaggio offensivo, ma al momento della percezione dello stesso da parte di soggetti che siano "terzi" rispetto all'agente ed alla persona offesa. Sul punto, ha avuto modo di pronunziarsi, sia pure implicitamente, la giurisprudenza di questa Corte […].

Per di più, nel caso in cui l'offesa venga arrecata tramite Internet, l'evento appare temporalmente, oltre che concettualmente, ben differenziato dalla condotta. Ed invero, in un primo momento, si avrà l'inserimento "in Rete", da parte dell'agente, degli scritti offensivi e/o delle immagini denigratorie, e, solo in un secondo momento (a distanza di secondi, minuti, ore, giorni ecc.), i terzi, connettendosi con il "sito" e percependo il messaggio, consentiranno la verificazione dell'evento. Tanto ciò è vero, che, nel caso in esame sono ben immaginabili sia il tentativo (l'evento non si verifica perché, in ipotesi, per una qualsiasi ragione, nessuno "visita" quel "sito"), sia il reato impossibile (l'azione è inidonea, perché, ad esempio, l'agente fa uso di uno strumento difettoso, che solo apparentemente gli consente l'accesso ad uno spazio *web*, mentre in realtà il suo messaggio non è mai stato immesso "in Rete").

Orbene, l'art.6 c.p., al comma 2, stabilisce che il reato si considera commesso nel territorio dello Stato, quando su di esso si sia verificata, in tutto, ma anche in parte, l'azione o l'omissione, ovvero l'evento che ne sia conseguenza. La cosiddetta teoria dell'ubiquità, dunque, consente al giudice italiano di conoscere del fatto-reato, tanto nel caso in cui sul territorio nazionale si sia verificata la condotta, quanto in quello in cui su di esso si sia verificato l'evento. Pertanto, nel caso di un *iter criminis* iniziato all'estero e conclusosi (con l'evento) nel nostro Paese, sussiste la potestà punitiva dello Stato italiano.

[…]

P.Q.M.

La Corte annulla l'impugnata ordinanza con rinvio al Tribunale di Genova per nuovo esame.

[…]

2. LE REGOLE DI INTERNET

2.1. L'anarchia della Rete

J.P. Barlow - A Declaration of the Independence of Cyberspace

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 blanketed 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

2.2. Analogia: telefonate ed *email*

Corte di Cassazione, sez.I penale, 30 giugno 2010, n.24510

[…]

1. - Con sentenza, deliberata l'11 maggio 2009 e depositata il 3 luglio 2009, il Tribunale di Cassino, in composizione monocratica - per quanto qui rileva - ha condannato alla pena dell'ammenda in euro duecento, nel concorso di circostanze attenuanti generiche, D.M., imputato della contravvenzione di molestia alla persone per aver inviato, colla posta elettronica, a G.O. un messaggio contenente "apprezzamenti gravemente lesivi della dignità e dell'integrità personale e professionale" del convivente della destinataria, reato commesso in Cassino il 24 febbraio 2005 (capo sub B della originaria rubrica), motivando, in relazione al punto controverso dell'accertamento della colpevolezza: il messaggio è stato inviato dalla casella di posta elettronica "barma71", attivata […] il 17 gennaio 2004, alle ore 12.24 (con spendita delle generalità di persona inesistente), mediante collegamento effettuato tramite l'utenza telefonica intestata all'imputato; inoltre nella memoria di un computer in uso al medesimo giudicabile risultano registrati accessi alla suddetta casella; deve considerarsi fallita la prova d'alibi di D.M. (costui ha sostenuto che al momento dell'attivazione della casella non era a casa, ma si trovava in compagnia di amici a una festa di compleanno); i riferimenti del testimoniale a discarico devono essere valutati con margini di approssimazione, avuto riguardo all'incertezza palesata da uno dei testimoni in ordine ad altra circostanza dell'incontro e al generico e dubitativo riferimento cronologico offerto dall'altro teste; costituisce, poi, mera congettura e illazione l'assunto difensivo che persona ignota possa aver attivato la casella di posta elettronica attraverso l'utenza telefonica residenziale, installata nell'abitazione dell'imputato; laddove, poi, il computer in uso a D.M. ha memorizzato l'accesso alla casella, che presuppone la conoscenza dell'indirizzo di posta elettronica e della parola d'ordine (note a chi attiva la casella stessa).

2. - Ricorre per Cassazione l'imputato […].

2.1 - Con il primo motivo il ricorrente oppone: al momento dell'attivazione della casella di posta elettronica barma7l esso D.M. era fuori casa, come dimostrato dal testimoniale a discarico; non è possibile attribuire l'invio del messaggio molesto in difetto della dimostrazione della registrazione del casella, dell'uso esclusivo della utenza telefonica e della disponibilità del "*personal computer* - per dir così - di partenza" al momento della spedizione del messaggio.

2.2 - Con il secondo motivo il ricorrente deduce: difetta il dolo specifico; il Tribunale ha riconosciuto che al momento dell'attivazione della casella non era stata concepita la condotta molesta; è illogico e incomprensibile supporre che i messaggi siano stati inviati dopo alcuni mesi; non è dimostrato che l'imputato fosse animato da astio nei confronti della persona molestata o del convivente di lei.

[…]

La *quaestio juris* è se l'interpretazione estensiva della previsione della norma incriminatrice, circa la molestia o il disturbo recati "col mezzo del telefono", possa essere dilatata sino a comprendere l'invio di corrispondenza elettronica sgradita, che provochi turbamento o, quanto meno, fastidio.

Innanzi tutto non coglie nel segno l'argomento del giudice di merito secondo il quale la "*email* … viene propriamente inoltrata col mezzo del telefono", così integrando la previsione della norma incriminatrice.

Il rilievo è improprio e inesatto. La posta elettronica utilizza la rete telefonica e la rete cellulare delle bande di frequenza, ma non il telefono, né costituisce applicazione della telefonia che consiste, invece, nella teletrasmissione, in modalità sincrona, di voci o di suoni.

Né, poi, giova il richiamo al precedente di questa Corte suprema relativo alla molestia citofonica, citato dal Tribunale (sez.VI, 5 maggio 1978, n.8759 […]: "nella generica dizione di cui all'art.660 c.p. "col mezzo del telefono" sono compresi anche la molestia e il disturbo recati con altri analoghi mezzi di comunicazione a distanza - citofono eccetera -".

In relazione all'oggetto giuridico della norma incriminatrice l'azione perturbatrice dei due sistemi di telecomunicazione vocale (telefono e citofono) è perfettamente identica; le differenze

tecniche tra telefonia e citofonia sono, sotto tale aspetto, assolutamente irrilevanti; e deve, pertanto, ribadirsi l'interpretazione estensiva della disposizione penale.

Notevolmente diversa è, invece, la comunicazione effettuata con lo strumento della posta elettronica.

La modalità della comunicazione è asincrona. L'azione del mittente si esaurisce nella memorizzazione di un documento di testo (colla possibilità di allegare immagini, suoni o sequenze audiovisive) in una determinata locazione dalla memoria dell'elaboratore del gestore del servizio, accessibile dal destinatario; mentre la comunicazione si perfeziona, se e quando il destinatario, connettendosi, a sua volta, all'elaboratore e accedendo al servizio, attivi una sessione di consultazione della propria casella di posta elettronica e proceda alla lettura del messaggio.

Di tutta evidenza è l'analogia con la tradizionale corrispondenza epistolare in forma cartacea, inviata, recapitata e depositata nella cassetta (o casella) della posta sistemata presso l'abitazione del destinatario.

Epperò l'invio di un messaggio di posta elettronica - esattamente proprio come una lettera spedita tramite il servizio postale - non comporta (a differenza della telefonata) nessuna immediata interazione tra il mittente e il destinatario, né veruna intrusione diretta del primo nella sfera delle attività del secondo.

Orbene, l'evento immateriale - o psichico - del turbamento del soggetto passivo istituisce condizione necessaria ma non sufficiente; infatti per integrare la contravvenzione prevista e punita dall'art.660 c.p., devono concorrere (alternativamente) gli ulteriori elementi circostanziali della condotta del soggetto attivo, tipizzati dalla norma incriminatrice: la pubblicità (o l'apertura al pubblico) del teatro dell'azione ovvero l'utilizzazione del telefono come mezzo del reato.

E il mezzo telefonico assume rilievo - ai fini dell'ampliamento della tutela penale altrimenti limitata alle molestie arrecate in luogo pubblico o aperto al pubblico - proprio per il carattere invasivo della comunicazione alla quale il destinatario non può) sottrarsi, se non disattivando l'apparecchio telefonico, con conseguente lesione, in tale evenienza, della propria libertà di comunicazione, costituzionalmente garantita (art.15, comma 1, Cost.).

Tanto esclude la possibilità dell'interpretazione estensiva seguita dal Tribunale.

Soccorre, infine, anche la considerazione delle ragioni che hanno indotto questa Corte a risolvere positivamente la questione dell'inclusione nella previsione della norma incriminatrice dei messaggi di testo telefonici (sez. III, 26 giugno 2004, n.28680 […]: "La disposizione di cui all'art.660 c.p. punisce la molestia commessa col mezzo del telefono, e quindi anche la molestia posta in essere attraverso l'invio di *short messages system*, SMS, trasmessi attraverso sistemi telefonici mobili o fissi)."

Nell'occasione, il Collegio di legittimità, ribadendo che la molestia "commessa col mezzo epistolare, anche se idonea … a ledere la tranquillità privata della persona destinataria, … non è punibile per se stessa", ai sensi dell'art.660 c.p., ha argomentato, per l'appunto, che i messaggi di testo inviati col mezzo del telefono "non possono essere assimilati a - quelli - di tipo epistolare, in quanto il destinatario di essi è costretto, sia *de auditu* che *de visu*, a percepirli, con corrispondente turbamento della quiete e tranquillità psichica, prima di poterne individuare il mittente, il quale in tal modo realizza l'obiettivo di recare disturbo al destinatario".

Conclusivamente, l'avvertita esigenza di espandere la tutela del bene protetto (della tranquillità della persona) incontra il limite coessenziale della legge penale costituito dal "principio di stretta legalità" e di tipizzazione delle condotte illecite, sanciti dall'art.25, comma 2, Cost. e dall'art.1 c.p. […].

Consegue l'annullamento, senza rinvio, della sentenza impugnata, in relazione al capo impugnato, perché il fatto non è previsto dalla legge come reato.

[…]

2.3. Analogia: stampa ed Internet

Corte di Cassazione, sez.V penale, 1 ottobre 2010, n.35511

[…]

XXXX era direttore del periodico telematico WWWW, sul quale risultava pubblicata una lettera ritenuta diffamatoria nei confronti del ministro della Giustizia (YYYY) e del suo "consulente per l'edilizia penitenziario" (ZZZZ).

[…]

L'art.57 c.p. punisce, come è noto, il direttore del giornale che colposamente non impedisca che, tramite lo pubblicazione sul predetto mezzo di informazione, siano commessi reati. Il codice, per altro, tra i mezzi di informazione, distingue la stampa rispetto a tutti gli altri mezzi di pubblicità (art.595, comma 3, c.p..) e l'art.57 si riferisce specificamente all'informazione diffusa tramite lo "carta stampata". La lettera della legge è inequivoca e a tale conclusione porta anche l'interpretazione "storica" della norma.

In dottrina e in giurisprudenza si è comunque discusso circa l'estensibilità del concetto di stampa, appunto agli altri mezzi di comunicazione. E così una risalente pronunzia […] ha escluso che fosse assimilabile al concetto di stampato la videocassetta preregistrata, in quanto essa viene riprodotta con mezzi diversi da quelli meccanici e fisico-chimici richiamati dall'art.1 della legge 47/1948.

D'altra parte, è noto che la giurisprudenza ha concordemente negato (ad eccezione della sent. n.12960 della sez. feriale […] 12 dicembre 2000 […]) che al direttore della testata televisiva sia applicabile la normativa di cui all'art.57 c.p. […]), stante la diversità strutturale tra i due differenti mezzi di comunicazione (la stampa, da un lato, la radiotelevisione dall'altro) e la vigenza nel diritto penale del principio di tassatività.

Analogo discorso, a parere di questo Collegio, deve esser fatto per quel che riguarda l'assimilabilità di Internet (*rectius* del suo "prodotto") al concetto di stampato.

L'orientamento prevalente in dottrina è stato negativo, atteso che, perché possa parlarsi di stampa in senso giuridico (appunto ai sensi del ricordato art.1 della legge 47/1948), occorrono due condizioni che certamente il nuovo *medium* non realizza: a) che vi sia una riproduzione tipografica (*prius*), b) che il prodotto di tale attività (quella tipografica) sia destinato alla pubblicazione e quindi debba essere effettivamente distribuito tra il pubblico (*posterius*).

Il fatto che il messaggio Internet (e dunque anche la pagina del giornale telematico) si possa stampare non appare circostanza determinante, in ragione della mera eventualità, sia oggettiva, che soggettiva. Sotto il primo aspetto, si osserva che non tutti i messaggi trasmessi via Internet sono "stampabili": si pensi ai video, magari corredati di audio; sotto il secondo, basta riflettere sulla circostanza che, in realtà, è il destinatario colui che, selettivamente ed eventualmente, decide di riprodurre a stampa la "schermata".

E se è pur vero che la "stampa" - normativamente intesa - ha certamente a oggetto, come si è premesso, messaggi destinati alla pubblicazione, è altrettanto vero che deve trattarsi - e anche questo si è anticipato - di comunicazioni che abbiano veste di riproduzione tipografica.

Se pur, dunque, le comunicazioni telematiche sono, a volte, stampabili, esse certamente non riproducono stampati (è in realtà la stampa che – eventualmente - riproduce la comunicazione, ma non l'incorpora, così come una registrazione "domestica" di un film trasmesso dalla TV, riproduce - ad uso del fruitore- un messaggio, quello cinematografico appunto, già diretto "al pubblico" e del quale, attraverso lo duplicazione, in qualche modo il fruitore stesso si appropria, oggettivizzandolo).

Bisogna pertanto riconoscere lo assoluta eterogeneità della telematica rispetto agli altri media, sinora conosciuti e, per quel che qui interessa, rispetto alla stampa.

D'altronde, non si può non sottolineare che differenti sono le modalità tecniche di trasmissione del messaggio a seconda del mezzo utilizzato: consegna materiale dello stampato e sua lettura da parte del destinatario, in un caso (stampa), irradiazione nell'etere e percezione da parte di chi si sintonizza, nell'altro (radio e TV), infine, trasmissione telematica tramite un *ISP* (*Internet service provider*), con utilizzo di rete telefonica nel caso di Internet.

Ad abundantiam si può ricordare che l'art.14 del d.lgs. 9 aprile 2003, n.70 chiarisce che non sono responsabili dei reati commessi in rete gli *access provider*, i *service provider* e - *a fortiori* - gli *hosting provider* […], a meno che non fossero al corrente del contenuto criminoso del messaggio diramato (ma, in tal caso, come è ovvio, essi devono rispondere a titolo di concorso nel reato doloso e non certo *ex* art.57 c.p.).

Qualsiasi tipo di coinvolgimento poi va escluso (tranne, ovviamente, anche in questo caso, per l'ipotesi di concorso) per i coordinatori dei *blog* e dei *forum*.

Non diversa è la figura del direttore del giornale diffuso sul *web*.

Peraltro, anche nel caso oggi in esame, sarebbe, invero, ipotizzabile, in astratto, la responsabilità del direttore del giornale telematico, se fosse stato d'accordo con l'autore della lettera (lo stesso discorso varrebbe per un articolo giornalistico). A maggior ragione, poi, se lo scritto fosse risultato anonimo.

Ma - è del tutto evidente - in tal caso il direttore avrebbe dovuto rispondere del delitto di diffamazione (eventualmente in concorso) e non certo di quello di omesso controllo *ex* art.57 c.p., che come premesso, non è realizzabile da chi non sia direttore di un giornale cartaceo.

Al XXXX, tuttavia, è stato contestato il delitto colposo *ex* art.57 c.p. e non quello doloso *ex* art.595 c.p..

Sul piano pratico, poi, non va trascurato che la cd. interattività (la possibilità di interferire sui testi che si leggono e si utilizzano) renderebbe, probabilmente, vano - o comunque estremamente gravoso - il compito di controllo del direttore di un giornale *online*.

Dunque, accanto all'argomento di tipo sistematico (non assimilabilità normativamente determinata del giornale telematico a quello stampato e inapplicabilità nel settore penale del procedimento analogico *in malam partem*), andrebbe considerata anche la problematica esigibilità dell'ipotetica condotta di controllo del direttore (con quel che potrebbe significare sul piano dell'effettiva individuazione di profili di colpa).

Da ultimo, va considerata anche l'implicita *voluntas legis*, atteso che, da un lato, risultano pendenti diverse ipotesi di estensione della responsabilità *ex* art.57 c.p. al direttore del giornale telematico (il che costituisce ulteriore riprova che - ad oggi - tale responsabilità non esiste), dall'altro, va pur rilevato che il legislatore, come ricordato dal ricorrente, è effettivamente intervenuto, negli ultimi anni, sulla materia senza minimamente innovare sul punto.

Invero, né con la legge 7 marzo 2001 n.62, né con il già menzionato d.lgs. del 2003, è stata effettuata l'estensione dell'operatività dell'art.57 c.p. dalla carta stampata ai giornali telematici, essendosi limitato il testo del 2001 a introdurre la registrazione dei giornali *online* (che dunque devono necessariamente avere al vertice un direttore) solo per ragioni amministrative e, in ultima analisi, perché possano essere richieste le provvidenze previste per l'editoria (come ha chiarito il successivo decreto legislativo).

Allo stato, dunque, "il sistema" non prevede la punibilità ai sensi dell'art.57 c.p. (o di un analogo meccanismo incriminatorio) del direttore di un giornale *online*.

Rimanendo pertanto assorbita la censura *sub* 1), deve concludersi che la sentenza impugnata va annullata senza rinvio perché il fatto non è previsto dalla legge come reato.

P.Q.M.

la Corte annulla senza rinvio la sentenza impugnata perché il fatto non è previsto dalla legge come reato.

[…]

2.4. Analogia: danno morale e *social network*

Tribunale di Monza, sez.IV civile, 2 marzo 2010, n.770

[…]

La presente controversia, di indubbia peculiarità, trae le proprie origini dal rapporto instaurato tra le odierne parti per il tramite del sito *web* denominato "Fa." Trattasi, come è ormai notorio, di un cd. *social network* ad accesso gratuito fondato nel 2004 da uno studente dell'Università di Ha. al quale, a far tempo dal settembre 2006, può partecipare chiunque abbia compiuto dodici anni di età; peraltro, se scopo iniziale di "Fa." era il mantenimento dei contatti tra studenti di università e scuole superiori di tutto il mondo, in soli pochi anni ha assunto i connotati di una vera e proprie rete sociale destinata a coinvolgere, in modo trasversale, un numero indeterminato di utenti o di navigatori Internet.

Questi ultimi partecipano creando "profili" contenenti fotografie e liste di interessi personali, scambiando messaggi (privati o pubblici) e aderendo ad un gruppo di cd. "amici": quest'ultimo aspetto è rilevante, anche ai fini della presente decisione, in quanto la visione dei dati dettagliati del profilo di ogni singolo utente è di solito ristretta agli "amici" dallo stesso accettati.

"Fa.", come detto, include alcuni servizi tra i quali la possibilità per gli utenti di ricevere ed inviare messaggi e di scrivere sulla bacheca di altri utenti e consente di impostare l'accesso ai vari contenuti del proprio profilo attraverso una serie di "livelli" via via più ristretti e/o restrittivi (dal livello "Tutti" a quello intermedio "Amici di amici" ai soli "Amici") per di più in modo selettivo quanto ai contenuti o alle stesse "categorie" di informazioni inserite nel profilo medesimo.

Quindi, agendo opportunamente sul livello e sulle impostazioni del proprio profilo, è possibile limitare l'accesso e la diffusione dei propri contenuti, sia dal punto di vista soggettivo che da quello oggettivo.

È peraltro nota agli utenti di "Fa." l'eventualità che altri possano in qualche modo individuare e riconoscere le tracce e le informazioni lasciate in un determinato momento sul sito, anche a prescindere dal loro consenso: trattasi dell'attività di cd. "*tagging*" (tradotta in lingua italiana con l'uso del neologismo "*taggare*") che consente, ad esempio, di copiare messaggi e foto pubblicati in bacheca e nel profilo altrui oppure *email* e conversazioni in *chat*, che di fatto sottrae questo materiale dalla disponibilità dell'autore e sopravvive alla stessa sua eventuale cancellazione dal *social network*.

I gestori del sito (statunitensi, secondo la Polizia Postale), pur reputandosi proprietari dei contenuti pubblicati, declinano ogni responsabilità civile e/o penale ad essi relativa (come dimostra, eloquentemente, una recentissima e dibattuta controversia giudiziaria riguardante il motore di ricerca "Go.").

In definitiva, coloro che decidono di diventare utenti di "Fa." sono ben consci non solo delle grandi possibilità relazionali offerte dal sito, ma anche delle potenziali esondazioni dei contenuti che vi inseriscono: rischio in una certa misura indubbiamente accettato e consapevolmente vissuto.

Il caso di specie è emblematico in tal senso.

Due giovani si conoscono e socializzano tramite "Fa." e tra loro ha inizio una relazione da entrambi definita sentimentale, con sviluppi non lineari ed irreprensibili, descritti dal convenuto in modo minuzioso, pur se irrilevanti ai fini della presente decisione.

In tale contesto si inserisce l'invio da parte di T.P. di un messaggio a mezzo "Fa." a F.B., datato 1 ottobre 2008 e del seguente eloquentissimo tenore: "Senti brutta troia strabica che nn sei altro ... T consiglio di smetterla. Nn voglio fare il cattivo sputtanandoti nella tua sfera sociale dove le persone t stimano (*Facebook*, *MySpace*, ecc.). Purtroppo nn siamo To. Ve. o Fi. Na. ... quindi nn appetibili sessualmente per te. T consiglio di caricare le foto ove la frangia nn t nasconde il litigio continuo dei tuoi occhi e nello stesso tempo il numero di un bravo psichiatra che può prescriverti al più presto possibile, pastiglie rettali da cavallo con funzione antidepressiva (se t piaceva il dito nn mi immagino il farmaco). Con queste affermazioni, vere, chiedo di eclissarti e di smetterla di ossessionarmi come il tuo grande idolo e modello comportamentale ... Mentos! Ah ... Tutti i miei orgasmi erano finti ...=) ihoho".

Trattasi, in tutta evidenza, di un messaggio denotante la conoscenza non solo dell'imperfezione fisica sofferta da F.B., ma anche e soprattutto di alcune sue presunte preferenze maschili e abitudini sessuali. Per di più, il messaggio presuppone precedenti conversazioni non gradite al mittente ("T consiglio di smetterla") e che trovano riscontro nelle difese del convenuto, laddove ha lamentato il preteso comportamento persecutorio di parte attrice e la propria conseguente giustificata reazione.

Difese che, ad onor del vero, si appalesano *ictu oculi* come contraddittorie nel momento in cui alla contestazione della provenienza del messaggio è poi soggiunta la non riferibilità a F.B. del suo contenuto.

Immeritevoli di accoglienza appaiono, comunque, le generiche eccezioni svolte dal convenuto in relazione all'effettiva provenienza del messaggio *de quo*, posto che è ampiamente documentata dall'attrice la partecipazione di T.P. alla discussione in *chat* messaggistica sul profilo di un comune "amico Fa." (tale G.F.) a commento di una foto che li ritrae assieme, l'inserimento di F.B. in tale conversazione *web* e la replica finale suggellata dal messaggio del quale oggi si discute (doc. 2).

Maggiormente dimostrativo della provenienza dal convenuto del messaggio in esame è l'ulteriore scambio di messaggi avvenuto tra le parti in ora tarda (ore 22,37 attrice - ore 1,03 convenuto: doc.3), dal quale si evince anche la volontà di T.P. di rivendicare nuovamente il contenuto di quanto in precedenza scritto ("Se fosse stato per me il commento l'avrei lasciato, ma il mio amico l'ha voluto cancellare ...") e di voler sin da allora individuare una possibile scappatoia nella pretesa non riferibilità all'attrice delle gravi espressioni adottate ("Non vedo il tuo nome scritto nel commento pubblico della mia foto con i miei amici").

Quest'ultima affermazione del convenuto è, di contro, dimostrativa del carattere pubblico delle offese arrecate: offese certamente riconducibili in modo immediato e diretto a F.B., non solo per la riferita forzata condivisione con i comuni "amici Fa." delle abitudini di vita dell'attrice e dei suoi asseriti comportamenti vessatori (v. pag.4 comparsa di risposta), ma anche più semplicemente per l'evidente circostanza che il messaggio ingiurioso è immediatamente successivo a quello inviato dalla stessa F.B. a commento della foto pubblicata dal comune "amico Fa." G.F. (il quale, poi, a detta dello stesso convenuto ebbe a "cancellare" il messaggio *de quo*).

La nota impossibilità di registrazione nel *social network* a nome di un utente già registrato […] e l'assenza di formali denunzie del convenuto concernenti eventuali e non dimostrati "furti d'identità" (anzi escludibili, alla luce dell'utilizzazione del medesimo recapito *email*, in altre occasioni pubblicato: doc. 7) consentono di affermare la provenienza del messaggio da T.P.

Se a ciò si aggiungono le ulteriori considerazioni già ampiamente svolte in relazione alle note caratteristiche di "Fa.", ai suoi altrettanto notori e conosciuti limiti ed alla consapevole accettazione dei conseguenti rischi di una sua non corretta utilizzazione, non possono sussistere ragionevoli dubbi sull'affermazione di civile responsabilità del convenuto quanto agli effetti ed ai pregiudizi arrecati dal messaggio del giorno 1 ottobre 2008 e dalla reale (e ancor potenziale) sua diffusione.

Dunque, T.P. deve essere condannato al risarcimento dei danni arrecati per tale via a F.B., dovendosi al riguardo escludere le invocate scriminanti o diminuenti di cui all'art.599, comma 2, c.p. ed all'art.1227 c.c., certamente apparse incongrue anche in ossequio alla stessa prospettazione dei fatti offerta dalla difesa del convenuto.

[…]

Qui va rimarcata la risarcibilità, attesi i limiti della domanda attrice, del solo danno morale soggettivo inteso quale "transeunte turbamento dello stato d'animo della vittima" del fatto illecito, vale a dire come complesso delle sofferenze inferte alla danneggiata dall'evento dannoso, indipendentemente dalla sua rilevanza penalistica.

Rilevanza che, peraltro, ben potrebbe essere ravvisata nel fatto dedotto in giudizio, concretamente sussumibile nell'ambito dell'astratta previsione di cui all'art.594 c.p. (ingiuria) ovvero in quella più grave di cui all'art.595 c.p. (diffamazione) alla luce del cennato carattere pubblico del contesto che ebbe a ospitare il messaggio *de quo*, della sua conoscenza da parte di più persone e della possibile sua incontrollata diffusione a seguito di *tagging*.

Elemento, quest'ultimo, idoneo ad ulteriormente qualificare la potenzialità lesiva del fatto illecito, in uno con i documentati problemi di natura fisica ed estetica sofferti da F.B. […].

Alla luce di quanto accertato in fatto, dell'evidente lesione di diritti e valori costituzionalmente garantiti (la reputazione, l'onore, il decoro della vittima) e delle conseguenti indubbie sofferenze

inferte all'attrice dalla vicenda della quale si discute, in via di equità, può essere liquidata ai valori attuali, a titolo di danno morale ovvero non patrimoniale, la somma di euro 15.000,00.

[…]

2.5. Le norme sociali

RFC 1855 – Netiquette guidelines, 28 ottobre 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.

Table of Contents

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.

We've organized this material into three sections: One-to-one communication, which includes mail and talk; One-to-many communications, which includes mailing lists and NetNews; and Information Services, which includes ftp, WWW, Wais, Gopher, MUDs and MOOs. Finally, we have a Selected Bibliography, which may be used for reference.

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 your 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).

- Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending.

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

[…]

- Remember that people with whom you communicate are located across the globe. If you send a message to which you want an immediate response, the person receiving it might be at home asleep when it arrives. Give them a chance to wake up, come to work, and login before assuming the mail didn't arrive or that they don't care.

- Verify all addresses before initiating long or personal discourse.

It's also a good practice to include the word "Long" in the subject header so the recipient knows the message will take time to read and respond to. Over 100 lines is considered "long".

[…]

- 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 email message to let the sender know you got it, even if you will send a longer reply later.

- "Reasonable" expectations for conduct via email depend on your relationship to a person and the context of the communication. Norms learned in a particular email environment may not

apply in general to your email communication with people across the Internet. Be careful with slang or local acronyms.

- The cost of delivering an email 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 email 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.

- Don't send large amounts of unsolicited information to people.

[…]

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!

2.2 Administrator Issues

- Be sure you have established written guidelines for dealing with situations especially illegal, improper, or forged traffic.

- Handle requests in a timely fashion - by the next business day.

- Respond promptly to people who have concerns about receiving improper or illegal messages. Requests concerning chain letters should be handled immediately.

- Explain any system rules, such as disk quotas, to your users. Make sure they understand implications of requesting files by mail such as: Filling up disks; running up phone bills, delaying mail, etc.

[…]

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 Newsgroups 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.

- If you are sending a reply to a message or a posting be sure you summarize the original at the top of the message, or include just enough text of the original to give a context. This will make sure readers understand when they start to read your response. Since NetNews, especially, is proliferated by distributing the postings from one host to another, it is possible to see a response to a message before seeing the original. Giving context helps everyone. But do not include the entire original!

- Again, be sure to have a signature which you attach to your message. This will guarantee that any peculiarities of mailers or newsreaders which strip header information will not delete the only reference in the message of how people may reach you.

- Be careful when you reply to messages or postings. Frequently replies are sent back to the address which originated the post - which in many cases is the address of a list or group! You may accidentally send a personal response to a great many people, embarrassing all involved. It's best to type in the address instead of relying on "reply."

- Delivery receipts, non-delivery notices, and vacation programs are neither totally standardized nor totally reliable across the range of systems connected to Internet mail. They are invasive when sent to mailing lists, and some people consider delivery receipts an invasion of privacy. In short, do not use them.

- If you find a personal message has gone to a list or group, send an apology to the person and to the group.

- If you should find yourself in a disagreement with one person, make your responses to each other via mail rather than continue to send messages to the list or the group. If you are debating a point on which the group might have some interest, you may summarize for them later.

- 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

There are several ways to find information about what mailing lists exist on the Internet and how to join them. Make sure you understand your organization's policy about joining these lists and posting to them. In general it is always better to check local resources first before trying to find information via the Internet. Nevertheless, there are a set of files posted periodically to news.answers which list the Internet mailing lists and how to subscribe to them. This is an invaluable resource for finding lists on any topic […].

- Send subscribe and unsubscribe messages to the appropriate address. Although some mailing list software is smart enough to catch these, not all can ferret these out. It is your responsibility to learn how the lists work, and to send the correct mail to the correct place. Although many many mailing lists adhere to the convention of having a "-request" alias for sending subscribe and unsubscribe messages, not all do. Be sure you know the conventions used by the lists to which you subscribe.

- Save the subscription messages for any lists you join. These usually tell you how to unsubscribe as well.

[…]

- 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-replys 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.

- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting.

- If you ask a question, be sure to post a summary. When doing so, truly summarize rather than send a cumulation of the messages you receive.

- Some mailing lists are private. Do not send mail to these lists uninvited. Do not report mail from these lists to a wider audience.

- If you are caught in an argument, keep the discussion focused on issues rather than the personalities involved.

3.1.3 NetNews Guidelines

NetNews is a globally distributed system which allows people to communicate on topics of specific interest. It is divided into hierarchies, with the major divisions being: *sci* - science related discussions; *comp* - computer related discussions; news - for discussions which center around NetNews itself; *rec* - recreational activities; *soc* - social issues; *talk* - long-winded never-ending discussions; *biz* - business related postings; and *alt* - the alternate hierarchy. *Alt* is so named because creating an *alt* group does not go through the same process as creating a group in the other parts of the hierarchy. There are also regional hierarchies, hierarchies which are widely distributed such as Bionet, and your place of business may have its own groups as well. Recently, a "humanities" hierarchy was added, and as time goes on its likely more will be added. […]

- In NetNews parlance, "Posting" refers to posting a new article to a group, or responding to a post someone else has posted. "Cross-Posting" refers to posting a message to more than one group. If you introduce Cross-Posting to a group, or if you direct "Followup-To:" in the header of your posting, warn readers! Readers will usually assume that the message was posted to a specific group and that followups will go to that group. Headers change this behavior.

- Read all of a discussion in progress (we call this a thread) before posting replies. Avoid posting "Me Too" messages, where content is limited to agreement with previous posts. Content of a follow-up post should exceed quoted content.

- Send mail when an answer to a question is for one person only. Remember that News has global distribution and the whole world probably is NOT interested in a personal response. However, don't hesitate to post when something will be of general interest to the Newsgroup participants.

[…]

- Consider using Reference sources (Computer Manuals, Newspapers, help files) before posting a question. Asking a Newsgroup where answers are readily available elsewhere generates grumpy "RTFM" (read the fine manual - although a more vulgar meaning of the word beginning with "f" is usually implied) messages.

- Although there are Newsgroups which welcome advertising, in general it is considered nothing less than criminal to advertise off-topic products. Sending an advertisement to each and every group will pretty much guarantee your loss of connectivity.

[…]

- If you've posted something and don't see it immediately, don't assume it's failed and re-post it.

[…]

- Forging of news articles is generally censured. You can protect yourself from forgeries by using software which generates a manipulation detection "fingerprint", such as PGP (in the US).

- Postings via anonymous servers are accepted in some Newsgroups and disliked in others. Material which is inappropriate when posted under one's own name is still inappropriate when posted anonymously.

[…]

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

3.2 Administrator Guidelines

3.2.1 General Issues

- Clarify any policies your site has regarding its subscription to NetNews groups and about subscribing to mailing lists.
- Clarify any policies your site has about posting to NetNews groups or to mailing lists, including use of disclaimers in .sigs.
- Clarify and publicize archive policy. (How long are articles kept?)
- Investigate accusations about your users promptly and with an open mind.
- Be sure to monitor the health of your system.
- Consider how long to archive system logs, and publicize your policy on logging.

3.2.2 Mailing Lists

- Keep mailing lists up to date to avoid the "bouncing mail" problem.
- Help list owners when problems arise.
- Inform list owners of any maintenance windows or planned downtime.
- Be sure to have "-request" aliases for list subscription and administration.
- Make sure all mail gateways operate smoothly.

[…]

3.3 Moderator Guidelines

3.3.1 General Guidelines

- Make sure your Frequently Asked Questions (FAQ) is posted at regular intervals. Include your guidelines for articles/messages.

If you are not the FAQ maintainer, make sure they do so.

- Make sure you maintain a good welcome message, which contains subscribe and unsubscribe information.

[…]

4.0 Information Services (Gopher, Wais, WWW, ftp, telnet)

In recent Internet history, the 'Net has exploded with new and varied Information services. Gopher, Wais, World Wide Web (WWW), Multi-User Dimensions (MUDs) Multi-User Dimensions which are Object Oriented (MOOs) are a few of these new areas. Although the ability to find information is exploding, "Caveat Emptor" remains constant. […]

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 online without permission.

4.2 Administrator Guidelines

4.2.1 General Guidelines

- Make clear what's available for copying and what is not.
- Describe what's available on your site, and your organization. Be sure any general policies are clear.
- Keep information, especially READMEs, up-to-date. Provide READMEs in plain ascii text.

[…]

- When providing information, make sure your site has something unique to offer. Avoid bringing up an information service which simply points to other services on the Internet.

- Don't point to other sites without asking first.

- Remember that setting up an information service is more than just design and implementation. It's also maintenance.

- Test applications with a variety of tools. Don't assume everything works if you've tested with only one client. Also, assume the low end of technology for clients and don't create applications which can only be used by Graphical User Interfaces.

- Have a consistent view of your information. Make sure the look and feel stays the same throughout your applications.

- Be sensitive to the longevity of your information. Be sure to date time-sensitive materials, and be vigilant about keeping this information well maintained.

- Export restrictions vary from country to country. Be sure you understand the implications of export restrictions when you post.

- Tell users what you plan to do with any information you collect, such as WWW feedback. You need to warn people if you plan to publish any of their statements, even passively by just making it available to other users.

- Make sure your policy on user information services, such as home pages, is well known.

[…]

2.6. La *self-regulation*

Codice di autoregolamentazione Internet e minori, 19 novembre 2003

[…]

Art.1 - Definizioni

1.1 Aderente

Il soggetto che svolge attività imprenditoriale su Internet, anche a titolo non direttamente oneroso per Clienti ed Utenti, e che aderisce al Codice direttamente o per il tramite delle Associazioni firmatarie.

1.2 Cliente

Il soggetto giuridico che stipula un contratto con l'Aderente.

1.3 Utente

Il soggetto, anche diverso dal Cliente, che utilizza i servizi forniti dall'Aderente.

1.4 *Access provider*

Il soggetto che offre al pubblico e nell'ambito della propria attività imprenditoriale servizi di accesso ad Internet.

1.5 *Hosting/housing provider*

Il soggetto che offre al pubblico spazi raggiungibili dall'esterno (*shared/dedicated hosting provider*) o la possibilità di collegare computer di proprietà del Cliente alla rete Internet (*housing provider*).

1.6 *Content provider*

Il soggetto che, direttamente o indirettamente, mette a disposizione del pubblico, con qualsiasi mezzo o protocollo tecnico, dati, informazioni e programmi.

1.7 Gestore dell'Internet Point

Il soggetto che mette a disposizione del pubblico locali e strumenti, non ad uso esclusivo, che consentono l'accesso ai servizi della rete Internet.

1.8 Servizi di navigazione differenziata

Servizi di accesso ad Internet che, sulla base di criteri indicati dall'Aderente ai sensi del successivo p.to 3.2, circoscrivono o escludono l'accesso a determinati contenuti.

1.9 Accesso condizionato

Modalità di accesso a contenuti, altrimenti non disponibili all'Utente, mediante procedure e/o strumenti di tipo logico o fisico (ad es. codice identificativo di utente, *password*, *smart card*, ecc.).

1.10 Marchio "Internet e Minori"

Logotipo che testimonia l'adesione al Codice del soggetto che svolge attività imprenditoriale su Internet e ne attesta la conformità dei comportamenti agli impegni assunti. Il marchio verrà prescelto dal Comitato di Garanzia di cui al successivo art.6.

Art.2 - Ambito e modalità di applicazione

2.1 Adesione

Il Codice, promosso dalle Associazioni firmatarie, si applica a tutti gli Aderenti che lo sottoscrivono direttamente o attraverso le Associazioni medesime.

L'Aderente potrà pubblicare, sui propri servizi e nelle comunicazioni commerciali, la dicitura "Aderente al Codice di autoregolamentazione Internet e Minori" oltre al relativo logo che viene concesso in licenza d'uso gratuito e a tempo indeterminato fino all'eventuale revoca, secondo quanto disposto all'art.7.

2.2 Obblighi conseguenti all'adesione

L'adesione volontaria al presente Codice di autoregolamentazione implica inderogabilmente:

– l'accettazione integrale dei contenuti del Codice stesso e in particolare l'accettazione delle attività di vigilanza e delle sanzioni ivi previste;

– l'adattamento delle condizioni contrattuali di prestazione dei servizi alle disposizioni del presente Codice.

2.3 Recesso

L'adesione al Codice ed ai suoi aggiornamenti periodici è a tempo indeterminato. L'eventuale recesso dell'Aderente dovrà essere comunicato secondo le modalità fissate dal Regolamento di Organizzazione di cui al successivo p.to 6.2.

Art.3 - Strumenti per la tutela del minore

3.1 Informazione alle Famiglie e agli Educatori

L'Aderente pubblica nella pagina Internet iniziale (*home page*) dei propri servizi un riferimento "TUTELA DEI MINORI", chiaramente visibile, che rimanda ad apposite pagine *web* con le quali fornire informazioni sulle corrette modalità per un utilizzo sicuro della rete Internet, sull'esistenza degli strumenti più utilizzati per la tutela dei minori e sulle modalità di segnalazione, al Comitato di Garanzia di cui all'art.6, delle violazioni del Codice. Il contenuto minimo delle pagine *web* verrà definito dal Comitato di Garanzia.

3.2 Servizi di navigazione differenziata

L'Aderente offrirà, secondo le tecnologie disponibili, alle Famiglie, agli Educatori, alle Scuole, alle Biblioteche e alle Aggregazioni giovanili, Servizi di navigazione differenziata che dovranno essere chiaramente identificabili come tali, ovvero indirizzerà il Cliente e gli Utenti verso altri fornitori di Servizi di navigazione differenziata. Nel rispetto del principio di non discriminazione, tali servizi non potranno impedire l'accesso ai contenuti sicuri offerti dai *content providers* aderenti.

3.3 Classificazione dei contenuti

Il *content provider* aderente potrà applicare i sistemi di classificazione ai contenuti che riterrà opportuno subordinare ad Accesso condizionato.

3.4 Identificatori d'età

L'Aderente potrà utilizzare Sistemi di individuazione dell'età dell'Utente, a condizione che, nel rispetto delle norme sul trattamento dei dati personali, ne venga tutelata e garantita la massima riservatezza, sicurezza e dignità. In particolare, tali sistemi non dovranno consentire di risalire all'identità, al domicilio, all'indirizzo di posta elettronica, all'eventuale pseudonimo ("*alias*" o "*nickname*"), all'indirizzo Internet (numero IP) del minore e non dovranno comunque permettere a terzi di raggiungerlo direttamente o indirettamente.

3.5 Profilazione e trattamenti occulti

Nel rispetto del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n.196), l'Aderente non esegue alcuna profilazione dell'Utente minore né alcun trattamento dei suoi dati personali senza la previa autorizzazione espressa, a seguito di informativa chiara e trasparente sulla tipologia delle profilazioni che l'Aderente medesimo intende effettuare e sull'uso che di tali informazioni intende fare, da parte di chi esercita la potestà genitoriale.

3.6 Custodia di *password*

L'Aderente custodisce le *passwords* di accesso ai servizi assegnate agli Utenti con adeguate misure di sicurezza. L'Aderente si impegna a fornire all'Utente la possibilità di cambiare la *password*.

3.7 Anonimato protetto

L'Aderente potrà consentire agli Utenti di utilizzare i propri servizi in modo da apparire totalmente anonimi.

In ogni caso, l'Aderente dovrà essere effettivamente informato della reale identità personale del soggetto cui viene concesso di fruire dell'anonimizzazione. All'interno dell'informazione di cui al p.to 3.1 l'Aderente dovrà altresì avvertire preventivamente gli Utenti della possibilità che elaborazioni non autorizzate, effettuate abusivamente da terze parti all'insaputa dell'Aderente, possano comunque consentire di risalire alla loro identità.

3.8 Identificazione dell'Utente

L'Aderente eroga i propri servizi solo ed esclusivamente a Utenti identificati direttamente o identificabili tramite elementi univoci anche se indiretti.

3.9 Prestazione di servizi fiduciari

L'Aderente che offre servizi in via fiduciaria (ad esempio registrazione di un nome a dominio per conto di un Cliente che vuole rimanere ignoto) è obbligato a identificare in modo certo il Cliente che richiede tali servizi, serbando la massima riservatezza.

3.10 Gestione dei dati utili alla tutela dei minori

3.10.1 Individuazione dei dati

L'accesso alla rete Internet richiede l'assegnazione permanente o temporanea all'Utente di un indirizzo di rete (indirizzo IP). Nei limiti imposti dalla normativa vigente, l'Aderente conserva, come dati utili:

a) i registri di assegnazione degli indirizzi IP;

b) il numero IP utilizzato per l'accesso alle eventuali funzioni di pubblicazione dei contenuti.

Nel caso di assegnazione temporanea dell'indirizzo IP, il relativo registro conterrà: data e ora di inizio e cessazione dell'assegnazione, numero di IP assegnato temporaneamente ed eventuale numero telefonico utilizzato (se disponibile).

3.10.2 Modalità e tempi di conservazione dei dati

L'Aderente conserva i dati di cui al p.to 3.10.1 con modalità che ne garantiscano una ragionevole attendibilità e non ripudiabilità, comunque nel rispetto delle disposizioni vigenti in materia.

I dati medesimi vengono custoditi per sei mesi, salva la scelta individuale di conservarli per periodi maggiori, senza comunque eccedere i limiti temporali indicati dalla normativa vigente.

3.10.3 Modalità di comunicazione dei dati

3.10.3.1 All'Autorità giudiziaria

Nel caso di provvedimento dell'Autorità giudiziaria, l'Aderente, eseguirà quanto richiesto documentando per iscritto le operazioni compiute.

3.10.3.2 Al Cliente

Secondo quanto previsto dalle norme sul trattamento dei dati personali (d.lgs. 196/2003), l'Aderente fornirà al Cliente solo ed esclusivamente le informazioni che lo riguardano e comunque a fronte di richiesta scritta e identificazione certa del richiedente.

3.11 Contrasto alla pedopornografia *online*

L'Aderente, nel rispetto delle normative vigenti in materia di trattamento dei dati personali, si impegna a conservare il numero IP utilizzato dall'Utente per l'accesso alle funzioni di pubblicazione dei contenuti, anche se ospitati gratuitamente.

L'Aderente pone in essere tutte le iniziative atte a realizzare la collaborazione con le autorità competenti, e in particolare con il Servizio della Polizia Postale e delle Comunicazioni, al fine di rendere identificabili gli assegnatari delle risorse di rete utilizzate per la pubblicazione dei contenuti ospitati presso i propri *server*, così come risultanti dai relativi contratti o documenti equipollenti, entro e non oltre i tre giorni lavorativi successivi al ricevimento del provvedimento dell'Autorità richiedente.

Art.4 - Responsabilità

4.1 *Access provider*

L'Aderente che offre servizi di accesso ad Internet dovrà verificare direttamente (p.e. tramite l'avvenuta sottoscrizione di un contratto) o indirettamente (almeno tramite CLI - *Calling Line Identifier* - o metodi analoghi) l'accesso alla rete.

Nei contratti di accesso ad Internet l'Aderente inserisce clausole che responsabilizzano il Cliente anche per l'uso dei servizi concessi a terzi.

4.2 *Housing/hosting provider*

L'Aderente che offre servizi di *housing* e *hosting* dedicato dovrà identificare con ragionevole certezza il proprio Cliente che ha il controllo degli apparati oggetto di tali servizi. Nel caso di servizi di *hosting* condiviso, l'Aderente è tenuto a conservare i dati di cui alla lett.b) del p.to 3.10.

4.3 *Content provider*

L'Aderente che offre direttamente contenuti tramite qualsiasi metodo o protocollo di comunicazione, è tenuto a identificare in modo chiaro, ricorrendo eventualmente alle metodologie indicate al p.to 3.3, la natura e i contenuti della comunicazione stessa, adoperandosi per adeguare o rimuovere il contenuto su segnalazione del Comitato di Garanzia, di cui al successivo art.6, e comunque delle Autorità competenti.

4.4 Gestore dell'*Internet Point*

L'Aderente che offre servizi di accesso al pubblico come "Internet Point" o simili deve fornire strumenti adeguati per la navigazione dei minori ed identificare, direttamente o indirettamente, l'utilizzatore dei servizi medesimi.

Art.5 - Vigilanza

La vigilanza sulla corretta applicazione del Codice è affidata al Comitato di Garanzia di cui al successivo art.6.

In un'ottica di armonizzazione e di verifica degli sviluppi tecnologici e normativi il Comitato di Garanzia suggerisce eventuali aggiornamenti e modifiche del presente Codice.

Art.6 - Comitato di Garanzia

6.1 Costituzione

La corretta, imparziale e trasparente applicazione del Codice è affidata ad un apposito Comitato di Garanzia (in seguito indicato anche come "Comitato") costituito da undici componenti

effettivi, esperti in materia, nominati con Decreto del Ministro delle Comunicazioni, adottato di concerto con il Ministro per l'Innovazione e le Tecnologie ed individuati come segue:

– quattro componenti in rappresentanza degli Aderenti designati dalle Associazioni di categoria firmatarie del presente Codice;

– due componenti, di cui uno con funzioni di Presidente, in rappresentanza del Ministero delle Comunicazioni e due in rappresentanza della Presidenza del Consiglio dei Ministri - Dipartimento dell'Innovazione e delle Tecnologie;

– tre componenti designati dalle Associazioni per la tutela dei minori e dal Consiglio Nazionale degli Utenti. In sede di prima nomina tali ultimi componenti saranno scelti tra i partecipanti al Gruppo di lavoro Internet@minori, istituito presso il Ministero delle Comunicazioni.

Il Ministero delle Comunicazioni assicura la Segreteria per le attività di supporto al Comitato.

Con i medesimi criteri e modalità sono nominati anche undici componenti supplenti.

I componenti ed il Presidente nominati durano in carica tre anni.

6.2 Funzionamento

Le regole di funzionamento del Comitato e della Segreteria sono definite da un apposito Regolamento di Organizzazione adottato di comune accordo dai componenti del Comitato medesimo entro 30 giorni dal suo insediamento.

Nel medesimo Regolamento verranno indicate le modalità di realizzazione dell'apposito sito *web* dedicato al Codice.

6.3 Poteri

Il Comitato controlla che l'Aderente possieda tutti i requisiti e abbia assunto tutti i comportamenti previsti dal Codice, segnalando agli interessati eventuali inottemperanze al Codice medesimo.

Nel caso di accertate inottemperanze da parte degli Aderenti si applicheranno le sanzioni di cui al successivo art.7.

6.4 Tempi di attuazione del Codice

Il Comitato di Garanzia individuerà i tempi per rendere effettivi gli obblighi di cui al presente Codice, che comunque entreranno in vigore entro e non oltre i sei mesi successivi alla firma dello stesso.

6.5 Decadenza dei componenti

Il Comitato di Garanzia definisce nel Regolamento di Organizzazione le ragioni che determinano la decadenza dei componenti del Comitato.

6.6 Rimborsi

Le Associazioni firmatarie del presente Codice si impegnano a segnalare, entro i trenta giorni successivi alla sottoscrizione del presente Codice, l'Associazione, tra quelle firmatarie, che garantirà il rimborso delle spese sostenute, e documentate, dai rappresentanti delle Associazioni per la tutela dei minori per la loro partecipazione alle sedute del Comitato di Garanzia, secondo le modalità che saranno stabilite dal Regolamento di organizzazione del Comitato medesimo. Tali spese saranno suddivise tra tutte le Associazioni firmatarie. Il limite massimo annuo complessivo di tali spese è fissato in 8.000 euro. Saranno ricercate altre forme di finanziamento e sostegno anche da parte di enti istituzionali per l'eventuale svolgimento di attività di studio, promozione, ricerca e comunicazione anche in relazione alla campagna d'informazione che sarà auspicabilmente effettuata sul tema della tutela dei minori in Rete.

Art.7 - Procedure e misure di autodisciplina

7.1 Procedura per l'irrogazione dei provvedimenti disciplinari

7.1.1 Attivazione del procedimento

Chiunque ritenga fondatamente che sia intervenuta da parte dell'Aderente una violazione degli obblighi definiti all'art.3, può segnalare al Comitato di Garanzia tale violazione inviando una comunicazione alla Segreteria del Comitato medesimo secondo le indicazioni del p.to 3.1.

Per attivare la segnalazione dovrà essere compilato l'apposito modulo guidato, contenuto nelle pagine *web* informative, di cui al p.to 3.1, indicando:

– le sue generalità;

– i suoi recapiti (indirizzo completo e numero di telefono, nonché, eventualmente, numero di fax ed indirizzo *email*);

– descrizione dettagliata della violazione della norma del Codice e degli elementi di responsabilità dell'Aderente riscontrati;

All'invio della segnalazione "telematica" di cui sopra, verrà attribuito un Numero di Protocollo che l'interessato dovrà indicare nella lettera di conferma (contenete gli stessi elementi informativi) da inviare per posta, tramite Raccomandata A.R., alla Segreteria del Comitato.

La Segreteria procede ad una classificazione e registrazione delle segnalazioni ricevute ed accompagnate dalla relativa conferma postale.

I dati trasmessi verranno trattati secondo le norme sulla tutela dei dati personali.

7.1.2 Comunicazione di apertura del procedimento

La Segreteria, esaminate le segnalazioni pervenute, entro una settimana dal ricevimento della lettera raccomandata di conferma, comunica all'Aderente l'apertura del procedimento di autodisciplina nei suoi confronti e le contestazioni oggetto della segnalazione. Vengono considerate inammissibili le segnalazioni prive dei requisiti di cui al p.to 7.1.1.

7.1.3 Richiesta di documentazione

L'Aderente che riceve una comunicazione di apertura di un procedimento di autodisciplina nei suoi confronti, può trasmettere alla Segreteria, entro quindici giorni dalla comunicazione, la documentazione che ritiene utile per chiarire la sua posizione.

7.1.4 Audizione dell'Aderente

L'Aderente al quale sia stata comunicata l'apertura di un procedimento di autodisciplina, può richiedere un'audizione al Comitato negli stessi tempi previsti per l'invio di documentazione.

L'audizione sarà effettuata in occasione della prima riunione del Comitato, che informerà l'interessato con un preavviso non inferiore a dieci giorni.

7.1.5 Decisione

Il Comitato opera, di norma, per via telematica e la Segreteria predispone i verbali delle attività che vengono sottoposti all'approvazione dei singoli componenti. Il Comitato completa l'iter procedurale entro sessanta giorni dall'apertura del procedimento di autodisciplina. Le decisioni finali vengono prese a maggioranza dei due terzi (con approssimazione all'unità superiore).

Le audizioni si svolgono nell'ambito di riunioni del Comitato valide, ai fini delle decisioni, solo se alla presenza di almeno i due terzi (con approssimazione all'unità superiore) del numero dei componenti.

Gli esiti delle procedure di autodisciplina rimangono agli atti del Comitato e vengono conservati a cura della Segreteria che li trasmette alle parti interessate e ne cura la pubblicazione sull'apposito sito *web* previsto dal Regolamento di Organizzazione.

7.1.6 Esecuzione della decisione

L'Aderente dà seguito a quanto deciso dal Comitato tempestivamente e comunque non oltre i quindici giorni successivi alla comunicazione del provvedimento adottato. La mancata esecuzione di quanto previsto nella decisione comporta, a seguito della procedura prevista dall'art.7, l'applicazione della revoca prolungata di cui al p.to 7.2.3.2 seguente.

7.2 Individuazione dei provvedimenti disciplinari

7.2.1 Richiamo

Qualora il Comitato di Garanzia accerti, al termine del procedimento di cui al p.to 7.1, la violazione di uno o più degli obblighi previsti dall'art.3, invierà all'Aderente una comunicazione di richiamo, invitandolo ad ottemperare entro 15 giorni agli impegni sottoscritti con l'adesione al Codice.

7.2.2 Censura

Nel caso in cui l'Aderente non provveda, nei termini previsti, ad adeguarsi alle indicazioni contenute nella comunicazione di richiamo ovvero nel caso in cui la violazione sia di particolare gravità per quantità o rilevanza degli inadempimenti al Codice, il Comitato invia all'interessato una comunicazione di censura invitandolo ad ottemperare entro 15 giorni a quanto previsto nel provvedimento adottato.

7.2.3 Revoca dell'autorizzazione all'uso del marchio "Internet e Minori"

7.2.3.1 Revoca temporanea

Nel caso in cui l'Aderente non provveda, nei termini previsti, ad adeguarsi alle indicazioni contenute nella comunicazione di censura, il Comitato revocherà l'autorizzazione all'uso del marchio "Internet e Minori". L'uso del marchio sarà nuovamente autorizzato dal Comitato una volta accertato, su richiesta dell'Aderente, l'adeguamento dei suoi comportamenti agli impegni assunti.

7.2.3.2 Revoca prolungata

Nel caso in cui, dopo un primo provvedimento di revoca temporanea, intervengano le condizioni per un secondo provvedimento di revoca, l'Aderente non potrà avanzare richiesta di riammissione all'uso del marchio "Internet e minori" prima di un anno.

7.2.4 Pubblicazione dei provvedimenti di revoca

L'Aderente al quale sia stato revocato l'uso del marchio "Internet e Minori" non potrà più utilizzare il marchio medesimo fino a che non sia stato nuovamente autorizzato o riammesso all'uso.

Tutti i provvedimenti di revoca saranno raccolti ed oggetto di pubblicazione secondo quanto previsto al p.to 7.1.5.

Firmato:

AIIP - *Associazione Italiana Internet Providers*
ANFoV - *Associazione per la convergenza nei servizi di comunicazione*
Assoprovider - *Associazione Provider Indipendenti*
Federcomin - *Federazione delle imprese delle Comunicazioni e dell'informatica*
Il Ministro delle Comunicazioni
Il Ministro per l'Innovazione e le Tecnologie

2.7. Internet e deontologia professionale

Codice deontologico forense

(Testo approvato dal Consiglio Nazionale Forense il 17 aprile 1997, più volte modificato)

Art.17 - Informazioni sull'attività professionale

1. L'avvocato può dare informazioni sulla propria attività professionale.

2. Il contenuto e la forma dell'informazione devono essere coerenti con la finalità della tutela dell'affidamento della collettività e rispondere a criteri di trasparenza e veridicità, il rispetto dei quali è verificato dal competente Consiglio dell'Ordine.

3. Quanto al contenuto, l'informazione deve essere conforme a verità e correttezza e non può avere ad oggetto notizie riservate o coperte dal segreto professionale.

4. L'avvocato non può rivelare al pubblico il nome dei propri clienti, ancorché questi vi consentano.

5. Quanto alla forma e alle modalità, l'informazione deve rispettare la dignità e il decoro della professione.

6. In ogni caso, l'informazione non deve assumere i connotati della pubblicità ingannevole, elogiativa, comparativa.

[…]

Art.17-*bis* - Modalità dell'informazione

1. L'avvocato che intende dare informazione sulla propria attività professionale deve indicare:

- la denominazione dello studio, con l'indicazione dei nominativi dei professionisti che lo compongono qualora l'esercizio della professione sia svolto in forma associata o societaria;
- il Consiglio dell'Ordine presso il quale è iscritto ciascuno dei componenti lo studio;
- la sede principale di esercizio, le eventuali sedi secondarie ed i recapiti, con l'indicazione di indirizzo, numeri telefonici, fax, *email* e del sito *web*, se attivato.
- il titolo professionale che consente all'avvocato straniero l'esercizio in Italia, o che consenta all'avvocato italiano l'esercizio all'estero, della professione di avvocato in conformità delle direttive comunitarie.

2. Può indicare:

- i titoli accademici;
- i diplomi di specializzazione conseguiti presso gli istituti universitari;
- l'abilitazione a esercitare avanti alle giurisdizioni superiori;
- i settori di esercizio dell'attività professionale e, nell'ambito di questi, eventuali materie di attività prevalente;
- le lingue conosciute;
- il logo dello studio;
- gli estremi della polizza assicurativa per la responsabilità professionale;
- l'eventuale certificazione di qualità dello studio; l'avvocato che intenda fare menzione di una certificazione di qualità deve depositare presso il Consiglio dell'Ordine il giustificativo della certificazione in corso di validità e l'indicazione completa del certificatore e del campo di applicazione della certificazione ufficialmente riconosciuta dallo Stato;

3. L'avvocato può utilizzare esclusivamente i siti *web* con domini propri e direttamente riconducibili a sé, allo studio legale associato o alla società di avvocati alla quale partecipa, previa comunicazione tempestiva al Consiglio dell'Ordine di appartenenza della forma e del contenuto in cui e espresso.

4. Il professionista è responsabile del contenuto del sito e in esso deve indicare i dati previsti dal primo comma.

5. Il sito non può contenere riferimenti commerciali e/o pubblicitari mediante l'indicazione diretta o tramite *banner* o *pop-up* di alcun tipo.

3. RUOLO E RESPONSABILITA' DEL *PROVIDER*

3.1. Pedopornografia e responsabilità del *provider*

Tribunale Milano, sez.V penale, 18 marzo 2004, n.1993

[…]

Sentenza

nel procedimento nei confronti di B.G. […] imputato del delitto di cui all'art.600-*ter*, comma 3, c.p. per aver distribuito, divulgato e pubblicizzato a mezzo del sito *web* http://www.**********.com, 5 filmati pedo-pornografici e 14 immagini pedo-pornografiche.

[…]

Svolgimento del processo e motivi della decisione

Con decreto che dispone il giudizio emesso in data 7 maggio 2003 B.G. veniva chiamato a rispondere del reato specificato in epigrafe per aver distribuito attraverso il suo sito *web* http://www.**********.com dei filmati ed immagini pedo-pornografici.

[…]

Appare interessante, prima di procedere ad analizzare le risultanze processuali, esaminare i termini in cui si è espresso l'orientamento dottrinale che ha affrontato i problemi circa il fondamento ed i limiti della responsabilità penale del *service provider* […] analizzandola sia sotto il profilo della responsabilità omissiva (o per omesso impedimento dei reati realizzati dagli autori dei contenuti illeciti diffusi via Internet) sia sotto quello della responsabilità commissiva (a titolo di concorso nei reati dei predetti autori da parte del sito ospitante o che ha permesso il *link*).

Innanzitutto si osserva che con la legge 3 agosto 1998, n.269, che raccoglie le norme contro lo sfruttamento della prostituzione, della pornografia e del turismo sessuale in danno dei minori, è stato introdotto nel codice penale l'art.600-*ter* che punisce l'attività di chi distribuisce o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie finalizzate all'adescamento ed allo sfruttamento sessuale di minori degli anni 18. La varietà delle condotte tipiche elencate dalla norma e la loro elencazione risulta in effetti porre delle incertezze rispetto ad una serie di categorie di soggetti operanti in Internet che pur non essendo gli autori materiali dell'immissione in rete dei dati illeciti (cd. *content providers* o produttori di contenuti) risultano però distribuirli, pubblicizzarli e divulgarli materialmente. Ci si chiede infatti se detti soggetti, ed in particolare i proprietari delle infrastrutture di telecomunicazione (che […] sono i cd. *network providers*), i fornitori di accessi (cd. *access providers* i quali offrono l'accesso in rete ovvero la possibilità per il *content provider* di pubblicare su Internet le pagine del proprio sito mediante l'utilizzo di spazio *web* offerto sul proprio *server*) ed i fornitori di servizi (cd. *service providers* i quali si rivolgono all'utente finale consentendogli il collegamento ad Internet ed i suoi ulteriori servizi come ad esempio i *news server*), possano a loro volta ritenersi corresponsabili della distribuzione, divulgazione, pubblicizzazione e cessione a terzi del materiale pedo-pornografico. Se infatti non vi è dubbio sulla loro responsabilità in tutte le ipotesi in cui vi sia una violazione diretta da parte degli stessi di una norma, diverso è il caso in cui vengano sostanzialmente chiamati a rispondere del fatto illecito altrui (del *content provider* che abbia agito attraverso le loro infrastrutture). Peraltro, per inciso, si deve anche osservare come in concreto la riconducibilità diretta alla figura di uno di questi *access* o *services providers* dell'attività di divulgazione in rete di contenuti illeciti si limiti ad ipotesi marginali (per esempio quando questi abbia agito come moderatore di un *newsgroup* e/o laddove abbia provveduto ad un controllo dei messaggi pervenuti sul suo spazio *web* attraverso i siti ospitati o richiamati ed abbia influito - proprio in funzione di tale analisi - nell'organizzarne la fruibilità per gli utenti attraverso il suo servizio per esempio con l'applicazione di un *banner* od altro). Nei casi invece di responsabilità indiretta la loro attività è del tutto autonoma rispetto a quell'illecita del *content provider* pur essendo causalmente la *condicio sine qua non* del realizzarsi della seconda.

Ora, per sostenere la responsabilità a titolo di omissione del *service* o *host provider* occorre affermare a loro carico un obbligo giuridico di impedimento (in questo caso non già dell'evento ma della stessa condotta illecita del *content provider*) e quindi da un lato una sua posizione di garanzia e dall'altro lato una possibilità effettiva di controllo preventivo sul contenuto dei messaggi. Sotto il primo profilo, e quindi per quanto riguarda detta posizione di garanzia, si deve osservare che questa non è ravvisabile, a parere dei menzionati autori ed anche secondo questo Tribunale, nel

diritto vigente e ciò stante l'assenza di una previsione specifica in tal senso e la non applicabilità in via analogica - *in malam partem* - degli artt.57 e 57-*bis* c.p. (riguardanti il direttore della stampa periodica ed anche l'editore e stampatore nel caso di anonimità o non imputabilità dell'autore degli scritti illeciti). Né la posizione di garanzia può argomentarsi sostenendo l'esercizio precedente da parte di detto *provider* di un'attività pericolosa in quanto tale non può considerarsi la sua offerta di uno spazio *web* e l'apertura di un *link* con un determinato sito che rappresenta un'azione consentita e del tutto neutra per il diritto penale. Sotto il secondo profilo, poi, si deve notare che non è ravvisabile la possibilità concreta di esercitare un efficace controllo sui messaggi ospitati sul proprio sito visto l'enorme afflusso dei dati che transitano sui *server* e la possibilità costante di immissione di nuove comunicazioni anche attraverso collegamenti alternativi proprio per la struttura aperta di Internet che non rappresenta alcun unitario sistema centralizzato, ma una possibilità di molteplici connessioni fra reti e *computers* diversi. Per tali motivi dunque non appare possibile fondarsi un giudizio di responsabilità del *service* e *host-access provider* sotto il mero profilo omissivo.

D'altra parte si potrebbe sostenere che anche il *service provider* divulga o comunque agevola la divulgazione di dati illeciti. Però laddove l'attività del *provider* sia stata solo quella di offrire uno spazio in rete od offrire un accesso al sito dove è pubblicato il contenuto illecito la sua responsabilità penale non appare configurabile innanzitutto sotto il profilo oggettivo. Infatti non si può sanzionare penalmente un'attività che appaia di per sé neutra e lecita (se non venga diversamente qualificata per la conoscenza dell'illiceità dei contenuti che si sono ospitati od a cui si è dato accesso). Perché si possa configurare un contributo causale all'illecito del *content provider* da parte del *server* occorre che quest'ultimo si sia inserito nella divulgazione del messaggio con un *quid pluris* rispetto alla sua solita attività, con un'interazione con detto sito.

Deve inoltre verificarsi se il dolo dell'*access* e/o *service provider* abbia ad evidenziarsi attraverso le modalità di svolgimento del servizio da lui prestato (e cioè se si riscontri un dolo di partecipazione od un'oggettiva possibilità di impedire la commissione del reato di cui abbia avuto comunque notizia). Non appare invece soddisfacente un'impostazione della responsabilità del *server* con riferimento alla categoria del dolo eventuale ogniqualvolta non vi siano specifici elementi che consentano di ricondurre nella sua sfera di conoscibilità una specifica attività illecita commessa per suo tramite e ciò, come si è già detto, per la struttura aperta di Internet (che rende in astratto possibile immissioni costanti, autonome e non controllabili sugli spazi gestiti dal *server* laddove lo stesso anche per il tipo di servizio gestito non abbia potuto applicare alcuna tutela rispetto a dette immissioni). In assenza di detti elementi si finirebbe per equiparare il dolo eventuale a un dolo *in re ipsa*.

Fatte queste brevi premesse, passando ad esaminare i risultati dell'istruttoria dibattimentale, si osserva che nel caso di specie può escludersi che il sito T******** (www.**********.com) intestato e gestito dal B. abbia svolto il ruolo di *content provider* del materiale illecito (foto di bambini in età anche prepubere intenti in attività sessuali) che era in realtà offerto dal sito E**** C***. Il sito dell'imputato aveva infatti rivestito solo la funzione di *service provider* rispetto al sito ospitato. L'*host provider* dell'E**** C*** era invece Tiscali ([…]). Inoltre al sito E**** C*** poteva accedersi anche indipendentemente dal tramite di T******** ([…]). Il sito T******** forniva solo un sito di classifiche (organizzate a seconda dei loro contenuti in 30 categorie) dei siti più votati ([…]) e fra questi era stato inserito anche l'E**** C***. Per offrire il suo servizio T******** procedeva ad analizzare ([…]) solo l'*home page* dei siti che si iscrivevano secondo una procedura automatizzata al suo servizio così da accertare la corrispondenza del sito neoiscritto alla categoria dallo stesso indicata. Ora, […], la *home page* dell'E**** C*** non conteneva alcuna foto o richiamo a materiale illecito (per accedere al quale doveva infatti entrarsi in dei sottomenu e poi risolvere un piccolo enigma molto facile), né la presenza di questo materiale pedopornografico si poteva automaticamente immaginare e neanche sospettare vuoi per il nome del sito, vuoi per l'esplicita indicazione del nominativo del titolare del sito (l'E**** C*** risulta infatti aver indicato sulla stessa *home page* il suo indirizzo e questo ne ha permesso la pronta individuazione del titolare […]). Nel corso delle indagini inoltre non risulta essere stato verificato che T******** avesse in passato interferito sul contenuto di alcuno dei siti ospitati ed in particolare dell'E**** C*** (che fra l'altro già il 23 agosto 2000, pochi giorni dopo l'avvio delle indagini, risultava non più raggiungibile). Infine nessun collegamento né personale, né economico è stato verificato tra il B. e R.F. o A., rispettivamente titolari del sito e dell'abbonamento via *web* dello stesso.

Alla luce pertanto delle premesse e dell'analisi della concreta situazione in esame si deve escludere la penale responsabilità del B. in quanto non è possibile individuare suoi comportamenti che dimostrino vuoi un apporto causale - una partecipazione specifica - alla divulgazione delle foto pedopornografiche esposte dall'E**** C***, vuoi la sua conoscenza del contenuto illecito del materiale divulgato dal sito ospitato sul suo spazio *web*.

B. deve pertanto essere assolto dal reato ascrittogli per non aver commesso il fatto.

[…]

3.2. *Peer-to-peer*, responsabilità del *provider*, sequestro e inibitoria

Corte di Cassazione, sez.III penale, 23 dicembre 2009, n.49437

[…]

1. Con ordinanza emessa in data 1 agosto 2008 nel procedimento penale nei confronti di S.K.P., L.C., N.F. e di S.G., tutti indagati per il reato di cui all'art.110 c.p. e legge 22 aprile 1941, n.633, art.171-*ter*, comma 2, lett.a-*bis*), il G.I.P. presso il Tribunale di Bergamo, accogliendo la richiesta del P.M., ordinava il sequestro preventivo del sito *web www.thepiratebay.org* disponendo altresì che i fornitori di servizi Internet *(Internet service provider*) e segnatamente i *providers* operanti sul territorio dello Stato italiano inibissero ai rispettivi utenti - anche a mente del d.lgs. 9 aprile 2003, n.70, artt.14 e 15 - l'accesso all'indirizzo suddetto, ai relativi *alias* e nomi di dominio rinvianti al sito medesimo.

Il G.I.P. - dopo aver diffusamente descritto la tecnica informatica (cd. *peer-to-peer* a mezzo di *file torrent*) di messa in circolazione nella rete Internet di opere protette dal diritto d'autore, senza averne diritto - riteneva sussistere il *fumus delicti* ed il *periculum* del reato di cui all'art.110 c.p. e 171-*ter*, comma 2, lett.a-*bis*), citati.

Con ricorso *ex* art.324 c.p.p. e successiva memoria i difensori di S.K. chiedevano l'annullamento del sequestro preventivo, eccependo il difetto di giurisdizione, l'insussistenza del *fumus delicti*, nonché la falsa applicazione dell'art.321 c.p.p. e del d.lgs. 70/2003, artt.14 e 15.2. Con ordinanza del 24 settembre 2008 il Tribunale per il riesame di Bergamo, in accoglimento del ricorso, annullava il sequestro preventivo.

Il Tribunale riteneva la sussistenza del *fumus delicti*, alla luce di quanto evidenziato dalla Guardia di Finanza, che riferiva di un elevatissimo numero di contatti al sito in questione, registrati sul territorio nazionale, che operavano il *downloading* di opere coperte da diritto d'autore senza averne diritto. Risultava quindi in punto di fatto che gli indagati, attraverso il sito *www.thepiratebay.org* e con un'innovativa tecnologia informatica di trasferimento di file (cd. *peer-to-peer* a mezzo di *file torrent*), mettevano a disposizione del pubblico della rete Internet opere dell'ingegno protette; condotta questa riconducibile a quella tipizzata nell'art.171-*ter*, comma 2, lett.a-*bis*), citato.

Il Tribunale inoltre riconosceva sussistere anche il *periculum*, osservando che l'elevatissimo numero di connessioni rilevate induceva a ritenere l'attualità della condotta del delitto ipotizzato.

[…]

Motivi della decisione

1. Il ricorso del Procuratore della Repubblica presso il Tribunale di Bergamo è articolato in due motivi.

Con il primo motivo il ricorrente deduce l'erronea applicazione dell'art.321 c.p.p. nella parte in cui l'adito Tribunale per il riesame ha ritenuto la nullità dell'ordinanza con cui il G.I.P. ha disposto il sequestro preventivo per asserita carenza di conformità tra il suddetto provvedimento ed il paradigma del sequestro preventivo, come disciplinato negli artt.321 ss. c.p.p.. Censura quindi l'ordinanza impugnata nella parte in cui ha annullato il sequestro, qualificandolo come provvedimento atipico, esorbitante dal vigente ordinamento processuale, come tale inammissibile in sede penale.

A tal fine osserva il ricorrente che deve ammettersi che un sito Internet possa costituire oggetto di sequestro. La sua natura di bene immateriale non pregiudica, in linea di principio, l'applicabilità del vincolo non potendo negarsi che ad un sito Internet in generale (ed al sito oggetto del sequestro *de quo* in particolare) possa attribuirsi una sua "fisicità", ovvero una dimensione materiale e concreta.

Inoltre secondo il ricorrente ben poteva il G.I.P. disporre che i fornitori di servizi Internet (*Internet service provider*) e segnatamente i *providers* operanti sul territorio dello Stato italiano inibissero ai rispettivi utenti - anche a mente del d.lgs. 70/2003, artt.14 e 15 - l'accesso all'indirizzo *www.thepiratebay.org*, ai relativi *alias* e nomi di dominio rinvianti al sito medesimo. Ed invero l'attività prescritta con l'ordinanza di sequestro, annullata dal Tribunale per il riesame, non si traduce in una surrettizia ed asseritamente atipica attività inibitoria né nei confronti degli indagati né nei confronti dei fornitori di servizi Internet.

Con il secondo motivo di ricorso il ricorrente denuncia la violazione o erronea applicazione del d.lgs. 9 aprile 2003, n.70, artt.14 e 16. Fermo restando l'esonero da responsabilità per i fornitori di contenuti telematici riconducibili a terzi, sussiste però un obbligo generale di vigilanza del *provider* sui flussi telematici in transito sui propri sistemi. Altresì può ritenersi operante - secondo il ricorrente - un principio di doverosa cooperazione del *provider* con l'Autorità giudiziaria, nell'ambito dei servizi erogati; principio che si traduce nell'obbligo di impedire o porre fine alle violazioni commesse, quando la predetta Autorità lo richieda.

[…]

3. Nel merito il ricorso, i cui due motivi possono essere esaminati congiuntamente in quanto connessi, è fondato nei limiti e con le precisazioni che seguono.

4. Innanzi tutto va affermato che correttamente l'impugnata ordinanza del Tribunale di Bergamo ha ritenuto sussistere, quale presupposto del sequestro preventivo, il *fumus commissi delicti* consistente nel trasferimento, a mezzo della rete Internet, di *files* aventi il contenuto di opere coperte da diritto d'autore in violazione del diritto esclusivo di comunicazione al pubblico di tali opere.

La particolare tecnologia informatica di condivisione di *files* tra utenti della rete Internet (cd. *file-sharing*) e l'utilizzo di protocolli di trasferimento dei *files* direttamente tra utenti (cd. *peer-to-peer*) per la diffusione in rete di opere coperte da diritto d'autore - secondo la ricognizione in punto di fatto operata dai giudici di merito - non escludono la configurabilità del reato; ciò di cui in realtà non dubita l'ordinanza impugnata, che puntualmente dà conto degli elementi di fatto rilevanti nella specie, confermando peraltro la ricostruzione, sempre in punto di fatto, operata dal G.I.P..

Può comunque considerarsi in proposito che - come emerge dalla ricognizione in punto di fatto operata dai giudici di merito - la caratteristica della condivisione di file (*file-sharing*) e dei protocolli di trasferimento dei file, del tipo *peer-to-peer*, è quella di aver decentrato plesso gli utenti (client) - verso i quali, in quanto utenti finali, c'è l'attività di ricezione di file per via telematica (cd. *downloading*) dell'opera coperta da diritto d'autore - anche l'attività di invio di file per via telematica (cd. *uploading*) dell'opera stessa. Quindi la "diffusione" dell'opera coperta da diritto d'autore non avviene dal centro (il sito *web*) verso la periferia (che riceve il *downloading*), ma da utente (che effettua l'*uploading*) ad utenti che lo ricevono; quindi da "pari a pari" (*peer-to-peer*) non essendoci un centro (il sito *web*) che "possiede" l'opera e la trasferisca in periferia agli utenti che accedono al sito. L'opera è invece in periferia, presso gli utenti stessi, e da questi è trasferita - e quindi diffusa - ad altri utenti. Pertanto il reato di diffusione dell'opera, senza averne diritto, mediante la rete Internet è commesso innanzi tutto da chi fa l'*uploading*; reato previsto, rispettivamente, dalla legge 22 aprile 1941, n.633, art.171, comma 1, lett.a-*bis*), se c'è la messa a disposizione dell'opera in rete "a qualsiasi scopo e in qualsiasi forma", ma non a scopo di lucro, ovvero dall'art.171-*ter*, comma 2, lett.a-*bis*), se c'è la comunicazione dell'opera in rete a fine di lucro; reato quest'ultimo che, nella specie, è quello per il quale si procede essendosi ravvisato - da parte dei giudici di merito - il fine di lucro negli introiti delle inserzioni pubblicitarie a pagamento. La condotta attribuita agli imputati è attualmente descritta dalla legge 633/*1*941, art.171-*ter*, comma 2, lett.a-*bis*), introdotto dal d.l. 22 marzo 2004, n.72, art.1, comma 3, convertito, con modificazioni, dalla legge 21 maggio 2004, n.128, e poi ulteriormente modificato dal d.l. 31 gennaio 2005, n.7, art.3, comma 3-*quinquies*, convertito in legge 31 marzo 2005, n.43, che ancora la punibilità a tale titolo mediante il riferimento all'ipotesi che il fatto venga commesso "a fini di lucro" (cfr. Cass., sez.III, 9 gennaio 2007, n.149).

5. Il problema che nella specie si pone è se a questa condotta delittuosa sia estraneo, o meno, il titolare del sito che mette in comunicazione gli utenti i quali commettono l'illecito con l'attività di *uploading*. Se il sito *web* si limitasse a mettere a disposizione il protocollo di comunicazione (quale quello *peer-to-peer*) per consentire la condivisione di *files*, contenenti l'opera coperta da diritto d'autore, ed il loro trasferimento tra utenti, il titolare del sito stesso sarebbe in realtà estraneo al reato.

Però se il titolare del sito non si limita a ciò, ma fa qualcosa di più - ossia indicizza le informazioni che gli vengono dagli utenti, che sono tutti potenziali autori di *uploading*, sicché queste informazioni (i.e. chiavi di accesso agli utenti periferici che posseggono, in tutto o in parte, l'opera), anche se ridotte al minimo, ma pur sempre essenziali perché gli utenti possano orientarsi chiedendo il *downloading* di quell'opera piuttosto che un'altra, sono in tal modo elaborate e rese disponibili nel sito, ad es. a mezzo di un motore di ricerca o con delle liste indicizzate - il sito cessa di essere un mero "corriere" che organizza il trasporto dei dati. C'è un *quid pluris* in quanto viene

resa disponibile all'utenza del sito anche un'indicizzazione costantemente aggiornata che consente di percepire il contenuto dei file suscettibili di trasferimento. A quel punto l'attività di trasporto dei *files* (*file transfert*) non è più agnostica; ma si caratterizza come trasporto di dati contenenti materiale coperto da diritto d'autore. Ed allora è vero che lo scambio dei file avviene da utente ad utente (*peer-to-peer*), ma l'attività del sito *web* (al quale è riferibile il protocollo di trasferimento e l'indicizzazione di dati essenziali) è quella che consente ciò e pertanto c'è un apporto causale a tale condotta che ben può essere inquadrato nella partecipazione imputabile a titolo di concorso di persone *ex* art.110 c.p. […].

Né la circostanza che la condotta di partecipazione sia stata posta in essere all'estero fa venir meno la giurisdizione del giudice nazionale laddove una parte della condotta comune abbia avuto luogo in ****; cfr. Cass., sez.V, 20 ottobre 2008, n.39205, secondo cui, in caso di concorso di persone nel reato, ai fini della sussistenza della giurisdizione penale del giudice italiano e per la punibilità di tutti i concorrenti, è sufficiente che nel territorio dello Stato sia stata posta in essere una qualsiasi attività di partecipazione da parte di uno qualsiasi dei concorrenti […].

In altre parole la tecnologia *peer-to-peer* decentra sì l'*uploading* (la diffusione in rete dell'opera), ma non ha anche l'effetto, per così dire, di decentrare l'illegalità della diffusione dell'opera coperta da diritto d'autore senza averne diritto. Rimane comunque un apporto del centro (ossia del titolare del sito *web*) a ciò che fa la periferia (gli utenti del servizio informatico che, utilizzando quanto reso disponibile nel sito *web*, scaricano l'opera protetta dal diritto d'autore), apporto che, nel nostro ordinamento giuridico, consente l'imputazione a titolo di concorso nel reato previsto dal citato art.171-*ter*, comma 2, lett.a-*bis*).

6. Se poi si considerano in particolare più sofisticate tecnologie di tale trasferimento di *files* - quale quella che frammenta l'opera in modo da coinvolgere più utenti nell'attività di *uploading* (a mezzo dei cd. *files torrent*) - si ha in realtà che, sotto il profilo giuridico appena considerato, non cambia nulla. La diffusione dell'opera coperta da diritto d'autore avviene sempre da utente ad utente tramite un più sofisticato protocollo *peer-to-peer* che, frammentando l'attività di *uploading*, ha l'effetto di velocizzarla e di evitare le "code" di attesa nel caso in cui tale attività sia operata da un unico utente. Questa possibile frammentazione dell'attività di *uploading* comporta che la messa in rete dell'opera è riferibile non più ad un determinato utente, ma ad una pluralità di essi che concorrono tutti diffondendo una parte dell'opera coperta da diritto d'autore. Portando al limite questa frammentazione si può anche ipotizzare che il singolo utente diffonda un frammento dell'opera che, preso in sé, non sia sufficientemente significativo sotto il profilo strettamente giuridico, sì da non potersi considerare di per sé solo coperto da diritto d'autore. Ma, ricomponendo i frammenti secondo le istruzioni di tracciamento che sono nel sito *web*, si ha il trasferimento dell'opera intera (o di parti di essa), la cui diffusione è ascrivibile innanzi tutto ai singoli utenti. Mentre l'attività di indicizzazione e di tracciamento, che è essenziale perché gli utenti possano operare il trasferimento dell'opera (che in tal caso va da una pluralità di utenti autori dell'*uploading* verso una potenziale pluralità di utenti ricettori del *downloading*) è ascrivibile al (gestore del) sito *web* e quindi rimane l'imputabilità a titolo di concorso nel reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato.

Sarebbe possibile predicare l'estraneità del sito *web* - o, più precisamente, del suo titolare - alla diffusione dell'opera solo nel caso estremo in cui la sua attività fosse completamente agnostica, ove ad es. anche l'indicizzazione dei dati essenziali tosse decentrata verso la periferia. In tal caso sì vi sarebbe solo una comunità di utenti (un *social network*) che condividono un protocollo di trasferimento di dati ed i quali tutti indicizzano i dati stessi consentendo la reperibilità delle informazioni essenziali. In questa evenienza il materiale messo in comune e reso disponibile per il trasferimento potrebbe essere il più vario (coperto, o meno, da diritto d'autore) e la responsabilità penale sarebbe solo degli utenti che operano l'*uploading* e prima ancora l'indicizzazione dei dati.

7. Tutto ciò considerato in generale sull'astratta configurabilità del reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato, deve rilevarsi, con riferimento al caso di specie, che nell'ordinanza impugnata è detto che le "chiavi" per accedere agli archivi degli utenti che posseggono l'opera coperta dal diritto d'autore si trovano nel sito *web* denominato *www.thepiratebay.org;* quindi l'attività di indicizzazione e il risultato della stessa (i cd. *files* di tracciamento) sono nel sito. Ciò consente - sotto il profilo del *fumus* - di escludere che dagli atti emerga il decentramento anche dell'attività di indicizzazione, essenziale per la diffusione dell'opera, e di affermare invece la sussistenza di una condotta riferibile al menzionato sito *web* - e più precisamente agli attuali

indagati quali titolari e gestori dello stesso - e rilevante sul piano penale a titolo di concorso nel reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato.

[…]

Quindi in sintesi sussistono - per le ragioni finora esaminate - sia l'astratta configurabilità del reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato, verificabile in sede di legittimità costituendo ciò una questione di diritto e stante il generale disposto dell'art.129 c.p.p., sia anche il *periculum*, non oggetto di censure.

8. Proseguendo oltre nell'esame dei presupposti del sequestro preventivo disposto dal G.I.P., ma annullato dal Tribunale per il riesame, deve considerarsi che la circostanza che l'*hardware* del sito non sia in **** non esclude la giurisdizione del giudice penale nazionale in ragione del disposto dell'art.6 c.p.. Infatti il reato di diffusione in rete dell'opera coperta da diritto d'autore si perfeziona con la messa a disposizione dell'opera in favore dell'utente finale. Se si considerano gli utenti nel territorio dello Stato che accedono, tramite *provider*, al sito *www.thepiratebay.org* e scaricano da altri utenti, non localizzati, opere coperte da diritto d'autore, c'è comunque che la condotta penalmente illecita di messa a disposizione in rete dell'opera stessa si perfeziona nel momento in cui l'utente in **** riceve il *file* o i *files* che contengono l'opera. Quindi, pur essendo globale e sovranazionale l'attività di trasmissione di dati a mezzo della rete Internet, vi è comunque, nella fattispecie, una parte dell'azione penalmente rilevante che avviene nel territorio dello Stato e ciò consente di considerare come commesso nel territorio dello Stato il reato di diffusione non autorizzata di opere coperte da diritto d'autore limitatamente agli utenti in ****.

[…]

9. L'impugnata l'ordinanza del Tribunale di Bergamo ha ritenuto che la misura cautelare adottata dal G.I.P. presso il Tribunale di Bergamo è illegittima in quanto non ha il contenuto tipico del sequestro, ma costituisce, nella sostanza, un'inammissibile inibitoria, al pari di un provvedimento cautelare civile, violando così il principio della tipicità delle misure cautelari che opera nel processo penale, a differenza del processo civile che segnatamente non tipicizza il contenuto dei provvedimenti cautelari d'urgenza. Su questa affermazione si appuntano in particolare le censure del Procuratore della Repubblica ricorrente, che - come rilevato - sono fondate.

10. Deve innanzi tutto considerarsi che il provvedimento del G.I.P. ha un contenuto complesso perché da una parte ha sequestrato il sito *web* in questione ed ha d'altra parte disposto che i *providers* inibiscano l'accesso al sito; questo duplice contenuto della misura cautelare converge verso l'obiettivo di interdire l'attività penalmente rilevante, ossia l'illecita diffusione di opere coperte da diritto d'autore verso utenti in ****. Questo provvedimento è stato annullato dal Tribunale che ha ritenuto che il decreto censurato ha il contenuto di un ordine imposto dall'autorità giudiziaria a soggetti ... estranei al reato" (i *providers* della connessione); quindi si tratterebbe solo di una mera inibitoria *sub specie* di sequestro preventivo.

In realtà così non è perché c'è innanzi tutto il sequestro del sito *web*, come emerge anche e soprattutto dall'ordinanza del G.I.P. dove si legge "La struttura organizzativa, invero, appare organizzata e realizzata interamente all'estero, in quanto gli apparati informatici dei *server* come risulta dalle informazioni di pubblico dominio reperibili in Internet - sono stati materialmente collocati dapprima in ****, quindi in ****".

Il fatto che l'*hardware* sia collocato all'estero, non è però di impedimento all'adottabilità del provvedimento di sequestro preventivo una volta che si ritenga - come si è sopra affermato - la giurisdizione del giudice penale nazionale *ex* art.6 c.p..

11. Va poi ribadito che il sequestro preventivo ha carattere reale nel senso che esso ha ad oggetto l'apprensione di una *res*, pur non necessariamente "materiale" in senso stretto (cfr. Cass., sez.III, 24 ottobre 2007, n.39354, sul sequestro preventivo di un sito *web* recante messaggi ed annunci di contenuto osceno; Cass., sez.III, 10 ottobre 2006, n.33945, sull'ammissibilità del sequestro preventivo di un portale *web* […].

[…]

Nel caso di specie - che vede […] essere oggetto del sequestro un sito *web* che, per le considerazioni sopra svolte, partecipa all'attività di diffusione nella rete Internet di un'opera coperta da diritto d'autore senza averne diritto (cfr. in particolare Cass., sez.III, 10 ottobre 2006, n.33945, cit.) - c'è indubbiamente un risvolto della misura cautelare che può essere riguardato come un'inibitoria a proseguire in tale attività penalmente illecita. Ma si rimane nell'ambito del sequestro

preventivo che investe direttamente la disponibilità del sito *web* e che, solo come conseguenza, ridonda anche in inibizione di attività.

Sicché sussiste, sotto questo profilo, il carattere reale del sequestro preventivo che quindi non viola il principio di tipicità delle misure cautelari penali.

12. L'originario provvedimento del G.I.P., annullato dal Tribunale per il riesame, ha disposto poi che i fornitori di servizi Internet (*Internet service provider*) e segnatamente i *providers* operanti sul territorio dello Stato italiano inibissero ai rispettivi utenti l'accesso all'indirizzo del sito *web* denominato *www.thepiratebay.org*, ai relativi *alias* e nomi di dominio rinvianti al sito medesimo.

Nella specie pertanto al sequestro preventivo del sito *web* si accompagna una vera e propria inibitoria che - questa sì - è priva del carattere reale, ma ciò non inficia la legittimità della misura cautelare nel suo complesso giacché comunque è soddisfatto il principio di tipicità e di legalità.

Occorre infatti considerare in proposito che in questa specifica materia (della circolazione di dati sulla rete informatica Internet) uno speciale potere inibitorio è assegnato all'autorità giudiziaria dal d.lgs. 9 aprile 2003, n.70, artt.14 e 16, di attuazione della direttiva 2000/31/CE relativa ai servizi della società dell'informazione. Tale normativa speciale, nel prevedere in generale la libera circolazione - nei limiti però del rispetto del diritto d'autore: art.4, comma 1, lett.a) - di tali servizi, quali quelli prestati dai *providers* per l'accesso alla rete informatica Internet, contempla anche, come deroga a tale principio, che la libera circolazione di un determinato servizio possa essere limitata con provvedimento dell'autorità giudiziaria per motivi attinenti all'opera di prevenzione, investigazione, individuazione e perseguimento di reati. In particolare l'art.14, comma 3, art.15, comma 3, e art.16, comma 3, prevedono che l'autorità giudiziaria possa esigere, anche in via d'urgenza, che il prestatore del servizio impedisca o ponga fine alle violazioni commesse; disposizioni queste che vanno lette unitamente al successivo art.17; il quale esclude sì un generale obbligo di sorveglianza nel senso che il *provider* non è tenuto a verificare che i dati che trasmette concretino un'attività illecita, segnatamente in violazione del diritto d'autore, ma - congiuntamente all'obbligo di denunciare l'attività illecita, ove il prestatore del servizio ne sia comunque venuto a conoscenza, e di fornire le informazioni dirette all'identificazione dell'autore dell'attività illecita - contempla che l'autorità giudiziaria possa richiedere al prestatore di tali servizi di impedire l'accesso al contenuto illecito (art.17, comma 3).

La lettura congiunta di tali disposizioni consente di affermare che sussiste un potere inibitorio dell'autorità giudiziaria penale avente il contenuto di un ordine ai *providers* dei servizi suddetti di precludere l'accesso alla rete informatica Internet al solo fine di impedire la prosecuzione della perpetrazione del reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato

Tale inibitoria peraltro deve essere rispettosa del principio di "proporzionalità" (d.lgs. 70/2003, art.5, comma 2, lett.b, cit.) della limitazione dell'accesso rispetto all'obiettivo di individuazione e perseguimento di reati, atteso che la circolazione di informazioni sulla rete informatica Internet rappresenta pur sempre una forma di espressione e diffusione del pensiero che ricade nella garanzia costituzionale dell'art.21, comma 1, Cost. (cfr. in proposito Cass., sez.III, 10 marzo 2009, n.10535, che, con riferimento ai *blog* sulla rete Internet, distingue tra libertà di manifestazione del pensiero e libertà di stampa); profilo questo che però nella specie non viene in rilievo perché il ricorso in esame pone solo il quesito dell'astratta configurabilità, o meno, di un'inibitoria di accesso ad un sito *web* mediante la rete informatica Internet, quale provvedimento del giudice penale che acceda ad un sequestro preventivo del sito stesso. Tale inibitoria può essere adottata "anche in via d'urgenza", come espressamente prevedono l'art.14, comma 3, art.15, comma 3, e art.16, comma 3, sicché, coniugando tali disposizioni con l'art.321 c.p.p., è possibile che il giudice penale, nel disporre il sequestro preventivo del sito *web*, che - come già rilevato - costituisce una misura cautelare di carattere reale, possa contestualmente richiedere ai *providers* di escludere l'accesso al sito al limitato fine, nella specie, di precludere l'attività di illecita diffusione di opere coperte da diritto d'autore; così realizzandosi un rafforzamento della cautela che dalla mera sottrazione della disponibilità della cosa, tipica del sequestro preventivo, si amplia fino a comprendere anche una vera e propria inibitoria di attività, rispettosa anch'essa, nella particolare fattispecie in esame, del principio di tipicità e di legalità in quanto riferibile ad espresse e specifiche previsioni normative.

Quindi il quesito di diritto sopra posto trova, nelle citate disposizioni, una risposta affermativa nel senso che, sussistendo gli elementi del reato di cui all'art.171-*ter*, comma 2, lett.a-*bis*), citato, il giudice può disporre il sequestro preventivo del sito *web* il cui gestore concorra nell'attività penalmente illecita di diffusione nella rete Internet di opere coperte da diritto d'autore, senza

averne diritto, richiedendo contestualmente che i *providers* del servizio di connessione Internet escludano l'accesso al sito al limitato fine di precludere l'attività di illecita diffusione di tali opere.

13. Pertanto il ricorso va accolto con conseguente rinvio al Tribunale di Bergamo.

[…]

3.3. Diritto d'autore e responsabilità del *provider*

Tribunale di Roma, sez. specializzata in materia di proprietà industriale ed intellettuale, ord. 22 gennaio 2010

[…]

Nei procedimenti speciali sommari riuniti nn.86220/2009 e 87722/2009 relativi a reclamo avverso provvedimento cautelare vertente tra *YouTube* LLC anche nella sua qualità di incorporante per fusione di *YouTube Inc.* (di seguito *YouTube*) e *Google Inc.* (di seguito *Google*) […], *Google UK Ltd* […], e Reti televisive Italiane s.p.a. (di seguito RTI) […]

Con reclamo regolarmente notificato, depositato in cancelleria in data 31 dicembre 2009, le reclamanti, premesso:

Che con ricorso *ex* artt.156-163 della legge 633/1941 e 669-*bis* c.p.c. RTI aveva lamentato la violazione dei diritti di autore, in particolare di utilizzazione e di sfruttamento economico, ad essa spettanti in esclusiva in tutto il territorio dello Stato, del programma televisivo Grande Fratello trasmesso dalla rete televisiva "Canale 5" concesso in licenza alla Endemol Italia spa e diffuso sul sito *YouTube* e *Google Video*;

Che in particolare la RTI, titolare oltre che dei diritti di sfruttamento economico del programma anche del diritto di uso sul titolo Grande Fratello, sul relativo logo e sul marchio, aveva lamentato che tra il 26 e il 27 ottobre 2009 erano stati rilevati sui predetti siti 174 sequenze di immagini in movimento tratte dalla decima edizione del programma Grande Fratello per un totale di circa nove ore di trasmissione;

Che a seguito della diffusione via Internet del programma la RTI aveva lamentato un danno grave ed irreparabile per il rischio di sviamento di clientela in quanto gli utenti si astenevano dal guardare il programma a pagamento sulle *pay tv* di RTI, essendo disponibile il programma sulle reti Internet delle reclamanti a titolo gratuito;

Che, contrariamente a quanto affermato da RTI, *Google* e *YouTube* erano meri *hosting provider*s che si limitavano ad offrire agli utenti una piattaforma attraverso cui rendere disponibili al pubblico contenuti audio e video senza alcun obbligo di sorveglianza ai sensi dell'art.17, d.lgs. 70/2003;

Che il giudice italiano era carente di giurisdizione in quanto il servizio di *hosting provider* era svolto dalle reclamanti esclusivamente e completamente in territorio straniero, in particolare negli Stati Uniti dove avviene il caricamento da parte di terzi dei contenuti sul *data center* dell'*hosting provider* (in altre parole sui servizi di *YouTube*);

Che *Google UK Ltd* era estranea ai fatti oggetto del ricorso, in particolare per aver cessato dal 28 novembre 2008 di essere assegnataria del nome a dominio *www.youtube.it;*

Che il giudice aveva accolto il ricorso ed emesso ordinanza in data 15-16 dicembre 2009 notificata in data 18 dicembre 2009 con la quale aveva ordinato alle reclamanti l'immediata rimozione dai propri *server* di tutti i contenuti riproducenti sequenze di immagini relative al programma Grande Fratello ed inibito l'ulteriore prosecuzione della violazione dei diritti di utilizzazione e sfruttamento economico del programma;

tutto ciò premesso hanno proposto reclamo avverso l'ordinanza depositata in cancelleria in data 16 dicembre 2009 chiedendone la modifica. Si è costituita la reclamata RTI con memoria di risposta […].

Il reclamo proposto appare infondato e deve essere respinto con conferma dell'ordinanza emessa in fase cautelare.

In ordine al primo motivo di reclamo, relativo alla carenza di giurisdizione del giudice italiano, le società reclamanti lamentano che non potevano essere destinatarie di un provvedimento di inibizione o parziale oscuramento dei propri siti Internet da parte dell'autorità italiana in quanto svolgono il servizio di *hosting provider* esclusivamente e completamente in territorio straniero, in particolare negli Stati Uniti dove avviene il caricamento da parte di terzi dei contenuti sul data center dell'*hosting provider* (in altre parole sui servizi di *YouTube*). Ritiene il Collegio che tale motivo di reclamo sia infondato in quanto del tutto irrilevante appare la questione della sussistenza in Italia di una struttura organizzata facente capo alle società reclamanti. Infatti poiché l'illecito inteso come danno evento ha luogo in Italia nel momento in cui i filmati vengono visionati

dall'utente italiano non appare condivisibile subordinare l'esercizio del potere inibitorio all'esistenza di una struttura in Italia, posto che presupposto dell'ordine di inibitoria non è un'organizzazione più o meno stabile in territorio italiano ma solo l'offerta in Italia ed agli utenti italiani tramite la rete Internet di trasmissioni di cui RTI possiede la titolarità dei diritti in esclusiva (vedi anche sul punto la recente sentenza Cassazione sezioni unite n.21661 del 13 ottobre 2009).

Occorre poi rilevare che la circostanza che *YouTube* e *Google* svolgano attività di Internet *service provider* cioè servizio di "*hosting*", consistente nell'offrire ai propri utenti una piattaforma attraverso la quale conservare e rendere disponibili al pubblico contenuti audio e video e quindi memorizzazione di informazioni fornite da un destinatario del servizio, (circostanza peraltro contestata da RTI la quale afferma che *YouTube* e *Google* svolgono al contrario attività imprenditoriale a fini di lucro e cioè una "articolata attività di impresa finalizzata a fornire una complessa serie di servizi aggiuntivi al fine di offrire agli utenti dei siti Internet un ampio palinsesto di video, fonte di utili milionari per gli spazi pubblicitari correlati ai video") non esclude l'illiceità della condotta lamentata. Infatti, ove si consideri che la trasmissione via Internet del Grande Fratello lede sicuramente i diritti di utilizzazione e sfruttamento economico di RTI, pur senza voler affermare un obbligo di sorveglianza generale del *provider* rispetto al contenuto dei dati trasmessi conformemente al disposto dell'art.17 del d.lgs. 70/2003 direttiva sul commercio elettronico ("il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza"), non appare nemmeno ragionevole sostenere l'assoluta estraneità alla commissione dell'illecito posto che le reclamanti hanno continuato la trasmissione del Grande Fratello nei loro siti Internet, organizzando la gestione dei contenuti video anche a fini pubblicitari, nonostante le ripetute diffide ed azioni giudiziarie iniziate da RTI che rivendicava la paternità e titolarità dell'opera.

Non si tratta quindi di pretendere dal *provider* un'attività preventiva di controllo e di accertamento di ciascun singolo frammento caricato dagli utenti ma di rimuovere materiale illecitamente trasmesso, dopo aver avuto conoscenza dall'avente diritto a mezzo di diffide della sua presenza in rete con conseguente denunciata lesione di diritti esclusivi, e ciò senza dover attendere apposito ordine, come pretenderebbe di fare la reclamata *YouTube*, da parte dell'autorità giudiziaria. Né può farsi carico a RTI che agisce per la tutela dei propri diritti di fornire alle reclamanti i riferimenti necessari all'esatta individuazione dei singoli materiali caricati sulla piattaforma *URLs*, oggetto questo anche di domanda riconvenzionale nell'ambito del procedimento cautelare, e ciò in quanto le modalità di esecuzione dell'ordinanza reclamata sono già oggetto di apposito procedimento per attuazione davanti al giudice che ha emesso l'ordinanza. Del resto la richiesta di un simile provvedimento in questa sede non potrebbe comunque essere accolta, stante la mancanza del presupposto di pericolo imminente e soprattutto irreparabile per la reclamata che lo sollecita in via riconvenzionale al fine di scongiurare un comportamento ostruzionistico il quale, qualora esistente, potrebbe tutt'al più giustificare una mera richiesta risarcitoria.

[…]

P.Q.M.

Rigetta il reclamo proposto, conferma l'ordinanza cautelare impugnata.

[…]

3.4. Mancata informativa e responsabilità del *provider*

Tribunale Milano, sez.IV penale, 12 aprile 2010, n.1972

[…]

2) Il capo B di imputazione: il trattamento dei dati personali del […]

"Il trattamento dei dati personali sensibili senza in consenso dell'interessato, dal quale derivi nocumento per la persona offesa, già punito ai sensi dell'art.35, comma 3, della legge 31 dicembre 1996, n.675, è tutt'ora punibile con la stessa pena ai sensi dell'art.167, comma 2, del d.lgs. 30 giugno 2003, n.196, in quanto tra le due fattispecie sussiste un rapporto di continuità normativa, essendo identici sia l'elemento soggettivo, caratterizzato dal dolo specifico, sia gli elementi oggettivi, in quanto le condotte di "comunicazione" e "diffusione" dei dati sensibili, sono ora ricomprese nella più ampia dizione di "trattamento" dei dati sensibili, ed il nocumento della persona offesa, che si configurava nella previgente fattispecie come circostanza aggravante, rappresenta nella disposizione in vigore una condizione obiettiva di punibilità" (Cass., sez.III, n.28680 del 26 marzo 2004).

La sentenza della Suprema Corte, di cui si è riportata la massima, rappresenta una sintesi completa dei parametri giuridici di riferimento al fine di inquadrare la complessa vicenda qui in esame; elencando, gli elementi essenziali del reato contestato sono i seguenti:

a) L'avvenuto trattamento dei dati sensibili di una persona;

b) Il mancato consenso da parte del soggetto;

c) Il nocumento della persona offesa;

d) Il dolo specifico da parte del soggetto agente.

[…]

Nella vicenda in questione i P.M. di Milano ritengono che gli imputati D., D.L.R. e Fl., nello loro rispettiva qualità di responsabili di *Google Italy* i primi due e di *Google Inc.* il terzo, in relazione alla *policy* per la privacy per l'Europa, abbiano commesso il reato in questione, omettendo il corretto trattamento dei dati personali e sensibili di D.L.F.G., consentendo il caricamento del *file* video incriminato in data 8 settembre 2006 ed il suo mantenimento sul sito *Google video.it*, al fine di trarne un profitto; tale profitto deriverebbe, sempre secondo l'accusa, dal rapporto esistente tra la società *Google Italy* ed il servizio *Google Video* (gestito da *Google Inc*), rapporto commerciale consistente, tramite la gestione e l'operatività del sistema *AdWords*, nel beneficiare degli indotti pubblicitari degli inserzionisti, indotti collegati alla gestione dei dati immessi su *Google Video*, e quindi direttamente dipendenti dalla quantità e qualità dei medesimi.

In parole più semplici, *Google Italy* sarebbe stato il motore pubblicitario ed economico, in Italia, di *Google Inc,* che (a partire dal luglio del 2006, data di localizzazione in Italia del servizio *Google Video*), avrebbe, con una politica aggressiva e spregiudicata nel mercato dei video sul *web*, tentato di accaparrarsi una grossa fetta del mercato italiano dei video amatoriali, consentendone il caricamento e l'utilizzo senza rispettare in modo adeguato le regole relative alla concreta protezione dei dati personali.

Questo comportamento, fatto, come si è detto, per un fine di lucro (e cioè consentire a *Google Italy* l'accaparramento di numerosi ed importanti clienti privati che pagavano per potersi "inserire", attraverso la gestione di parole chiave, nel sito dei video privati) avrebbe causato una voluta "disattenzione" nelle politiche societarie relative alle problematiche del trattamento dei dati personali, al fine di occupare una fetta di mercato consistente a livello quantitativo e di poter quindi scalzare i relativi concorrenti (tra i quali c'era, non bisogna dimenticarlo, anche *YouTube*, allora non ancora di proprietà di *Google Inc.).*

Sempre secondo i P.M., le complessive modalità di esplicazione di tale servizio, incidendo sui dati immessi nel sistema *Google Video*, comporterebbero necessariamente un trattamento degli stessi, e quindi escluderebbero la possibilità di considerare *Google Italy* (o comunque *Google Video*) un "mero intermediario passivo" (*host provider*) che agisce a richiesta del destinatario del servizio, ma un "*content provider*" e cioè un gestore di contenuti, con tutte le relative conseguenze in termini di responsabilità penale per i contenuti immessi.

Le difese degli imputati, naturalmente, contestano le affermazioni e le valutazioni dei P.M. facendo osservare:

- Che il cd. Codice Privacy (d.lgs. 196/2003) non è applicabile a *Google Italy*, in quanto il trattamento dei dati contenuti nel video incriminato non sarebbe avvenuto in Italia, ma, al più negli Stati Uniti, a Denver, luogo ove sono ubicati i *server* di *Google Inc*. che immagazzinano e trattano i dati provenienti dal caricamento dei video in ogni parte del mondo;

- Che *Google Italy*, in quanto esercente mera attività di *marketing* a favore di *Google Inc*., non aveva alcun potere ed alcuna possibilità di trattare i dati di proprietà di *Google Inc.*;

- Che non vi è alcun legame tra il sistema *AdWords* e *Google Video*;

- Che *Google Video* (e quindi a maggior ragione *Google Italy*) è soltanto un intermediario di *hosting* (e quindi un *host provider*) e, anche sulla base della recente normativa sul commercio elettronico (d.lgs. 70/2003), non è assolutamente responsabile del contenuto dei dati sullo stesso immessi;

- Che non vi è quindi nessun "obbligo di controllo" da parte della medesima società sulle informazioni che trasmette o memorizza, né un obbligo generale di ricerca di fatti o circostanze che indichino la presenza di attività illecite sulle informazioni medesime (vedi art.17, d.lgs. 70/2003);

- Che l'unico obbligo di controllo sui dati contenuti nel video incriminato spettava a chi ha caricato il video, che avrebbe dovuto procurarsi il consenso del D.L.;

- Che l'unico obbligo dell'*host provider*, nel caso in questione, nel momento in cui mette a disposizione del privato un servizio *web* quale quello poi concretamente utilizzato, è quello di indicare nelle "condizioni di servizio - termini del contratto" l'esistenza di obblighi a carico dell'utente, quale quelli relativi alla legge sulla privacy, la cui ottemperanza è di esclusiva responsabilità del privato, con assoluta esclusione della responsabilità del *provider*;

- Che, quindi, unica responsabile dell'eventuale illegittimo trattamento dei dati in questione è la persona che ha caricato il video senza procurarsi il consenso del D.L., non incombendo sull'*host provider* alcun obbligo di controllo successivo sui dati medesimi;

- Che, in ogni caso, i dati del D.L. rinvenibili sul video non riguardano il suo stato di salute (essendo egli autistico e non affetto da sindrome di *Down*), e quindi non possono essere considerati come dati sensibili;

- Che non vi è stata alcuna violazione né dell'art.17 che dell'art.13 del Codice Privacy, avendo *Google Video* fornito una completa informativa agli utenti in merito al trattamento dei dati;

- Che, infine, vi è un'assoluta insussistenza del fine di profitto da parte di *Google Italy*, che non trae alcun tipo di guadagno dal servizio *Google Video*, che è gratuito.

[…]

In primo luogo occorre, partendo dal capo di imputazione, verificare se si è in presenza di una violazione di cui all'art.167 del d.lgs. 196/2003, così come contestata agli imputati; "*in secundis*" va accertato se gli imputati medesimi siano da considerare colpevoli della stessa.

Ora, partendo dalla disamina della prima questione citata, deve rilevarsi che:

- Non vi è possibile dubbio sul fatto che il video in questione contenga delle "pesanti" allusioni allo stato di salute del soggetto D.L.: il fatto che tali allusioni siano state fornite in forma tecnicamente imprecisa e non siano pienamente corrispondenti all'effettiva situazione medica dello stesso, a parere di chi scrive, non appare così importante ai fini della responsabilità penale contestata; deve, tra l'altro, ritenersi, che la sola evidenziazione visiva dello stato di minorità del soggetto costituisca condotta colpevole del reato in questione; così come avverrebbe se, per esempio, si mostrasse in un video una particolare preferenza sessuale di un soggetto, pur non dando allo stesso alcuna connotazione negativa o derisoria. In altre parole la definizione verbale è solo uno dei modi in cui può esercitarsi il comportamento colpevole, ma non esaurisce le modalità commissive del reato contestato.

- In questo senso, non vi è nemmeno possibilità di dubbio in ordine al fatto che il video in questione sia, di per sé, un "dato personale e sensibile" riferibile al D.L., e, come tale, possa essere inquadrato nella previsione dell'art.167 del decreto legislativo citato.

- Nemmeno risulta dubitabile il fatto che il D.L. non abbia prestato alcun tipo di consenso in ordine alla divulgazione del video incriminato, men che meno scritto così come prevede la norma (artt.23 e 26, d.lgs. citato): lo dimostra, quantomeno, la denuncia relativa effettuata dalla parte (in questo caso il padre, trattandosi di soggetto minore).

- Che il consenso non gli sia stato nemmeno richiesto, risulta anche questo chiaramente dalla disamina degli atti processuali relativi (denuncia del padre, indagini di PG sul punto).

- Che vi sia stato, senza ombra di dubbio, un evidente nocumento della persona offesa, lo dimostra, se non altro, il risarcimento del danno a lui effettuato da parte degli imputati.

- Che quindi, concludendo su questo punto, si sia in presenza di una palese violazione dell'art.167 del d.lgs. 196/2003, perlomeno da un punto di vista oggettivo, è circostanza non dubitabile in alcun modo.

Occorre, a questo punto, verificare altre due circostanze fondamentali:

- Su chi incombesse l'obbligo previsto dalla norma di richiedere il consenso e comunque di non trattare i dati contenuti nel video senza il consenso medesimo;

- Se vi sia stato, e per chi, un fine di profitto nel comportamento in questione.

Ora, se non può esservi dubbio sul fatto che l'obbligo in questione incombesse certamente sul soggetto che ha girato e poi caricato il video sul sito *web Google Video*, va valutato con attenzione se tale obbligo fosse riferibile anche al soggetto che tale video ha avuto in carico, che tali dati poi ha gestito e diffuso tramite lo strumento di comunicazione che viene comunemente chiamato Internet (e cioè l'*ISP Internet service provider*).

La domanda che, a questo punto, bisogna porsi è molto precisa: esiste un obbligo per il proprietario o gestore del sito *web* (*provider*, *host provider*, *access provider*, *service provider*, *content provider* che sia) di adeguamento e di rispetto ai dettami di una legge della repubblica operativa (come si è visto) fin dal 1996?

E, se tale obbligo esiste, in che misura esso è richiedibile al soggetto/*web*?

Ovvero è un obbligo che impone un controllo preventivo dei dati immessi o che prevede soltanto un comportamento di corretta informazione degli utenti?

Per una risposta precisa a questa domanda occorre fare un passo indietro e verificare quali siano i comportamenti che la legge (anzi il d.lgs.) indica come automaticamente significativi di trattamento dei dati: come si è visto pocanzi, tali comportamenti (indicati all'art.4 d.lgs. citato) sono molteplici e vanno dalla raccolta dei dati alla loro diffusione ed (addirittura) alla cancellazione degli stessi.

Non può esservi quindi dubbio, a parere di chi scrive, che non esiste, in materia, una zona franca (da un punto di vista oggettivo) che consenta ad un qualsiasi soggetto (persona fisica o meno che sia) di ritenersi esente dall'obbligo di legge, nel momento in cui venga, in qualsiasi modo, in possesso di dati sensibili: trattamento di dati è qualsiasi comportamento che consenta ad un soggetto di "apprendere" un dato e di mantenerne il possesso, fino al momento della sua distruzione.

A maggior ragione non può escludersi (come si è detto da un punto di vista meramente oggettivo) che "tratti" un dato chi "raccolga, elabori, selezioni, utilizzi, diffonda, organizzi" dati che, per la loro natura, siano qualificabili come "sensibili".

In questo senso a poco vale la distinzione che fanno sia i P.M. che le difese fra *host provider* e *content provider*: il proprietario o il gestore di un sito *web* che compia anche solo una di tali attività prima indicate senza possibilità di dubbio si trova nella scomoda posizione di chi "tratti" i dati che gli vengono consegnati e che lui gestisce e, quantomeno, diffonde nell'esteso mondo di Internet.

Senza dubbio il *content provider* (e cioè il "gestore - produttore di contenuti") è in una posizione ancora più delicata, perché, in qualche modo, contribuisce a creare o comunque a far propri dei dati dallo stesso gestiti, ma, come si è detto e qui si ripete, anche l'*host provider* (e cioè il mero intermediario) non è esente da comportamento oggettivamente inquadrabile nella norma, attesa la sua funzione, quantomeno, di diffusore dei dati raccolti.

È evidente che questo comportamento può essere considerato colpevole ai fini della legge citata solo e soltanto se vi sia una coscienza e volontà dello stesso: prima di arrivare alla valutazione del dolo specifico (di cui tra poco si parlerà) deve ritenersi che non possa essere considerato punibile chi raccolga, utilizzi o diffonda dati che egli, in buona fede, debba o possa considerare come "lecitamente raccolti" da altri.

In questo senso l'IP (e cioè l'*Internet provider*) che fornisca agli utenti un semplice servizio di interconnessione e che avvisi correttamente gli stessi degli obblighi di legge concernenti la privacy, non può essere considerato punibile se non controlla preventivamente l'ottemperanza da parte dell'utente all'obbligo di legge citato.

"*Ad impossibilia nemo tenetur*", e cioè non è possibile imporre a qualcuno un obbligo a cui egli non è in grado di fare fronte con i normali mezzi a sua disposizione: sarebbe del tutto impossibile pretendere che un IP possa verificare che in tutti i migliaia di video che vengono caricati ogni momento sul suo sito *web* siano stati rispettati gli obblighi concernenti la privacy di tutti i soggetti negli stessi riprodotti.

È però necessario (ed è quindi legittimo richiedere il rispetto di tale comportamento) che l'IP fornisca agli utenti medesimi tutte le necessarie avvertenze in ordine al rispetto delle norme citate, con particolare attenzione a quelle che concernono la necessità di procurarsi l'obbligatorio consenso in ordine alla diffusione di dati personali sensibili.

Esiste quindi, a parere di chi scrive, un obbligo NON di controllo preventivo dei dati immessi nel sistema, ma di corretta e puntuale informazione, da parte di chi accetti ed apprenda dati provenienti da terzi, ai terzi che questi dati consegnano.

Lo impone non solo la norma di legge (art.13, d.lgs. cit.), ma anche il buon senso, nella particolare modulazione dello stesso che può applicarsi alla gestione di un sistema informatico.

Per la verità, in questo particolare segmento di ricostruzione logica e giuridica del fatto, i P.M. appaiono, nelle loro memorie scritte, molto più *tranchantes* di questo giudice monocratico, ritenendo che la responsabilità derivante dal trattamento dei dati sensibili possa essere addebitata all'*ISP* solo e soltanto ove lo stesso non svolga una mera intermediazione tecnica, ma compia un "qualcosa di più"rispetto all'*host provider*, assicurando mediante un servizio da esse sfruttato, la memorizzazione e la diffusione dei contenuti memorizzati, e diventando in tal modo un *hoster* attivo, responsabile dei contenuti medesimi.

Tale interpretazione viene corroborata con il richiamo al contenuto di un'importante sentenza della Suprema Corte (sez.III penale, n.49437 del 23 dicembre 2009), in materia di responsabilità penale degli *ISP* per quel che attiene il diritto d'autore; sentenza nella quale viene evidenziata una possibile partecipazione dell'*ISP* al reato contestato agli *uploaders* (a titolo di concorso *ex* art.110 c.p.) nel momento in cui il predetto non si limita ad una "messa a disposizione del protocollo di comunicazione" ma compie un *quid pluris* e cioè "indicizza le informazioni che gli vengono dagli utenti... perché gli utenti possano orientarsi.... Chiedendo il *downloading* di quest'opera piuttosto che di un'altra.. e quindi il sito cessa di essere un mero corriere che organizza il trasporto di dati... a quel punto l'attività di trasporto dei *files* non è più agnostica" consentendo una valutazione dell'apporto causale al reato lì contestato.

Sulla base di tale interpretazione dovrebbe quindi ritenersi corresponsabile del reato di cui all'art.167 del d.lgs. citato, quel tipo di *ISP* che (come nel caso in esame) non si limiti a fornire un semplice rapporto di interconnessione, ma, gestendo i dati in suo possesso, ne divenga in qualche modo "*dominus*" e quindi "titolare del trattamento" ai sensi di legge, con gli obblighi corrispondenti.

Deve dirsi che questo tipo di impostazione accusatoria da un lato sembra richiedere un livello di approfondimento probatorio forse troppo elevato (quando un *ISP* può con certezza definirsi un *hoster* attivo? quando può ritenersi esaurita la ricerca di quel *quid pluris* di cui parla la S.C.?), dall'altra esclude dal novero dei potenziali responsabili tutte le numerose platee degli *host providers* che, come si è cercato di dimostrare, non sembrano poter sfuggire alle ricadute concorsuali delle condotte di reato evidenziate.

La normativa che punisce le violazioni del diritto d'autore non sembra, peraltro, di così facile trasportabilità nell'ambito del presente procedimento: l'oggetto della tutela, in quel caso, appare chiaramente ricollegabile alla mera condotta di caricamento del dato, di talché l'eventuale "apprensione" del dato medesimo da parte dell'*ISP* (sotto forma di indicizzazione dello stesso o altro) costituisce di per sé un concorso nel reato preesistente; nel caso in esame, invece, la violazione della legge è, per così dire, più nascosta, o comunque occultata nelle pieghe di un possibile comportamento altrui, e non può essere quindi "trasportata" nelle mani del *provider* solo e soltanto perché il dato viene gestito o organizzato dallo stesso.

In parole più semplici il *provider* che indicizza dei testi coperti dal diritto d'autore che altri caricano e si scambiano, consentendone una commercializzazione più veloce e facile, certamente può essere ritenuto corresponsabile del reato contestato agli *uploaders* (cosi come indicato dalla S.C.); ma un *provider* che carica dei video contenenti dati sensibili di soggetti a cui non è stato richiesto il consenso, e li organizza e gestisce, non può essere ritenuto responsabile della mancata richiesta di consenso (nonostante la gestione dei dati in parola) se non viene provata la sua piena consapevolezza di tale mancanza; consapevolezza che, naturalmente, può e deve derivarsi da una mancanza di segnali o di elementi significativi all'atto della prima comunicazione del caricamento.

A parere di chi scrive, comunque, il fatto che l'*ISP* faccia qualcosa di più del suo dovere di mero intermediatore (e cioè diventi un *hoster* attivo o un *content provider*, come anche può dirsi), è, una volta provato, certamente un elemento importante ai fini della ricostruzione delle ipotesi di reato contestate o contestabili, ma non trasforma, *sic et simpliciter*, l'*ISP* in un immediato

realizzatore dei possibili reati emergenti dai dati caricati: non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli *ISP* un controllo preventivo dell'innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti *web*, e non appare possibile ricavarlo *aliunde* superando d'un balzo il divieto di analogia *in malam partem*, cardine interpretativo della nostra cultura procedimentale penale.

Ma, d'altro canto, non esiste nemmeno la "sconfinata prateria di Internet" dove tutto è permesso e niente può essere vietato, pena la scomunica mondiale del popolo del *web*.

Esistono, invece, leggi che codificano comportamenti e che creano degli obblighi, obblighi che, ove non rispettati, conducono al riconoscimento di una penale responsabilità.

È pertanto ovvio che l'*hoster* attivo o il *content provider* che dir si voglia avrà certamente un livello di obblighi e di comportamenti più elevato di quello di un semplice *host provider* o *service provider* o *access provider*: lo rende inevitabile il suo diventare "*dominus*" di dati che, per il solo fatto di essere organizzati e quindi selezionati e quindi "appresi", non sono più il flusso indistinto che non si conosce e che non si ha l'obbligo di conoscere; ma, tale fatto, non crea una specie di effetto a catena che fa dell'*hoster* attivo automaticamente il corresponsabile di tutti i reati che gli *uploaders* hanno commesso comunicando e caricando i dati in loro possesso.

In tutti questi casi varranno, come in effetti valgono, le normali coordinate interpretative e valutative che si usano per ogni tipo di reato che il legislatore ha inteso codificare nel codice penale o nelle leggi complementari, sia da un punto di vista oggettivo che soggettivo.

E perciò, nel caso in esame, se è ben vero che un *hoster* attivo (come nel caso *Google Italy*) ha sicuramente più elementi per poter riconoscere l'esistenza di un reato commesso da un singolo *uploader*, ed ha, inoltre, sicuramente degli obblighi che la legge gli impone per il trattamento dei dati sensibili dei soggetti che vengono "caricati" sul suo sito *web*, è altrettanto vero che non può essere imposto (perché irrealizzabile) allo stesso un obbligo generale e specifico di controllo su tutti i dati "sensibili" caricati (obbligo impossibile, se non altro, perché si imporrebbe ad un terzo la preventiva conoscenza di tutti i dati personali e particolari di tutte le persone che ogni momento "transitano" sul *web*); quello che, come si è detto, è imponibile allo stesso è un obbligo di corretta informazione agli utenti dei conseguenti obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli (oltre che, naturalmente, l'obbligo di immediata cancellazione di quei dati e di quelle comunicazioni che risultassero correttamente segnalate come criminose).

È peraltro evidente, perlomeno a parere di chi scrive, che NON costituisce condotta sufficiente ai fini che la legge impone, "nascondere" le informazioni sugli obblighi derivanti dal rispetto della legge sulla privacy all'interno di "condizioni generali di servizio" il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente; tale comportamento, improntato ad esigenze di minimalismo contrattuale e di scarsa volontà comunicativa, costituisce una specie di "precostituzione di alibi" da parte del soggetto/*web* e non esclude, quindi, una valutazione negativa della condotta tenuta nei confronti degli utenti.

Da questo punto di vista, tornando alla valutazione del caso concreto, non può dubitarsi dei seguenti elementi conoscitivi e probatori:

- *Google Italy* costituiva la "mano operativa e commerciale" di *Google Inc.* in Italia;

- Attraverso il sistema *AdWords* ed il riconoscimento di parole chiave, *Google Italy* aveva sicuramente la possibilità di collegare, attraverso la creazione di *links* pubblicitari, le informazioni riguardanti i clienti paganti alle schermate riguardanti *Google Video*, e quindi, in qualche modo, gestire, indicizzare, organizzare anche i dati contenuti in quest'ultimo sito;

- *Google Italy*, quindi, "trattava" i dati contenuti nei video caricati sulla piattaforma di *Google Video* e ne era quindi responsabile, perlomeno ai fini del d.lgs. sulla privacy;

- L'informativa sulla privacy, visualizzabile per l'utente dalla pagina iniziale del servizio *Google Video* in sede di attivazione del relativo *account* al fine di porre in essere il caricamento dei *files* da parte dell'utente medesimo, era del tutto carente, o comunque talmente "nascosta" nelle condizioni generali di contratto da risultare assolutamente inefficace per i fini previsti dalla legge.

- Si veda, in questo senso, l'annotazione […]della GdF di Milano del 19 giugno 2008 […], alla quale sono stati allegati i "termini e condizioni di servizio di *Google*", i "termini e condizioni del programma di caricamento di *Google Video*", "i punti salienti delle norme sulla privacy di *Google*" datate 14 ottobre 2005, "le norme sulla privacy di *Google*" datate 14 ottobre 2005", agli indirizzi *web* ricollegati ai servizi in questione: tutte le informazioni comunicate all'utente relative alla

privacy fanno riferimento, senza possibilità di dubbio, alla tutela della privacy dell'utente medesimo, utente che accetta di sottoscrivere il contratto con *Google* e che carica il video (o qualsiasi altro dato o informazione) in suo possesso, senza fare alcun esplicito riferimento alla privacy di altre persone eventualmente presenti nel video o nel contenuto dell'*uploading*; è ben vero che al p.to 9 dei "termini e condizioni del programma di caricamento di *Google Video*" si chiede all'utente di garantire che il contenuto "autorizzato" che sta caricando non violi "diritti o obblighi verso qualsiasi persona, inclusi... i diritti di privacy", ma l'avviso in questione, al di là della sua genericità ed astrattezza, è dato in modo "nascosto ed anonimo", quasi a garantirsi (come si è già detto) la presenza di un alibi in un eventuale momento successivo di contrasto. Ad assoluta riprova di quanto fin qui riferito, nel momento in cui l'utente più attento e testardo di altri avrebbe voluto compulsare "i punti salienti della normativa sulla privacy di *Google*" avrebbe scoperto, al p.to 2 della medesima ("Quali sono i dati personali e gli altri dati che raccogliamo") che "*Google* raccoglie dati personali quando vi registrate per accedere ad un servizio di *Google*…": non vi è chi non veda che chiunque legga questa frase non può che pensare ai "propri" dati personali e non certo a quelli delle persone incautamente citate o riprese nei "contenuti autorizzati".

- Il fine di profitto (richiesto dalla norma specificamente per la sussistenza del dolo) era, evidentemente, ricollegabile all'interazione commerciale ed operativa esistente tra *Google Italy* e *Google Video*, interazione derivante dalla operatività del sistema *AdWords* e dal collegamento esistente tra le *keywords* (parole chiave) utilizzate in quest'ultimo ed il sito *web* ospitante i video (vedi, sul punto, le precise risultanze di indagini effettuate dai P.M. e riportate nella parte iniziale della presente motivazione).

- Si vedano inoltre, ad ulteriore riprova di quanto fin qui riferito, le affermazioni di *Google* contenute nel p.to 17 dei "termini di servizio e condizioni di contratto": "alcuni dei servizi sono finanziati dalle pubblicità e possono visualizzare pubblicità e promozioni. Queste pubblicità possono avere come oggetto il contenuto di informazioni memorizzate nei servizi..."nonché il p.to 3 dei "termini e condizioni del programma di caricamento di *Google Video*": "*Google* può rendere disponibile...uno o più *links* al sito *web* specificato dall'utente ... in relazione a qualsiasi messa a disposizione dei contenuti autorizzati, e rendere disponibili i *links* ai siti *web* di rivenditori commerciali di terzi in cui, eventualmente, è possibile acquistare i contenuti autorizzati".

- L'esistenza di tutti questi "indici rivelatori" di tipo fattuale e documentale dimostra, a parere di chi scrive, una chiara accettazione consapevole del rischio concreto di inserimento e divulgazione di dati, anche e soprattutto sensibili, che avrebbero dovuto essere oggetto di particolare tutela; non solo, ma anche dell'interesse economico ricollegabile a tale accettazione del rischio e della chiara consapevolezza di quest'ultimo.

In parole semplici: non è la scritta sul muro che costituisce reato per il proprietario del muro, ma il suo sfruttamento commerciale può esserlo, in determinati casi ed in presenza di determinate circostanze.

Per queste ragioni non può esservi dubbio in ordine al riconoscimento della responsabilità penale degli imputati in relazione al reato contestato *sub* B (illecito trattamento di dati personali e sensibili): le risultanze probatorie ottenute ed utilizzabili permettono la ricostruzione del fatto/reato così come contestato dai P.M. nel decreto di citazione diretta e ne impongono la conseguente valutazione di responsabilità penale in termini di colpevolezza.

[…]

3) Il capo di imputazione *sub* A: il concorso nel reato di diffamazione

Quanto fin qui esposto in termini di responsabilità penale dell'*IP* (*Internet provider*) e di possibile prospettabilità della stessa in termini generali ed astratti secondo le normali regole del diritto penale vigente, può essere dato per accertato.

Il ragionamento fin qui riportato deve, ovviamente, essere calato nell'ambito del capo di imputazione riportato *sub* A, e cioè il concorso omissivo (*ex* art.40, cpv., c.p.) degli imputati nel reato di diffamazione commesso ai danni del D.L. e dell'Associazione *Vivi Down*; reato commesso ai sensi degli artt.595, commi 1 e 3 (con ogni altro mezzo di pubblicità), c.p. "*in primis*" dalle persone apparse nel video in questione in qualità di primi autori dell'atto di bullismo mediatico ai danni del D.L. medesimo e dell'associazione citata.

Il discorso che deve qui affrontarsi non può che partire dalla disamina del video contestato in quanto, a seguito della remissione di querela dei D.L. e quindi alla sentenza di improcedibilità emessa, i difensori degli imputati hanno evidenziato una carenza di offensività dei comportamenti

dei soggetti agenti nei confronti della parte lesa residua (e cioè l'Associazione *Vivi Down*), la cui reputazione non sarebbe stata offesa dalle parole pronunciate e dalle condotte tenute.

Le difese motivano tale affermazione sostanzialmente facendo rilevare che le parole pronunciate dal ragazzo, che appare nel video come "persecutore" della parte offesa D.L., sono evidentemente dette "*ioci causa*" da persona che non faceva parte dell'associazione e che, quindi, nessuna lesione effettiva della reputazione di quest'ultima è deducibile dai comportamenti in questione.

È bene ricordare che il contesto complessivo in cui si svolgono le azioni riportate nel video è quello di un'aula scolastica, e che il ragazzo citato dice, nel corso dello stesso, le seguenti parole: "Salve, siamo dell'associazione *Vivi Down*; un nostro mongolo si è cagato addosso, e mò non sappiamo che minchia fare, perché l'odore di merda ci è entrato nelle narici" accompagnando tali espressioni con numerosi ed odiosi atti di vessazione nei confronti della parte lesa.

Deve preliminarmente rilevarsi che è proprio la serie di comportamenti complessivi che vengono effettuati ai danni del ragazzo disabile (e non solo le parole citate) che evidenziano un atteggiamento dei responsabili del fatto che non può essere ridotto ad un "gioco", per quanto "cattivo" esso possa essere ritenuto […].

Di gioco si sarebbe trattato (anche se gioco pesante) se le parole fossero rimaste tali e non fossero state accompagnate da gesti inequivocabili e da comportamenti assolutamente vessatori e violenti nei confronti della parte lesa, il quale rimane numerosi (ed interminabili) minuti in balia dei suoi persecutori che lo deridono, lo spingono in un angolo, gli gettano addosso carte ed epiteti assolutamente gravissimi.

In breve, non sembra a questo giudicante di essere in presenza di un "gioco tra ragazzi", ma di qualcosa d'altro, di una serie di atti di persecuzione di una persona solo perché "diversa", atti nella sequenza dei quali le parole diffamatorie sono solo una piccola parte della violenza complessiva.

In questo senso anche la citazione dell'associazione *Vivi Down* come "responsabile" del fatto in questione appare tutt'altro che priva di elementi diffamatori, costituendo un'evidente denigrazione di tutto l'universo *Down*, comprensivo anche di quella parte di quel mondo che dovrebbe occuparsi della tutela dello stesso.

Non esiste, quindi, dubbio, a parere di questo giudicante, della portata e valenza diffamatoria del fatto (nel suo complesso) a danno della parte lesa *Vivi Down*.

Detto questo, ed esclusa la questione difensiva per improcedibilità per difetto di querela a cui questo giudice ha già esaurientemente risposto nella prima ordinanza di questo procedimento (a cui si fa integrale riferimento), si può passare a trattare il tema centrale della prospettazione accusatoria.

L'ufficio dell'accusa, infatti, ha costruito (con innegabile perizia) un capo di imputazione strutturato in modo tale da consentire una possibilità di concorso nel reato di cui all'art.595 c.p. (commesso, come si è detto, *in primis*, dai ragazzi apparsi nel video) anche ai responsabili del sito *web* (*Google Video.it*) dove il video è stato poi caricato (*uploading* dell'8 settembre 2006), facendo derivare un obbligo giuridico di controllo dei contenuti del video in questione dall'omissione del corretto trattamento dei dati personali della parte lesa D.L., omissione già affrontata nella disamina del capo B di imputazione.

Per la verità i P.M., nel corso della loro requisitoria e nelle memorie finali presentate, dicono anche qualcosa di più rispetto alla formulazione del capo di imputazione: che cioè i responsabili di *Google* indicati come imputati, essendo *Google Video*, a cui *Google.it* aveva accesso tramite il sistema AdW*ords*, una piattaforma *web* qualificabile come *hoster* attivo o come *content provider*, avevano un obbligo preventivo di controllo sul contenuto dei video caricati e "fatti propri", e che non avrebbero attivato tutti i possibili "filtri" che la tecnologia prevede in casi del genere per controllare i video, limitandosi ad un sistema di controllo successivo degli stessi solo in seguito alla segnalazione degli utenti (*flag in*).

Da un lato, quindi, i P.M. ritengono l'esistenza di una posizione di garanzia a carico del sito *web* in parola, posizione derivante da un obbligo giuridico contenuto nella legge sulla privacy; dall'altro si spingono a costruire tale posizione come causativa di un obbligo "preventivo" di controllo sui video caricati sul sito, di talché l'aver lasciato sul sito *Google Video* il video in questione per un periodo di quasi due mesi (8 settembre - 7 novembre 2006) senza rimuoverlo costituirebbe un'evidente compartecipazione omissiva nel reato di diffamazione.

Le difese degli imputati hanno rigettato con forza tale costruzione affermando l'inesistenza di tale obbligo giuridico di controllo preventivo e rilevando come l'attività dei responsabili di *Google Video* nella vicenda in esame sia da considerarsi priva di qualsiasi profilo di responsabilità penale, avendo gli stessi rimosso il video incriminato nell'arco di 24 ore dalla prima segnalazione pervenuta.

Prima di affrontare la disamina della questione "in diritto" qui evidenziata, occorre, molto brevemente, raccontare quello che è successo "in fatto" nella vicenda in questione:

- Il video viene girato nella classe di un Istituto Tecnico di Torino in data 24 maggio 2006;
- Tra l'8 ed il 10 settembre 2006 il video viene caricato su *Google Video* (da tale Gi.Li., che non risulta imputata nel presente procedimento);
- Il video, nel corso dei due mesi successivi, viene visualizzato dagli utenti del sito 5500 volte, prendendo il 1° posto tra i video più divertenti ed il 29° tra i video più scaricati;
- In data 5 novembre 2006 il "*blogger*" D.A.A. segnala sul suo *blog* (giornalettismo: il cannocchiale.it) la presenza del video sul sito (non è chiaro se egli abbia anche inviato una segnalazione a *Google Video* sull'inopportunità della presenza del video, come afferma, o comunque se la sua segnalazione sia stata correttamente recepita);
- In data 6 novembre tale Si.Ba. richiede la rimozione del video tramite il Centro di assistenza *Google*;
- In data 7 novembre la Polizia Postale di Roma richiede la rimozione del video;
- In data 7 novembre 2006 il video viene rimosso.

Sulla base di tali evidenze fattuali e di quanto poi ricostruito dai P.M. nel corso delle indagini preliminari, può affermarsi quanto segue:

- Dal momento della sua immissione nel circuito comunicazionale di Internet il video è stato messo a disposizione di un numero indeterminato di utenti (quantomeno 5500, così come risulta dal numero degli accessi al sito, ma tale valutazione deve ritenersi minimale attesa la possibilità di ulteriore comunicazione a terzi del video preventivamente scaricato - effetto virologico della comunicazione sul sito -);
- Secondo la costante giurisprudenza della Suprema Corte essendo la diffamazione un reato di evento, esso si consuma "nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa e dunque, nel caso in cui frasi o immagini lesive siano state immesse sul *web*, nel momento in cui il collegamento viene attivato" (Cass., sez. V, n.25875 del 21 giugno 2006).
- Per impedire la commissione del fatto (e, in particolare per evitare che la condotta lesiva sfoci nell'evento del reato) il soggetto/*web* proprietario o gestore del sito avrebbe dovuto "impedire l'evento" e cioè controllare preventivamente il contenuto della comunicazione, non ammettendone il caricamento a motivo della presenza, all'interno dello stesso di frasi ed espressioni ingiuriose e diffamatorie.
- Tale fatto (e cioè il controllo preventivo del video) non è avvenuto, tanto è vero che il video è stato presente sul sito *web* per quasi due mesi.
- Il video è stato rimosso soltanto all'esito di una doppia segnalazione (privato, Polizia postale), in un tempo ragionevolmente rapido dal ricevimento delle stesse (24 ore circa).

Secondo i P.M., come si è detto, la responsabilità degli imputati deriverebbe dal mancato controllo (preventivo) sul contenuto del video, agli stessi addebitabile in virtù della posizione di garanzia rivestita dal "*content provider*" nei confronti del trattamento dei dati personali dei soggetti contenuti negli *uploading* degli utenti: dicono cioè i P.M. che l'omesso controllo del corretto trattamento dei dati personali contenuti nel video, avrebbe causato l'evento del reato contestato, che altrimenti non sarebbe avvenuto (o sarebbe avvenuto con minor danno da diffusione per la persona offesa).

Ricavano tale convincimento dal fatto che, essendo il "*content provider*" un produttore o gestore di contenuti, l'illiceità del contenuto si propagherebbe al gestore medesimo in virtù del ricordato principio collegato alla posizione di garanzia (principio riaffermato, a loro dire, dalla sentenza della Suprema Corte in tema di diritti d'autore già ricordata).

L'assunto dell'accusa non può essere condiviso.

Come si è già affermato nel corso di questa motivazione: "non esiste, a parere di chi scrive, perlomeno fino ad oggi, un obbligo di legge codificato che imponga agli *ISP* un controllo preventivo dell'innumerevole serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti *web*, e non appare possibile ricavarlo *aliunde* superando d'un balzo il divieto di analogia *in malam partem*, cardine interpretativo della nostra cultura procedimentale penale."

La presenza di una "posizione di garanzia" da cui derivi un obbligo di attivazione in mancanza del quale ricorre la previsione del cpv. dell'art.40 c.p., non può essere frutto di una seppur ingegnosa costruzione giurisprudenziale, ma, come insegna la Suprema Corte, deve derivare da "da un lato, da una fonte normativa di diritto privato o pubblico, anche non scritta, o da una situazione di fatto per precedente condotta illegittima, che costituisca il dovere di intervento, dall'altro lato, dall'esistenza di un potere giuridico, ma anche di fatto, attraverso il corretto uso del quale il soggetto garante sia in grado, attivandosi, di impedire l'evento" (Cass., sez.IV, n.32298 del 6 luglio 2006).

Non appare quindi conforme a tali prescrizioni (ma anche alla possibilità logica ed umana di intervento sulla rete) far derivare l'esistenza di tale obbligo di intervento dalla violazione di una legge che non abbia per oggetto tali condotte e che sia stata emanata a copertura di comportamenti diversi da quello contestato.

In altre parole, pur non essendovi dubbio che il gestore o proprietario del sito *web* qualificabile come "*content provider*" possa e debba essere ritenuto potenzialmente responsabile della violazione del d.lgs. sulla privacy (per le ragioni che si sono esposte precedentemente e che trovano un appiglio diretto all'esistenza di una norma specifica), non appare conforme alle situazioni di fatto e di diritto finora esistenti, renderlo per ciò solo corresponsabile di altro reato di diffamazione (ma non solo) derivabile dal contenuto del materiale caricato.

Non lo consente sia l'attuale formulazione legislativa sul punto (che non prevede l'esistenza di una norma di controllo generale sugli *ISP*) sia la logica fattuale da applicarsi al caso concreto.

Ed infatti, pur ammettendo per ipotesi che esista un potere giuridico derivante dalla normativa sulla privacy che costituisca l'obbligo giuridico fondante la posizione di garanzia, non vi è chi non veda che tale potere, anche se correttamente utilizzato, certamente non avrebbe potuto "impedire l'evento" diffamatorio.

In altre parole anche se l'informativa sulla privacy fosse stata data in modo chiaro e comprensibile all'utente, non può certamente escludersi che l'utente medesimo non avrebbe caricato il *file* video incriminato, commettendo il reato di diffamazione.

In realtà i P.M., nel costruire la loro (come si è detto, ingegnosa) ipotesi accusatoria, hanno, in un certo senso, detto meno di quello che in effetti hanno pensato: perché la costruzione di una posizione di garanzia impone al soggetto nei cui confronti viene affidata, un obbligo "preventivo" di impedire l'evento e non un generico obbligo di farne cessare gli effetti già avvenuti.

Per cui, nell'ipotesi in esame, l'obbligo del soggetto/*web* di impedire l'evento diffamatorio, imporrebbe allo stesso un controllo o un filtro preventivo su tutti i dati immessi ogni secondo sulla rete, causandone l'immediata impossibilità di funzionamento.

Considerata l'estrema difficoltà tecnica di tale soluzione e le conseguenze che ne potrebbero derivare, si è quindi in presenza di un comportamento "inesigibile", e quindi non perseguibile penalmente ai sensi dell'art.40, cpv. c.p..

In breve, la "torsione" esegetica che i P.M. fanno nella lettura ed applicazione dell'art.167 del d.lgs. 196/2003, non può essere accolta o considerata applicabile nella vicenda in questione.

La responsabilità penale degli *ISP*, mancando una precisa legislazione in materia che li equipari alle produzioni stampate o alle reti televisive, non può essere costruita al di là dei canoni interpretativi ed applicativi dell'attuale quadro normativo (quadro a cui si è recentemente aggiunta la Legge sul commercio elettronico – d.lgs. 70/2003- che, tuttavia appare applicabile soltanto agli *host provider* e nei limiti oggettivi identificati dalla stessa).

Sarà possibile considerarli responsabili dei contenuti dei *files* sugli stessi caricati (soprattutto nel caso si tratti di *hoster* attivi o *content provider*) solo nel momento in cui si provi la consapevolezza del fatto delittuoso, al di là dell'esistenza di posizioni di garanzia non mutuabili da altri settori dell'ordinamento.

Per esempio, nel caso in questione, l'ufficio dell'accusa vi è andato molto vicino (si ripete, al di là dell'esistenza della posizione di garanzia): il fatto, indubitabile, che il video sia stato presente sul sito *web* per due mesi e che lo stesso sia stato inserito nei video più divertenti e più "cliccati" dagli utenti (sic!) già costituisce un principio di prova della "consapevolezza" da parte dei gestori del suo contenuto; principio che non ha raggiunto la pienezza della prova solo per l'estrema difficoltà dell'effettuazione delle indagini (e della ricostruzione del dolo del soggetto agente) in vicende di questo tipo, ma che segnala (a chi ha voglia di stare ad ascoltare) che aprire le cataratte della libertà assoluta e senza controllo non costituisce un buon esercizio del principio di

responsabilità e di correttezza, che sempre dovrebbe presiedere alle attività umane (anche se esercitate nel mondo "parallelo" di Internet).

Perciò, in attesa di una buona legge che costruisca un'ipotesi di responsabilità penale per il mondo dei siti *Web* (magari colposa, ed allora sì per omesso controllo), non resta che assolvere gli imputati dal reato di cui al capo A, reato che, così come formulato, non sussiste.

[…]

5) Considerazioni finali

La grande (ed inaspettata) ricaduta mediatica di questo procedimento e della sua sentenza finale di primo grado, impone a questo giudicante una breve chiosa conclusiva:

- Verrebbe da dire, parafrasando il titolo di una famosa commedia di Shakespeare, "*too much ado about nothing* (molto rumore per nulla)"; e cioè non sembra, a questo giudice, di aver alterato in modo sensibile i parametri valutativi e giurisdizionali che presiedono alla decisione di casi quali quello trattato (si vedano, in particolare, come riferimento le motivazioni delle sentenze del Tribunale penale di Milano del 28 marzo 2004 e del Tribunale civile di Lucca del 20 agosto 2007).

- La condanna del *webmaster* in ordine al reato di illecito trattamento dei dati personali, infatti, non viene qui costruita sulla base di un obbligo preventivo di controllo sui dati immessi, ma sulla base di un profilo valutativo differente che è, come detto, quello di un insufficiente (e colpevole) comunicazione degli obblighi di legge nei confronti degli *uploaders*, per fini di profitto.

- Il d.lgs. sulla privacy (legge attualmente vigente in Italia) "copre" in modo legislativamente completo i comportamenti di chi si trovi nella situazione di "maneggiare" dati sensibili, e quindi non può essere trascurato nel momento in cui se ne appalesi la possibilità di intervento.

- La distinzione tra *content provider* e *service provider* è sicuramente significativa ma, allo stato ed in carenza di una normativa specifica in materia, non può costituire l'unico parametro di riferimento ai fini della costruzione di una responsabilità penale degli *Internet providers*.

- Tuttavia questo procedimento penale costituisce, a parere di chi scrive, un importante segnale di avvicinamento ad una zona di pericolo per quel che concerne la responsabilità penale dei *webmasters*: non vi è dubbio che la travolgente velocità del progresso tecnico in materia consentirà (prima o poi) di "controllare" in modo sempre più stringente ed attento il caricamento dei dati da parte del gestore del sito *web*, e l'esistenza di filtri preventivi sempre più raffinati obbligherà ad una maggiore responsabilità chi si troverà ad operare in presenza degli stessi; in questo caso la costruzione della responsabilità penale (colposa o dolosa che sia) per omesso controllo avrà un gioco più facile di quanto non sia stato nel momento attuale.

- In ogni caso questo giudice, come chiunque altro, rimane in attesa di una "buona legge" sull'argomento in questione: Internet è stato e continuerà ad essere un formidabile strumento di comunicazione tra le persone e, dove c 'è libertà di comunicazione c'è complessivamente più libertà, intesa come veicolo di conoscenza e di cultura, di consapevolezza e di scelta; ma ogni esercizio del diritto collegato alla libertà non può essere assoluto, pena il suo decadimento in arbitrio. E non c'è peggior dittatura di quella esercitata in nome della libertà assoluta: "*legum servi esse debemus, ut liberi esse possumus*" dicevano gli antichi e, nonostante il tempo trascorso, non si è ancora arrivati a scoprire una definizione migliore.

P.Q.M.

Visti gli artt.438 c.p.p., 533/535 c.p.p., dichiara D.D.C., D.L.R.G., Fl.P. colpevoli del reato di cui al capo B della rubrica e, concesse agli stessi le attenuanti generiche e la diminuente del rito, li condanna alla pena di mesi 6 di reclusione ciascuno, oltre al pagamento delle spese processuali.

[…]

Visto l'art.530 c.p.p., assolve D.D.C., D.L.R.G., Fl.P. e De.A. dal reato di cui al capo A della rubrica, perché il fatto, così come per gli stessi contestato, non sussiste.

[…]

4. DIRITTI E LIBERTA' IN RETE: PRIVACY

4.1. Anonimato in Rete e dati personali

Corte di Cassazione, sez.I civile, 8 luglio 2005, n.14390

[…]

1. L'ispettore della Polizia di Stato, signor […], ricorreva davanti al Garante per la protezione dei dati personali […], sostenendo che il dipartimento della Pubblica Sicurezza del Ministero dell'Interno avrebbe acquisito e trattato dati sensibili che lo riguardavano, nell'ambito di un procedimento disciplinare, in asserita violazione delle disposizioni della legge 675/1996.

In particolare, l'interessato affermava che la raccolta iniziale dei dati sarebbe stata effettuata da parte di alcuni suoi colleghi, i quali avrebbero agito al di fuori del servizio ed in veste "privata" (un tale, sovrintendente L., in rapporto di amicizia con il ricorrente, trovandosi occasionalmente nella sua abitazione, avrebbe notato accanto al computer alcuni indirizzi Internet, che avrebbe successivamente utilizzato:

a) per accedere a "siti della Rete" ove erano rilevabili annunci erotici, corredati da immagini di tipo osceno o pornografico, fra le quali nonostante l'alterazione del viso del soggetto ritratto - anche quelle attribuibili al signor T. - aventi contenuto omosessuale e feticista -;

b) per segnalare il fatto ai superiori, i quali - a loro volta - avrebbero promosso un procedimento disciplinare sfociato in proposte di trasferimento e di sospensione dal servizio).

Il ricorrente chiedeva al Garante che fosse accertata l'illiceità della condotta dell'amministrazione e delle singole persone fisiche che avrebbero agito "al di fuori dell'attività di servizio", disponendo il blocco e la distruzione dei dati trattati.

L'amministrazione faceva rilevare che i propri dipendenti devono sempre osservare i doveri inerenti alle loro funzioni, anche al di fuori del servizio (art.68, legge 121/1981) e che tutti gli appartenenti alla Polizia di Stato hanno il dovere di attenersi al segreto d'ufficio (art.34, d.p.r. 782/1985 e 16, ultimo comma, d.p.r. 737/1981).

1.1. Il ricorso veniva respinto dall'Autorità Garante, in base alle seguenti considerazioni.

Innanzitutto, non si sarebbero verificate ipotesi di "comunicazione" a terzi o di "diffusione" dei dati (art.1, comma 2, lett.g e h), posto che il trattamento si sarebbe svolto del tutto all'interno della struttura organizzativa e avrebbe coinvolto solo organi ed uffici dell'amministrazione.

Inoltre, esso trattamento sarebbe risultato conforme al dettato normativo (art.27, comma 1 e 22, commi 3 e 3-*bis*, come modificato dal d.lgs. 135/1999) ed, in particolare, alla previsione di cui all'art.68 della legge 121/1981, secondo la quale "Gli appartenenti ai ruoli dell'amministrazione della P.S. sono comunque tenuti, anche fuori dal servizio, ad osservare i doveri inerenti alla loro funzione". L'attività di acquisizione dei dati, posta in essere da un collega, avrebbe costituito una modalità possibile di accertamento e di verifica dei comportamenti ritenuti contrastanti con i doveri d'ufficio, derivanti dall'appartenenza alla Polizia di Stato. L'attività di trattamento sarebbe stata consentita proprio perché il d.lgs. 135/1999 avrebbe espressamente ammesso la finalità di tipo disciplinare fra quelle ritenute di rilevante interesse pubblico. Né essa sarebbe stata svolta, secondo i fatti emersi, in modo eccedente o non pertinente.

2. Avverso tale decreto, il signor T., ha proposto opposizione, ai sensi dell'art.29 della legge 675/1996, davanti al Tribunale di Roma, notificando il ricorso sia al Garante, sia al Ministero dell'Interno. Secondo l'interessato il decreto non avrebbe specificato perché il trattamento sarebbe stato imputato all'amministrazione, anziché al sovrintendente […], dati i comportamenti tenuti da quest'ultimo (che avrebbe estratto i dati da una propria postazione privata, ecc), Inoltre, nella specie, sarebbe difettato sia il consenso dell'interessato sia l'esattezza dei dati trattati.

Il Garante avrebbe eluso tali censure, limitandosi a dichiarare legittima la condotta dell'amministrazione, e respinto la richiesta di blocco e distruzione dei dati, acquisiti in modo illegittimo (cioè vita privata, al di fuori dell'esercizio delle funzioni proprie dell'attività istituzionale di polizia). In particolare, il Garante avrebbe eluso la censura relativa alla violazione dell'art.1, comma 2, lett.g) ed h) della legge 675/1996, atteso che il sovrintendente […] avrebbe dato corso ad una diffusione dei dati all'interno degli uffici dell'amministrazione, normalmente affollati dal personale. In tal modo il Garante avrebbe deciso la soccombenza dell'interesse della riservatezza rispetto all'interesse della pubblica amministrazione. Ma il trattamento dei dati, anche per le finalità consentite, avrebbe bisogno di essere autorizzato dal Garante, ai sensi dell'art.9 del d.lgs.

135/1999, modificativo dell'art.22 della legge 675/1996. Infine, sarebbe erronea la decisione nella parte in cui essa ha consentito l'acquisizione dei dati al di fuori del servizio, in violazione dell'art.28 del d.p.r. 782/1985, disposizione che limita l'obbligo di relazionare al responsabile dell'ufficio ai soli fatti "di particolare rilievo avvenuti durante l'espletamento del servizio".

Al contrario, i dati acquisiti dal sovrintendente L. costituirebbero esclusivamente una forma di delazione, perché gli stessi sarebbero stati privi di rilevanza penale o amministrativa, anche in considerazione che, attenendo gli stessi alla sfera sessuale, avrebbero necessitato del consenso dell'interessato e della preventiva autorizzazione del Garante. Il ricorrente, pertanto, chiedeva la disapplicazione o l'annullamento del provvedimento del Garante, il blocco e la distruzione dei dati sensibili illegittimamente acquisiti.

3. Il Tribunale di Roma respingeva l'opposizione, osservando che sarebbe stato proprio il ricorrente, con l'inserimento della propria foto sul sito Internet, a effettuare la diffusione dei dati personali a lui riconducibili (come da riconoscimento avvenuto ad opera dei colleghi); né il rilevamento e l'acquisizione dei dati, avvenuti in sede privata, e la loro trasmissione, per via gerarchica, sarebbe contraria al dettato normativo.

4. Avverso tale sentenza ricorre per Cassazione il signor T., con ricorso affidato a quattro motivi. L'amministrazione resiste con controricorso. Il Garante non ha svolto difese.

Motivi della decisione

[…]

1.2. Con il secondo motivo di ricorso (con il quale deduce la omessa, insufficiente e contraddittoria motivazione circa un punto decisivo della controversia, in relazione all'art.360, n.5, c.p.c.) il ricorrente si duole della mancanza, nel provvedimento del Tribunale, di una motivazione sufficiente e adeguata, resa senza un puntuale riesame di tutti i motivi posti dal ricorrente a base del ricorso, se si eccettuano quelli relativi alle modalità di acquisizione dei dati personali, da agenti in veste privata, e alla loro scorretta "diffusione". Lamenta altresì che la motivazione sia stata data *per relationem* rispetto al provvedimento del Garante.

1.3. e 1.4. Con il terzo e quarto motivo di ricorso (con i quali deduce la violazione e/o falsa applicazione degli artt.9, 11 e 22 della legge 675/1996, e dell'art.68 della legge 121/1981, in relazione all'art.360, n.3, c.p.c.) il ricorrente sostiene che il provvedimento del Tribunale sarebbe affetto da un cospicuo numero di errori, perché esso avrebbe:

a) dato per scontato che, nella specie, l'"interessato" al trattamento dei dati, reperiti sul sito Internet, sia proprio il signor T.;

b) considerato "titolare" del trattamento l'amministrazione anziché il sovrintendente L., che aveva provveduto ad acquisire i dati;

c) omesso di rilevare la mancanza del consenso scritto dell'interessato al trattamento;

d) omesso di accertare le scorrette modalità di raccolta dei dati, in violazione dell'art.9 della legge 675;

e) disatteso la necessità di individuare le attività che perseguono rilevanti finalità di interesse pubblico per le quali è autorizzato il trattamento;

f) disatteso, una volta ammessa la finalità dell'interesse pubblico *ex lege*, la necessità di identificare i tipi di dati e delle operazioni, pertinenti e necessarie, in relazione a tale finalità pubblica;

g) considerato legittimo il comportamento (scorretto) dell'amministrazione, la quale può e deve prendere in considerazione solo i fatti rilevanti, rilevati durante l'espletamento del servizio dei suoi agenti.

2. Il ricorso è parzialmente fondato e va accolto, nei sensi di cui in motivazione.

[…]

2.3.1. In particolare, il decreto impugnato, risulta censurato sotto una pluralità di profili, alcuni dei quali si rivelano inammissibili o del tutto infondati. Tali sono quelli relativi alla qualificazione del ricorrente quale interessato (lett.a) e dell'amministrazione, che si sarebbe avvalsa dell'attività "privatistica" svolta da alcuni dei suoi dipendenti, quali "titolare" del trattamento dei dati (lett.b, d e g).

2.3.1.1. A quest'ultimo proposito, il giudice del merito ha mostrato di condividere la posizione del Garante, e ha concluso che, il funzionario di polizia, pur avendo svolto la ricerca dei dati presso la propria abitazione, aveva poi seguito l'iter istituzionale, cosicché le foto, apparse e "prelevate" nell'ambito della rete Internet, erano state poi "trasmesse per via gerarchica", a chi di competenza.

La censura a tale conclusione del giudice di merito è del tutto inammissibile in questa sede, comportando una ricostruzione dei fatti e una valutazione degli stessi che non può trovar luogo nel giudizio di legittimità. Né il ricorrente ha indicato per quale ragione si sarebbe "reciso" il nesso organico e funzionale tra l'attività svolta dagli agenti che ebbero ad occuparsi del caso e l'amministrazione di appartenenza che, da parte sua, non solo ha preso in esame la documentazione trasmessa "per via gerarchica: come si è detto, ma ha anche convalidate" la legittimità dell'azione dei propri dipendenti, adottando, a carico dell'odierno ricorrente, i provvedimenti disciplinari di cui ci si lamenta, sia pure di riflesso, anche in questa sede.

2.3.1.2. Nella doglianza di cui alla lett.g), invero, ci si duole della violazione dell'art.68 della legge 121/1981 e dell'art.28 del d.p.r. 782/1985, in quanto si assume che il dovere degli agenti di riferire i fatti accaduti e percepiti dagli stessi non attenga a quelli emersi fuori del servizio e, nell'ambito opposto, riguardi soltanto i cd. "fatti rilevanti". Ma tale doglianza è infondata.

Secondo l'interpretazione che delle leggi indicate ha fatto la Cassazione nel suo magistero penale, "gli agenti e gli ufficiali della polizia, così come i carabinieri, sono da considerare in servizio permanente: nel senso che, anche nei periodi di permesso o di licenza, sono obbligati ad assumere l'esercizio attuale delle funzioni, allorché se ne verifichino le condizioni di legge, a nulla rilevando la sussistenza di particolari rapporti di amicizia, parentela o altro con la parte offesa" (Cassazione penale, sent. n.7075/1989) .

Si è, a tal proposito, operato la distinzione tra la nozione di “servizio permanente”, e quella diversa, di “esercizio delle funzioni”, implicando quest'ultima che il pubblico ufficiale può in ogni momento intervenire ed esercitare le sue funzioni (Cassazione penale, sentt. n.11928/1993 e n.21730/2001).

Orbene, il provvedimento impugnato, anche attraverso la recezione della motivazione del Garante, ha pienamente risposto a tale doglianza, considerando legittimo il comportamento del sovrintendente L. e, poi, quello dell'altro suo collega che ebbe a trasmettere i dati acquisiti ai superiori gerarchici.

Né può censurarsi, al riguardo, la qualificazione (tutta fattuale) circa il "particolare rilievo" dei fatti, oggetto di rapporto, atteso che, in astratto, tale nozione si riferisce sia ai fatti rilevanti sul piano penale sia a quelli suscettibili di rilievo amministrativo; e, del resto, in concreto, la valutazione di particolare rilevanza è stata già positivamente compiuta nella fase di merito, e tale conclusione, involgente valutazioni di merito, non è riesaminabile nel giudizio di legittimità.

2.3.1.3. Nella doglianza di cui alla lett.b), invece, si contesta che il ricorrente sia proprio la persona "interessata" al trattamento, con ciò volendosi dire che lo stesso disconosce come riferibili alla sua persona quelle foto "aventi contenuto omosessuale e feticista".

La censura al decreto impugnato riguarda propriamente la parte di esso ove afferma con certezza "che il T. abbia inserito nel sito Internet una propria fotografia e altre nelle quali, benché con il viso travisato, sarebbe stato ugualmente riconoscibile", anche in ragione dello "pseudonimo Max 30", adottato, e perciò si possa "affermare che sia stata effettuata proprio da lui la diffusione dei dati personali sensibili". La conclusione del Tribunale, va esaminata insieme alla doglianza dal ricorrente, poiché essa costituisce l'antecedente logico della questione che si andrà a trattare appresso.

2.3.1.4. Perché una persona assuma la qualità di "interessato" al trattamento dei dati personali è necessario che i dati di cui si controverta riguardino la persona fisica o la persona giuridica o l'ente o l'associazione che si dolga proprio del loro trattamento: cfr. l'art.1 della legge 675/1996 (e, ora, l'art.4 del cd. Codice della Privacy, di cui al d.lgs. 196/2003).

La nozione di "interessato", perciò, non suppone che i dati appartengano, con certezza, alla persona che si duole di quelle operazioni compiute su di essi, poiché ciò che rileva è la loro attribuzione o la loro esclusione a colui che, al riguardo, accampi un diritto (alla titolarità dei dati o all’estraneità degli stessi).

Infatti, questa Corte ha già avuto modo di precisare che anche "l'inesatto trattamento di dati personali legittima l'interessato ad invocare, presso la competente autorità di garanzia, la tutela di cui agli artt.1 ss. della legge 675/1996" (Cassazione, sent. n.8889/2001, secondo la quale, la legge 675/1996 è funzionale, nelle sue linee generali, alla difesa della persona e dei suoi fondamentali diritti e tende ad impedire che l'uso, astrattamente legittimo, del dato personale avvenga con modalità tali da renderlo lesivo di essi.) (Nella specie, la ricorrente, dopo aver reiteratamente ed inutilmente richiesto al direttore di un quotidiano a diffusione nazionale di rettificare un dato personale ad essa relativo e riportato più volte in modo inesatto, per ottenere la rettifica si era

rivolta al Garante, il quale aveva ordinato sia la cessazione del comportamento - in quanto illegittimo ai sensi della legge 675/1996 -, sia la rettifica della registrazione e del trattamento del dato personale *de quo*).

Pertanto, ha torto il ricorrente a credere che, per aver contestato l'attribuzione - alla sua persona - di quelle immagini, "aventi contenuto omosessuale e feticista", egli si sia spogliato, per ciò stesso, della qualità di "interessato". Proprio il fatto che egli intenda escludere l'attribuzione a sé di quei dati iconici fa sì che abbia assunto, a ragione, quella qualificazione e, in forza di essa, possa chiedere i provvedimenti del tipo di quelli da lui domandati al Garante ed al Tribunale (blocco del trattamento e distruzione dei dati).

Ma ha torto anche il Tribunale, laddove ha concluso per la piena trattabilità di quei dati solo perché sarebbe stato proprio il ricorrente a diffonderli nell'ambito della rete Internet. La pubblicità delle informazioni consentirebbe il loro libero uso.

2.3.1.5. Ma, in contrario, si osserva che questa Corte ha già avuto occasione e modi di affermare che "sia la legge 675/1996, sia il d.lgs. 196/2003 (cosiddetto "codice della privacy"), hanno ad oggetto della tutela anche i dati già pubblici o pubblicati, poiché colui che compie operazioni di trattamento di tali informazioni, dal loro accostamento, comparazione, esame, analisi, congiunzione, rapporto od incrocio, può ricavare ulteriori informazioni e, quindi, un "valore aggiunto informativo", non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato (ai sensi degli artt.3, primo comma, prima parte, e 2 Cost.), valore sommo a cui è ispirata la legislazione sul trattamento dei dati personali" (Corte di Cassazione, sez.I, sent. n.11864/2004).

Non è dunque la pubblicità in sé del dato che ne consente il trattamento, ricavandosi da esso ulteriore valore informativo, ma la sussistenza dei presupposti previsti dalla legge.

Nel caso di specie, perciò, occorreva passare a valutare l'esistenza dei presupposti normativi perché il trattamento compiuto dall'amministrazione dell'Interno potesse dirsi legittimo. Ciò che ha formato oggetto delle restanti ragioni di censure (lettere c, e, ed f) contenute nel ricorso e che devono essere esaminate congiuntamente.

2.4. Il ricorrente si duole, innanzitutto, del fatto che il trattamento dei dati sia avvenuto senza il suo consenso; in secondo luogo, che l'attività abbia avuto luogo senza che siano state enunciate le finalità di interesse pubblico; infine, che essa si sia svolta senza che siano stati identificati e resi pubblici i tipi di dati da trattare e le operazioni consentite. Tale complessiva doglianza, che è parzialmente fondata, impone l'accoglimento del ricorso *in parte qua*.

2.4.1. Premesso che nel caso in esame si controverte del trattamento di dati cd. supersensibili (riguardanti la salute e il sesso delle persone), al riguardo va operato il richiamo alla legge 675/1996, che è applicabile al caso di specie, *ratione temporis*, non già nella sua versione originaria, sebbene in quella modificata dal d.lgs. 135/1999.

Tale composita disciplina, ancora la legittimità del trattamento dei dati sensibili (art.22, comma 1), in linea generale, alla contestuale presenza del consenso scritto dell'interessato e all'autorizzazione del Garante.

Tuttavia, il comma 3 della stessa previsione di legge (quale risulta dall'addizione apportata dall'art.5, comma 2, del d.lgs. 135/1999), consente il trattamento da parte dei soggetti pubblici, "solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite".

Presupposti che, secondo il ricorrente, difetterebbero nel caso in esame, senza che il Tribunale, nel richiamarsi alla motivazione adottata dal Garante, *per relationem*, l'abbia rilevato ed anzi avendo disatteso una sua specifica doglianza, pure ritualmente e tempestivamente avanzata.

2.4.2. La previsione del comma 3, novellato, dell'art.22 della legge n.675 deroga, per i soli "soggetti pubblici", sia alla regola del consenso scritto, sia a quella della preventiva autorizzazione del Garante. Ma essa impone, che vi sia: i) una finalità di interesse pubblico; ii) un'espressa disposizione di legge autorizzatoria; iii) una specificazione legislativa dei tipi di dati trattabili e delle operazioni eseguibili. Nel caso che ci occupa, la rilevante finalità di interesse pubblico, è stata, correttamente individuata nel Provvedimento del Garante, condiviso *per relationem* dal Tribunale, nella previsione dell'art.9, comma 2, lett.g), del d.lgs. 135/1999, il quale sussume sotto le attività di rilevante interesse quelle "dirette all'accertamento della responsabilità civile, disciplinare e contabile", nell'ambito dei rapporti di lavoro.

Tale disciplina legislativa riguardante i rapporti di lavoro, però, non indica i tipi di dati, fra quelli appartenenti a quelli cd. sensibili, riportati nel comma 1 dell'art.22, che - nell'ambito di tali finalità - possono essere trattati e le operazioni eseguibili, al riguardo.

2.4.3. I commi 3 e 3-*bis* dell'art.22, più volte menzionato, però consentono ai soggetti pubblici, che intendano compiere tali trattamenti, di: "*richiedere al Garante, nelle more della specificazione legislativa, l'individuazione delle attività, fra quelle demandate ai medesimi soggetti dalla legge, che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi del comma 2, il trattamento dei dati indicati al comma 1*" (comma 3, ult. parte); e "*nei casi in cui (...) non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici (...) identificano e rendono pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni, strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente*"; insomma, ove non sia stata la legge a specificare tipi di dati sensibili ed operazioni eseguibili su di essi, possono e debbono farlo i "*soggetti pubblici autorizzati al trattamento*" o, su loro richiesta, l'Autorità Garante.

La particolare natura di tali dati, e specialmente quelli appartenenti alla *species* dei supersensibili, che investe la parte più intima della persona nella sua corporeità e nelle sue convinzioni psicologiche più riservate, che riceve una tutela rafforzata proprio in ragione dei valori costituzionali posti a loro presidio (artt.2 e 3 Cost.), è oggetto di una protezione rafforzata, che si esplicita nelle garanzie poste anche riguardo al trattamento operato dai "soggetti pubblici". Queste, infatti, esigono il rispetto di un modulo procedimentale, corrispondente a quello stabilito dalla legge/1996, così come integrato nel 1999.

2.4.4. A tale riguardo il ricorrente ha avanzato le sue doglianze al Tribunale, lamentando la mancanza dei presupposti di legalità del trattamento, anche con specifico riguardo all'autorizzazione fornita dalla legge o accordata dall'Autorità Garante, e contestando le affermazioni contenute nel provvedimento di quest'ultima.

A tali doglianze, che non trovano risposta neppure in quella parte della motivazione del provvedimento amministrativo, richiamato *per relationem* dal decreto, il Tribunale ha omesso ogni risposta e, perciò, ai fini del ricorso, anche ogni esame.

La qualcosa rende il provvedimento giurisdizionale impugnato invalido e perciò, denunciandosene il vizio, con l'odierno ricorso, da cassare con rinvio ad altra sezione dello stesso organo giurisdizionale di merito, per un nuovo esame della controversia in ordine a tale complessiva omessa pronuncia, oltre che per regolare le spese di questa fase.

3. In conclusione, il giudice del rinvio dovrà valutare se l'amministrazione dell'Interno, in relazione al caso in esame, era legittimata al trattamento dei dati personali supersensibili del ricorrente, riguardanti i suoi presunti gusti, atteggiamenti e comportamenti sessuali, in relazione alla finalità disciplinare, nell'ambito del rapporto di lavoro, ai sensi dell'art.22 della legge 675/1996, come novellato dal d.lgs. 135/1999.

[…]

4.2. Identità personale in Rete

Corte di Cassazione, sez.V penale, 14 dicembre 2007, n.46674

[…]

Con l'impugnata sentenza è stata confermata la dichiarazione di colpevolezza di A.A.M. in ordine al reato p. e p. dagli artt.81, 494 c.p., contestatogli "perché, al fine di procurarsi un vantaggio e di recare un danno ad T.A., creava un *account* di posta elettronica, […] apparentemente intestato a costei, e successivamente, utilizzandolo, allacciava rapporti con utenti della rete Internet al nome della T., così induceva in errore sia il gestore del sito sia gli utenti, attribuendosi il falso nome della T.".

Ricorre per Cassazione il difensore deducendo violazione di legge per l'erronea applicazione dell'art.494 c.p., e per la mancata applicazione dell'art.129 c.p.p..

Lamenta che non siano state confutate dalla Corte fiorentina le critiche rivolte al convincimento di colpevolezza espresso dal primo giudice siccome basato sulla duplice errata considerazione, inerente la prima alla tutela di stampo civilistico al nome e allo pseudonimo, l'altra, più propriamente tecnica - informatica, alla sostenuta necessità di fornire all'ente gestore del servizio telefonico l'esatta indicazione anagrafica al momento della richiesta di fornitura della prestazione telematica.

Tali doglianze non possono essere condivise.

Oggetto della tutela penale, in relazione al delitto preveduto nell'art.494 c.p., è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome.

In questa prospettiva, è evidente la configurazione, nel caso concreto, di tutti gli elementi costitutivi della contestata fattispecie delittuosa.

Il ricorrente disserta in ordine alla possibilità per chiunque di attivare un "*account*" di posta elettronica recante un nominativo diverso dal proprio, anche di fantasia. Ciò è vero, pacificamente.

Ma deve ritenersi che il punto del processo che ne occupa sia tutt'altro.

Infatti il ricorso non considera adeguatamente che, consumandosi il reato "*de quo*" con la produzione dell'evento conseguente all'uso dei mezzi indicati nella disposizione incriminatrice, vale a dire con l'induzione di taluno in errore, nel caso in esame il soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della Rete, i quali, ritenendo di interloquire con una determinata persona (la T.), in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa.

E non vale obiettare che "il contatto non avviene sull'*intuitus personae*, ma con riferimento alle prospettate attitudini dell'inserzionista, dal momento che non è affatto indifferente, per l'interlocutore, che "il rapporto descritto nel messaggio" sia offerto da un soggetto diverso da quello che appare offrirlo, per di più di sesso diverso.

È appena il caso di aggiungere, per rispondere ad altra, peraltro fugace, contestazione difensiva, che l'imputazione *ex* art.494 c.p.p., debitamente menziona pure il fine di recare, con la sostituzione di persona un danno al soggetto leso: danno poi in effetti, in tutta evidenza concretizzato, nella specie, come il capo B) della rubrica (relativo al reato di diffamazione, peraltro poi estinto per remissione della querela) nitidamente delinea nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l'immagine e la dignità (sottolinea la sentenza impugnata che la T., a seguito dell'iniziativa assunta dall'imputato,"si ricevette telefonate da uomini che le chiedevano incontri a scopo sessuale").

Il ricorso va pertanto respinto, con le conseguenze di legge.

[…]

4.3. 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 del Parlamento europeo e del Consiglio 24 ottobre 1995, 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 Alseda (Svezia). Essa ha seguito un corso di informatica nell'ambito del quale doveva in particolare creare una pagina iniziale su 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".

2) Ove la questione precedente venga risolta negativamente, se il redigere, su una pagina iniziale su Internet, pagine che riguardano specificamente una quindicina di persone e il collegare tali pagine tra di esse in modo da consentire la ricerca nominativa possa essere considerato un "trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi" ai sensi dell'art.3, n.1, della direttiva.

Per il caso in cui una delle questioni precedenti venga risolta positivamente, lo *hovrätt* pone anche le questioni seguenti:

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.

Lo *hovrätt* desidera infine porre la seguente questione:

7) Se uno Stato membro possa, nelle circostanze indicate nelle questioni precedenti, prevedere una tutela più ampia dei dati personali o ampliare l'ambito di applicazione della direttiva 95/46/CE, anche ove non ricorra nessuna delle condizioni di cui all'art.13 della medesima».

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 passatempo.

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 seconda questione

28. Dato che la prima questione è stata risolta in senso affermativo, non occorre risolvere la seconda questione, che è stata posta solo per il caso di soluzione negativa della prima.

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 dell'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.

38. La prima eccezione riguarda i trattamenti di dati personali effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'Unione europea, e, comunque, i trattamenti aventi ad oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale.

39. Essendo le attività della sig.ra Lindqvist di cui trattasi nella causa principale sostanzialmente non economiche, ma a carattere religioso e svolte a titolo di volontariato, occorre accertare se esse costituiscano trattamenti di dati personali «effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario» ai sensi dell'art.3, n.2, primo trattino, della direttiva 95/46/CE.

40. La Corte ha già dichiarato, a proposito della direttiva 95/46/CE, fondata sull'art.100 A del Trattato, che il ricorso a questo fondamento giuridico non presuppone l'esistenza di un nesso effettivo con la libera circolazione tra Stati membri in ciascuna delle situazioni previste dall'atto fondato su tale base (v. sent. 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e a.,* […]).

41. Un'interpretazione in senso contrario rischierebbe di rendere particolarmente incerti e aleatori i limiti del campo di applicazione della detta direttiva, il che sarebbe contrario al suo obiettivo essenziale, che è quello di ravvicinare le disposizioni legislative, regolamentari ed amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali (sent. *Österreichischer Rundfunk e a., cit.*, p.to 42).

42. Di conseguenza, non sarebbe appropriato interpretare l'espressione «attività che non rientrano nel campo di applicazione del diritto comunitario» in modo da attribuirle una portata tale da rendere necessario verificare, caso per caso, se l'attività specifica in questione incida direttamente sulla libera circolazione tra gli Stati membri.

43. Le attività indicate, a mo' di esempio, nell'art.3, n.2, primo trattino, della direttiva 95/46/CE (cioè le attività previste nei titoli V e VI del Trattato sull'Unione europea nonché i trattamenti aventi ad oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività relative a settori del diritto penale) sono, in tutti i casi, attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli.

44. Si deve quindi ritenere che le attività menzionate a titolo esemplificativo nell'art.3, n.2, primo trattino, della direttiva 95/46/CE siano destinate a definire la portata dell'eccezione ivi prevista, di modo che detta eccezione si applica solo alle attività che vi sono così espressamente menzionate e che possono essere ascritte alla stessa categoria (*eiusdem generis*).

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 inserisca su una pagina Internet - caricata presso una persona fisica o giuridica che ospita il sito Internet sul quale la pagina può essere consultata (in prosieguo: 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 ottenerli. 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 ricomprendere nella nozione 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 specifiche, 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 di 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 garantiscano 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.

65. L'art.25 della direttiva 95/46/CE impone, da parte sua, agli Stati membri ed alla Commissione vari obblighi di controllo sui trasferimenti di dati personali verso i Paesi terzi, tenuto conto del livello di protezione concesso a siffatti dati in ciascuno di tali Paesi.

66. In particolare, l'art.25, n.4, della direttiva 95/46/CE prevede che, qualora la Commissione constati che un Paese terzo non garantisce un livello di protezione adeguato, gli Stati membri adottano 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 così 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 ch'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.

Sulla settima questione

91. Con la settima questione il giudice del rinvio chiede, in sostanza, se gli Stati membri possano prevedere una tutela più ampia dei dati personali o ampliare l'ambito in applicazione della direttiva 95/46/CE.

[…]

Soluzione della Corte

95. La direttiva 95/46/CE mira, come risulta in particolare dal suo ottavo "considerando", a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. Il decimo "considerando" aggiunge che il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurate, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità.

96. L'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa. È in quest'ottica che la direttiva 95/46/CE intende garantire la libera circolazione dei dati personali, pur assicurando un alto livello di tutela dei diritti e degli interessi delle persone cui si riferiscono tali dati.

97. Vero è che la direttiva 95/46/CE riconosce agli Stati membri un margine di manovra in taluni settori e che essa li autorizza a mantenere o a istituire regimi particolari per situazioni specifiche, come dimostrano molte delle sue disposizioni. Tuttavia, siffatte possibilità devono essere usate nel modo previsto dalla direttiva 95/46/CE ed in conformità del suo obiettivo, che consiste nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata.

98. Per contro, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/CE a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario.

99. Alla luce di queste considerazioni, la settima questione va risolta nel senso che le misure adottate dagli Stati membri per garantire la protezione dei dati personali devono essere conformi tanto alle disposizioni della direttiva 95/46/CE quanto al suo obiettivo, consistente nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata. Per contro, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/CE a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario.

[…]

4.4. Pubblicazione di dati fiscali in Rete

Garante per la protezione dei dati personali, provv. 6 maggio 2008

Redditi *online*: illegittima la diffusione dei dati sul sito Internet dell'Agenzia delle entrate

[…]

VISTA la disciplina che regola la pubblicazione degli elenchi nominativi dei contribuenti che hanno presentato le dichiarazioni ai fini dell'imposta sui redditi e dell'imposta sul valore aggiunto; rilevato che su questa base gli elenchi sono formati annualmente e depositati per un anno, ai fini della consultazione da parte di chiunque, presso i Comuni interessati e gli uffici dell'Agenzia competenti territorialmente; rilevato che con apposito decreto devono essere stabiliti annualmente *"i termini e le modalità"* per la loro formazione *(art.69 d.p.r. 29 settembre 1973, n.600, come mod. dall'art.19, legge 30 dicembre 1991, n.413; art.66-bis d.p.r. 26 ottobre 1972, n.633)*;

VISTO il provvedimento con il quale l'Agenzia delle entrate ha attuato tale disciplina per il 2005 disponendo che gli elenchi, distribuiti ai predetti uffici dell'Agenzia e trasmessi ai comuni mediante sistemi telematici, siano altresì pubblicati nell'apposita sezione del sito Internet dell'Agenzia *http://www.agenziaentrate.gov.it "ai fini della consultazione" "in relazione agli uffici dell'Agenzia delle entrate territorialmente competenti" (Provv. Direttore dell'Agenzia 5 marzo 2008 prot. 197587/2007)*;

VISTO il provvedimento del 30 aprile 2008 con il quale questa Autorità, appena avuta notizia di tale diffusione in Internet e avendo ritenuto sulla base di una verifica preliminare che essa non risultava conforme alla normativa di settore, ha invitato in via d'urgenza l'Agenzia a sospenderla;

RILEVATO che con tale provvedimento il Garante ha anche invitato l'Agenzia a fornire ulteriori chiarimenti che, sollecitati con nota dell'Autorità del 2 maggio, sono pervenuti nel termine indicato (nota Agenzia 5 maggio 2008, n.2008/68657); esaminate le deduzioni formulate e la documentazione allegata;

RILEVATO dalle segnalazioni pervenute e dagli elementi acquisiti nell'istruttoria preliminare che la diffusione in Internet a cura direttamente dell'Agenzia, contrariamente a quanto da questa sostenuto nella predetta nota, contrasta con la normativa in materia, in quanto:

1) il provvedimento del Direttore dell'Agenzia poteva stabilire solo *"i termini e le modalità"* per la formazione degli elenchi. La conoscibilità di questi ultimi è infatti regolata direttamente da disposizione di legge che prevede, quale unica modalità, la distribuzione di tali elenchi ai soli uffici territorialmente competenti dell'Agenzia e la loro trasmissione, anche mediante supporti magnetici ovvero sistemi telematici, ai soli Comuni interessati, in entrambi i casi in relazione ai soli contribuenti dell'ambito territoriale interessato. Ciò, come sopra osservato, ai fini del loro deposito per la durata di un anno e della loro consultazione - senza che sia prevista la facoltà di estrarne copia - da parte di chiunque *(art.69, commi 4 ss., d.p.r. 600/1973 cit.; v. anche art.66-bis d.p.r. 26 ottobre 1972, n.633)*;

2) il Codice dell'amministrazione digitale, invocato dall'Agenzia a sostegno della propria scelta, incentiva l'uso delle tecnologie dell'informazione e della comunicazione nell'utilizzo dei dati delle pubbliche amministrazioni. Tuttavia, il Codice stesso fa espressamente salvi i limiti alla conoscibilità dei dati previsti da leggi e regolamenti (come avviene nel menzionato art.69), nonché le norme e le garanzie in tema di protezione dei dati personali *(artt.2, comma 5, e 50, d.lgs. 7 marzo 2005, n.82)*;

3) la predetta messa in circolazione in Internet dei dati, oltre a essere di per sé illegittima perché carente di una base giuridica e disposta senza metterne a conoscenza il Garante, ha comportato anche una modalità di diffusione sproporzionata in rapporto alle finalità per le quali l'attuale disciplina prevede una relativa trasparenza. I dati sono stati resi consultabili non presso ciascun ambito territoriale interessato, ma liberamente su tutto il territorio nazionale e all'estero. L'innovatività di tale modalità, emergente dalle stesse deduzioni dell'Agenzia, non traspariva dalla generica informativa resa ai contribuenti nei modelli di dichiarazione per l'anno 2005. L'Agenzia non ha previsto "filtri" nella consultazione *online* e ha reso possibile ai numerosissimi utenti del sito salvare una copia degli elenchi con funzioni di trasferimento *file*. La centralizzazione della consultazione a livello nazionale ha consentito ai medesimi utenti, già nel ristretto numero di ore in

cui la predetta sezione del sito *web* è risultata consultabile, di accedere a innumerevoli dati di tutti i contribuenti, di estrarne copia, di formare archivi, modificare ed elaborare i dati stessi, di creare liste di profilazione e immettere tali informazioni in ulteriore circolazione in rete, nonché, in alcuni casi, in vendita. Con ciò ponendo anche a rischio l'esattezza dei dati e precludendo ogni possibilità di garantire che essi non siano consultabili trascorso l'anno previsto dalla menzionata norma;

4) infine, va rilevato che questa Autorità non è stata consultata preventivamente dall'Agenzia stessa, come prescritto rispetto ai regolamenti e agli atti amministrativi attinenti alla protezione dei dati personali *(art.154, comma 4, del Codice)*;

CONSIDERATO che, sulla base delle motivazioni suesposte, non risulta lecita la predetta forma di pubblicazione degli elenchi;

CONSIDERATO pertanto che, a conferma della sospensione già effettuata, va inibita all'Agenzia la diffusione ulteriore in Internet dei predetti elenchi con le modalità sopra indicate, nonché la loro diffusione in modo analogo per i periodi di imposta successivi al 2005 in carenza di un'idonea base normativa e della preventiva consultazione del Garante *(artt.143, comma 1, lett.c) e 154, comma 1, lett.a), b) e d), del Codice)*;

CONSIDERATO che con contestuale altro provvedimento va contestata all'Agenzia la violazione amministrativa per l'assenza di un'idonea e preventiva informativa ai contribuenti interessati *(artt.13 e 161 del Codice)*;

CONSIDERATO che coloro che hanno ottenuto i dati dei contribuenti provenienti, anche indirettamente, dal menzionato sito Internet, non possono metterli ulteriormente in circolazione stante la violazione di legge accertata con il presente provvedimento; considerato che tale ulteriore loro messa in circolazione - in particolare mediante reti telematiche o altri supporti informatici - configura un fatto illecito che, ricorrendo determinate circostanze, può avere anche natura di reato *(artt.11, commi 1, lett.a) e 2, 13, 23, 24, 161 e 167 del Codice)*; rilevata pertanto la necessità di favorire la più ampia pubblicità al presente provvedimento;

CONSIDERATO che restano tuttavia impregiudicate le altre forme di legittimo accesso agli elenchi consultabili da chiunque presso Comuni interessati e uffici dell'Agenzia competenti territorialmente, ai fini di un loro legittimo utilizzo anche per finalità giornalistiche;

CONSIDERATO che, qualora il Parlamento e il Governo intendessero porre mano a una revisione normativa della disciplina sulla conoscibilità degli elenchi dei contribuenti anche in rapporto all'evoluzione tecnologica, si porrà l'esigenza di individuare, sentita questa Autorità, opportune soluzioni e misure di protezione per garantire un giusto equilibrio tra l'esigenza di forme proporzionate di conoscenza dei dati dei contribuenti e la tutela dei diritti degli interessati;

[…]

Tutto ciò premesso il Garante

1) a conferma della sospensione della pubblicazione degli elenchi nominativi per l'anno 2005 dei contribuenti che hanno presentato dichiarazioni ai fini dell'imposta sui redditi e dell'imposta sul valore aggiunto, ai sensi degli artt.143, comma 1, lett.c) e 154, comma 1, lett.a), b) e d), del Codice, inibisce all'Agenzia di:

a) diffondere ulteriormente in Internet detti elenchi con le modalità che il presente provvedimento ha stabilito essere in contrasto con la disciplina di settore attualmente vigente;

b) diffonderli in modo analogo per i periodi di imposta successivi al 2005, in carenza di idonea base normativa e della preventiva consultazione del Garante;

2) manda all'Ufficio di contestare all'Agenzia, con contestuale provvedimento, la violazione amministrativa per l'assenza di un'idonea e preventiva informativa ai contribuenti interessati;

3) dispone che l'Ufficio curi la più ampia pubblicità del presente provvedimento, anche mediante pubblicazione sulla *Gazzetta ufficiale* della Repubblica italiana, al fine di rendere edotti coloro che hanno ottenuto i dati dei contribuenti provenienti, anche indirettamente, dal sito Internet dell'Agenzia, della circostanza che essi non possono continuare a metterli in circolazione stante la suesposta violazione di legge e che tale ulteriore messa in circolazione configura un fatto illecito che, ricorrendo determinate circostanze, può avere anche natura di reato.

[…]

4.5. 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 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 ampia 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 argomentato 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 *online* 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.

Peraltro, 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, intendendo 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;

[…]

4.6. La protezione dei minori

Corte di Cassazione, sez.III penale, 11 febbraio 2002, n.5397

[…]

Svolgimento del processo

Il giudice per le indagini preliminari del Tribunale di Lecce, con ordinanza del 17 aprile 2001, dispose la misura cautelare degli arresti domiciliari nei confronti di D.M., indagato per il delitto di cui all'art.600, comma 3, c.p.. Per avere per via telematica attraverso Internet, tramite una particolare procedura di collegamento denominata *F-server*, che permette nel corso di una *chat* di accedere a scambiare automaticamente i *files* esistenti sul disco rigido dell'interlocutore, distribuito e divulgato materiale fotografico avente ad oggetto minori degli anni 18, ritratti nel corso di rapporti sessuali tra loro ed adulti.

[…]

Motivi della decisione

[…]

Nell'ottobre del 1999, agenti della polizia postale di Reggio Calabria iniziarono un'attività di indagine in Internet alla ricerca di eventuale traffico di materiale pornografico a carattere pedofilo.

L'indagine si svolse dapprima con la verifica di siti campione (come *www.xxxxxxx.com*) e poi con l'individuazione di numerose liste (o gruppi) di discussione a tema specificamente pedofilo (come, *alt.xxxxxx.xxxxx.xxxxxx.xxxxxx-xxxxx*).

Dati questi risultati, raggiunti, così si legge nelle citate sentenze, grazie all'utilizzo di personale altamente qualificato, in data 11 aprile 2000 il pubblico ministero di Reggio Calabria autorizzò, a quanto sembrerebbe, gli agenti di polizia ad acquistare in rete materiale pornografico e ad individuare soggetti interessati allo scambio di esso.

A seguito di ciò, il 6 luglio 2000 un agente della polizia, attraverso l'uso del sistema *IRC*, entrò in un canale *MIRC* denominato *fotoporno*, relativo al servitore *IRC-net*, ed usando lo pseudonimo di *Mario123* iniziò a dialogare con altri utenti, tra cui uno di nome *Belfagor*, il quale ad un certo punto chiese lo scambio di foto pornografiche.

L'agente entrò allora in colloquio privato con *Belfagor* inviandogli delle foto e ricevendone due, di cui una definita a contenuto pedopornografico e l'altra ritraente due minori nude.

Mentre l'agente, attraverso il programma *Visual Route*, stava rilevando l'indirizzo IP dinamico dell'interlocutore, questi gli intimò di fermarsi e poi troncò la comunicazione.

Attraverso il riscontro dei tabulati telefonici si risalì quindi all'utenza telefonica dell'odierno ricorrente […].

Il secondo motivo è […] fondato.

Dinanzi al Tribunale del riesame l'indagato aveva eccepito che una delle due foto da lui inviate al suo interlocutore non poteva in alcun modo considerarsi come pornografica, in quanto ritraeva due soggetti nudi e quindi aveva semmai un semplice contenuto erotico.

Su tale accezione è ovviamente competente a decidere esclusivamente il giudice di merito.

Tuttavia, il Tribunale del riesame ha totalmente omesso di esaminare l'eccezione stessa e di fornire la benché minima motivazione in proposito sebbene, come esattamente rileva il ricorrente, la circostanza che eventualmente si tratti di una sola fotografia, anziché di due fotografie penalmente significative, non può in astratto ritenersi irrilevante in relazione alla valutazione sia delle esigenze cautelari sia delle possibilità di applicare la sospensione condizionale della pena, essendo entrambi detti profili connessi con la gravità delle condotte ipotizzate.

L'indagato aveva altresì espressamente eccepito che l'altra foto, quella a contenuto pornografico, raffigurava un rapporto sessuale con una giovane che non poteva ritenersi con sicurezza essere una minorenne.

Aveva anche rilevato che a favore della maggiore età della ragazza ritratta nella foto stava il fatto che lo scambio di foto era avvenuto in un canale MIRC denominato *fotoporno*, e cioè in un canale di contenuto pornografico ma non specificamente rivolto alla pedofilia e quindi era evidente che l'utente denominato Belfagor, nel chiedere lo scambio di foto, si era riferito a foto legate al

tema pornografico del sito, ma non risultava assolutamente che si trattasse di foto in qualche modo attinenti a minori.

Aveva quindi concluso nel senso che l'assoluta incertezza sul fatto che si potesse trattare di una minorenne precludeva di ravvisare i gravi indizi di colpevolezza.

Il Tribunale del riesame ha rigettato questa eccezione in base alla sola considerazione che il collegio non ha elementi per ritenere che i soggetti riprodotti siano adulti.

È di tutta evidenza l'erroneità e la manifesta illogicità della motivazione, che pretende di basarsi su un'inammissibile inversione dell'onere della prova, in quanto spetta all'accusa, anche in sede cautelare, fornire la prova dell'esistenza di gravi indizi di colpevolezza e quindi della sussistenza degli elementi costituitivi del reato addebitato, e non già alla difesa fornire la prova della loro inesistenza.

Spettava quindi all'accusa provare che vi erano gravi indizi che si trattasse di minorenni, e non già alla difesa provare che si trattava di maggiorenni.

Il Tribunale, pertanto, avrebbe dovuto prospettare in motivazione quegli elementi che, in base al suo giudizio di merito insindacabile in questa sede se logicamente motivato, fondavano la convinzione di trovarsi di fronte ad una foto che ritraeva uno o più soggetti minorenni, e non invece ricercare gli elementi per ritenere che i soggetti stessi fossero adulti.

Ed infatti, anche l'elemento costitutivo del reato rappresentato dalla minore età del soggetto coinvolto nel rapporto sessuale doveva essere coperto dai gravi indizi di colpevolezza necessari per il mantenimento in vita del titolo coercitivo, sicché è erroneo ed immotivato il ragionamento del Tribunale di Lecce, il quale, anziché preoccuparsi di chiarire l'iter logico che avrebbe condotto al riconoscimento della minore età e dunque alla sussistenza del delitto, ha preteso di imporre alla difesa l'onere di contrastare l'apoditticità della tesi accusatoria.

Ma la motivazione dell'ordinanza impugnata appare carente sotto un altro profilo.

All'indagato è stato contestato il delitto di cui all'art.603-*ter*, terzo comma, c.p., il quale punisce, con reclusione da uno a cinque anni e con multa da lire 5 milioni a lire 100 milioni, tra l'altro, chi, non avendo commesso uno dei fatti di cui al primo o al secondo comma, ossia non avendo sfruttato un minore degli anni diciotto al fine di realizzare esibizioni pornografiche o di produrre materiale pornografico e non avendo fatto commercio del detto materiale pornografico, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma.

Il successivo quarto comma, invece, punisce con reclusione fino a tre anni oppure con multa da lire 3 milioni a lire 10 milioni chi consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto.

Orbene, la giurisprudenza di questa Suprema Corte ha affermato che ai fini della configurabilità del reato di cui all'art.600-*ter*, comma 3, c.p. (distribuzione, divulgazione o pubblicizzazione del materiale pornografico di cui al precedente comma 1 con qualsiasi mezzo, anche in via telematica), se da una parte non basta la cessione di detto materiale a singoli soggetti, dall'altra è sufficiente che, indipendentemente dalla sussistenza o meno del fine di realizzare esibizioni pornografiche o di produrre il relativo materiale, questo venga propagato ad un numero indeterminato di destinatari (sez.III, 14 luglio 2000, *Salvalaggio* […]), e che rientrano nella fattispecie di cui all'art.600-*ter* c.p. la divulgazione e pubblicazione, le quali richiedono sia che la condotta sia destinata a raggiungere una serie indeterminata di persone, con cui l'agente ha stabilito un rapporto di comunicazione, sia un mezzo di diffusione accessibile ad una pluralità di soggetti (sez.III, 13 giugno 2000 *Tedde* […]).

Non può però ritenersi che, per la sussistenza del delitto di cui al comma 3 dell'art.600-*ter*, c.p., sia sufficiente, come a volte invece capita di leggere, la mera circostanza che le foto pornografiche di minori siano veicolate attraverso la rete Internet, a parte che non si comprende che cosa si intenda con tale espressione, data la sua vaghezza.

Così, il delitto in esame è certamente configurabile qualora il soggetto, ad esempio, inserisca le foto pornografiche minorili in un sito accessibile a tutti ovvero quando le propaghi attraverso *usenet*, inviandole ad un gruppo o lista di discussione, da cui chiunque le possa scaricare.

Al converso, pare ipotizzabile non il delitto in esame, ma quello più lieve di cui al comma 4, quando, ad esempio, il soggetto invii la foto ad una persona determinata allegandola ad un messaggio di posta elettronica.

E nemmeno sembra significativo, per la configurabilità del reato in questione, limitarsi a rilevare che la cessione delle foto è avvenuta attraverso un programma o stanza o canale di

discussione (in inglese, *chat-line*) del tipo *IRC*, come quello utilizzato nella specie, o similari, dovendosi invece distinguere l'ipotesi in cui si sia trattato di una sola isolata cessione avvenuta nel corso di una discussione privata con una singola determinata persona, di modo che la foto sia stata di fatto ceduta ad una sola persona e solo questa abbia avuto la possibilità di prelevarla, dall'ipotesi in cui invece la foto sia stata ceduta in un canale aperto a tutti gli utenti, di modo che qualsiasi soggetto si trovi nella stanza o nel canale abbia avuto la possibilità di prelevarla, oppure sia stata ceduta comunque ad una pluralità di soggetti sia pure attraverso una serie di diverse conversazioni private.

Ed infatti, nella specie, il capo di imputazione non si limita a contestare all'indagato di aver ceduto le foto nel corso di una discussione in un canale *IRC*, ma gli contesta di averle distribuite e divulgate effettuando la cessione tramite una particolare procedura di collegamento che permette nel corso di una discussione di accedere e scambiare direttamente i documenti esistenti sul disco rigido di un interlocutore.

E, se così fosse, sarebbe senz'altro ipotizzabile il delitto di cui al comma 3 dell'art.600-*ter* c.p.p..

Deve invero ritenersi che si realizza una distribuzione o divulgazione delle foto pornografiche ad una serie indeterminata di persone anche quando la loro cessione avvenga attraverso programmi (come, ad esempio, *Napster* nel caso di archivi musicali ovvero uno dei tanti programmi similari che si basano sullo stesso o su analogo principio di scambio dei documenti) che permettono a chi li utilizzi e sia collegato in quel momento e in quella particolare rete la condivisione di cartelle, archivi e documenti.

Se infatti il soggetto, attraverso l'uso di un programma e di una rete del genere, condivide con gli altri utenti le foto pornografiche registrate sul suo disco rigido o in un altro supporto, nel senso che mette a disposizione di tutti la parte del suo disco rigido o di altra memoria di massa dove sono contenute le foto pornografiche minorili in modo che chiunque possa accedere alle cartelle condivise e prelevare direttamente le foto, è evidente che è configurabile un'ipotesi di distribuzione e divulgazione ad un numero indeterminato di persone.

Ora, su questo aspetto, essenziale per la configurabilità del reato ipotizzato, la motivazione dell'ordinanza impugnata in parte è manifestamente illogica e contraddittoria ed in parte manca, non avendo invero il Tribunale risposto alle eccezioni che in proposito l'indagato aveva avanzato con memoria difensiva.

Il Tribunale del riesame, infatti, ha ritenuto esatta la qualificazione giuridica del fatto soltanto sulla base della considerazione che ai fini della sussistenza di tale reato è sufficiente che il materiale pedo-pornografico venga propagato ad un numero indeterminato di destinatari, come appunto si verifica nel caso in cui tale cessione venga effettuata mediante l'uso di una *chat-line*, e quindi attraverso la rete Internet attesa la possibilità di un qualunque ignoto utente interessato (dotato di adeguata strumentazione) di partecipare alla *chat*.

È chiaro come questa motivazione sia non solo erronea, come dinanzi osservato, ma anche totalmente elusiva, per la sua genericità, delle puntuali osservazioni avanzate dalla difesa e comunque manifestamente illogica, perché contrastante con elementi fattuali che emergono dallo stesso testo del provvedimento impugnato.

Innanzitutto, infatti, è pacifico che vi fu un unico collegamento, intervenuto il 6 luglio 2000, tra gli agenti di polizia giudiziaria e l'utenza del ricorrente.

In ogni caso, dall'originaria ordinanza cautelare del giudice per le indagini preliminari del Tribunale di Reggio Calabria risulta che, dopo un primo contatto in una stanza di discussione, l'agente di polizia entrò in colloquio privato con l'indagato, inviandogli delle foto e ricevendo le due foto in questione.

Nella medesima ordinanza si legge poi che è particolare degno di menzione … che mentre il personale operante, tramite il programma *Visual Route*, stava rilevando l'indirizzo IP dinamico, l'interlocutore intimava di fermarsi, e poi troncava la comunicazione, segno evidente che lo stesso fosse in possesso di software idoneo a controllare l'accesso alle porte del proprio *F-server*.

Inoltre, l'ordinanza del giudice per le indagini preliminari del Tribunale di Lecce afferma espressamente che il 6 luglio 2000 l'agente di polizia postale riuscì ad entrare in contatto con Belfagor, e cioè ad instaurare un rapporto diretto con l'indagato, e che fu proprio Belfagor che permise l'ingresso nella memoria del proprio *server* ed il trasferimento in favore dell'agente di polizia delle due fotografie.

Il difensore aveva espressamente osservato che tali circostanze non solo che l'indagato aveva semmai ceduto le foto nel corso di un colloquio privato ma anche che egli era capace di interdire l'accesso alle porte del proprio elaboratore a terzi estranei, così come in effetti lo interdisse immediatamente nel momento in cui l'agente a cui aveva ceduto le foto provò ad entrarvi senza il suo consenso.

Aveva quindi dedotto la difesa che per l'odierno ricorrente non potevano valere le osservazioni riferite ad altri coindagati, perché il ricorrente non aveva mai permesso l'indiscriminato accesso al disco rigido del suo elaboratore e lo scambio continuo degli archivi e quindi non aveva mai determinato la distribuzione o la divulgazione delle foto ad un numero illimitato, indeterminato ed indeterminabile di soggetti, ed anzi era in possesso di programmi idonei a controllare l'accesso alle proprie porte, di modo che nessuno poteva accedervi direttamente e senza il suo consenso ed egli era in grado di cedere a quel singolo determinato interlocutore unicamente il materiale predeterminato da lui voluto, senza alcuna possibilità di scaricare la restante documentazione presente sul disco rigido.

Orbene, il Tribunale di Lecce ha totalmente omesso di considerare le suddette circostanze indicate dalla difesa, sebbene le stesse fossero certamente rilevanti perché astrattamente idonee ad incidere sulla qualificazione giuridica del fatto e perché l'eventuale configurabilità del delitto di cui al comma 4 dell'art.600-*ter* c.p.p. al posto di quello contestato avrebbe escluso la possibilità di mantenere il vincolo cautelare, per carenza del presupposto costituito dal limite edittale della pena in astratto comminata.

È comunque manifestamente illogica l'affermazione che il possesso di un *software* idoneo a controllare l'accesso alle proprie porte sia indizio non già di selezione negli accessi bensì di accesso indiscriminato da parte di terzi ai propri documenti.

[…]

L'ordinanza impugnata deve pertanto essere annullata con rinvio per nuovo giudizio al Tribunale di Lecce, che si uniformerà ai principi di diritto enunciati.

[…]

5. DIRITTI E LIBERTA' IN RETE: LIBERTA' DI ESPRESSIONE

5.1. Linguaggio offensivo e indecente in Rete e libertà di parola

Corte Suprema degli Stati Uniti, 26 giugno 1997, no. 96/511 (*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.

(h) The Government's argument that this Court should preserve the CDA's constitutionality by honoring its severability clause, §608, and by construing nonseverable terms narrowly, is acceptable in only one respect. Because obscene speech may be banned totally, see *Miller* […] and §223(a)'s restriction of "obscene" material enjoys a textual manifestation separate from that for "indecent" material, the Court can sever the term "or indecent" from the statute, leaving the rest of §223(a) standing.

(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.

5.2. Pedopornografia in Rete e libertà di parola

Corte Suprema degli Stati Uniti, 16 aprile 2002, no.00-795 (*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, *e.g., 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, *e.g., 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.**

5.3. Minacce in Rete e libertà di espressione

Corte di Appello degli Stati Uniti, 9th Circuit, 16 maggio 2002, no. 99-35320

[…]

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.

[…]

5.4. Libertà di espressione e sequestro di pagine *web*

Corte di Cassazione, sez.V penale, 10 marzo 2009, n.10535

[…]

Con ordinanza 25 ottobre 2007 il giudice per le indagini preliminari del Tribunale di Catania respinse la richiesta dell'ADUC di revoca del sequestro preventivo di alcune pagine *web* di sua proprietà disposto il 20 novembre 2007 in relazione al reato di cui all'art.403 c.p.. Il Tribunale del riesame di Catania, con l'ordinanza in epigrafe, in parziale accoglimento dell'appello dell'ADUC, revoca il sequestro previa rimozione sul sito Internet dell'ADUC delle espressioni e dei messaggi oggetto dei reati contestati, inibendone l'ulteriore diffusione.

L'ADUC propone ricorso per Cassazione deducendo:

1) inosservanza dell'art.21, comma 6, Cost. e illegittimità del sequestro preventivo poiché non attiene a reati contro il buon costume. Osserva che l'art.21, comma 6, Cost. consente la limitazione dell'esercizio della libertà di manifestazione del pensiero nei soli casi di manifestazioni contrarie al buon costume;

2) inosservanza dell'art.21, comma 6, Cost. e illegittimità del sequestro preventivo perché l'offesa ad una confessione religiosa non è contraria al buon costume;

3) erronea applicazione dell'art.403 c.p. per erronea individuazione del bene giuridico protetto dalla norma. Osserva che, secondo un'interpretazione costituzionalmente orientata, non c'è offesa se non vengono individuati i singoli individui, soggetti passivi della norma e portatori del bene giuridico da essa tutelato;

4) erronea applicazione dell'art.21, comma 3, Cost. ed erronea individuazione dell'ambito applicativo del divieto di sequestro ivi previsto. Erronea interpretazione restrittiva del concetto di stampa che esclude l'informazione non ufficiale.

Motivi della decisione

Il primo motivo è inammissibile perché consiste in una censura nuova non dedotta con l'appello, e che non può quindi essere proposta per la prima volta in questa sede di legittimità.

Il motivo è comunque manifestamente infondato perché l'art.21, comma 6, Cost. vieta direttamente "le pubblicazioni a stampa, gli spettacoli e tutte le altre manifestazioni contrarie al buon costume", disponendo altresì che "la legge stabilisce provvedimenti adeguati a prevenire e a reprimere le violazioni", ma non ha inteso dire che un comportamento, costituente manifestazione del pensiero, possa essere dalla legge vietato e previsto come reato esclusivamente quando sia contrario al buon costume, e non anche quando sia lesivo di altri beni ritenuti meritevoli di tutela, sebbene non lesivo del buon costume. Se così non fosse, del resto, dovrebbe ritenersi che i reati di ingiuria e diffamazione non sarebbero legittimi quando colpiscano comportamenti lesivi solo dell'onore e della reputazione delle persone, e non anche del buon costume.

Per le stesse ragioni è inammissibile, sia perché nuovo sia perché manifestamente infondato, anche il secondo motivo. Con l'atto di appello, invero, non era stato dedotto che il sequestro in questione era illegittimo perché le frasi contestate non erano suscettibili di offendere il buon costume inteso come pudore sessuale della collettività. Né tale doglianza può essere proposta per la prima volta in sede di legittimità solo perché l'ordinanza impugnata ha osservato che alcune delle frasi incriminate, oltre ad avere offeso la religione cattolica mediante il vilipendio dei suoi fedeli e dei suoi ministri, avevano travalicato i limiti del buon costume alludendo espressamente a pratiche pedofile dei sacerdoti per diffondere il "sacro seme del cattolicesimo". In ogni caso il motivo è manifestamente infondato perché l'art.21, comma 6, Cost. non limita la possibilità della legge di prevedere, in caso di reato, il sequestro di cose che rappresentino manifestazioni del pensiero soltanto quando queste siano lesive del pudore sessuale.

Il terzo motivo è infondato perché esattamente il Tribunale del riesame ha ritenuto che per la configurabilità del reato di cui all'art.403 c.p. non occorre che le espressioni di vilipendio debbano essere rivolte a fedeli ben determinati, ben potendo invece, come nella specie, essere genericamente riferite all'indistinta generalità dei fedeli. La norma invero protegge il sentimento religioso di per sé, sanzionando le pubbliche offese verso lo stesso attuate mediante vilipendio dei fedeli di una confessione religiosa, o dei suoi ministri.

Opportunamente, invero, l'ordinanza impugnata ha ricordato la sent. n.188/1975 della Corte costituzionale, la quale affermò che "il sentimento religioso, quale vive nell'intimo della coscienza individuale e si estende anche a gruppi più o meno numerosi di persone legate tra loro dal vincolo della professione di una fede comune, è da considerare tra i beni costituzionalmente rilevanti, come risulta coordinando gli artt.2, 8 e 19 Cost., ed è indirettamente confermato anche dal comma 1 dell'art.3 e dall'art.20. Perciò il vilipendio di una religione, tanto più se posto in essere attraverso il vilipendio di coloro che la professano o di un ministro del culto rispettivo, come nell'ipotesi dell'art.403 c.p., che qui interessa, legittimamente può limitare l'ambito di operatività dell'art.21: sempre che, beninteso, la figura della condotta vilipendiosa sia circoscritta entro i giusti confini, segnati, per un verso, dallo stesso significato etimologico della parola (che vuol dire "tenere a vile", e quindi additare al pubblico disprezzo o dileggio), e per altro verso, dall'esigenza di rendere compatibile la tutela penale accordata al bene protetto dalla norma in questione con la più ampia libertà di manifestazione del proprio pensiero in materia religiosa", e che "il vilipendio, dunque, non si confonde né con la discussione su temi religiosi, così a livello scientifico come a livello divulgativo, né con la critica e la confutazione pur se vivacemente polemica; né con l'espressione di radicale dissenso da ogni concezione richiamantesi a valori religiosi trascendenti, in nome di ideologie immanentistiche o positivistiche od altre che siano. Sono, invece, vilipendio, e pertanto esclusi dalla garanzia dell'art.21 (e dell'art.19), la contumelia, lo scherno, l'offesa, per dir così, fine a se stessa, che costituisce ad un tempo ingiuria al credente (e perciò lesione della sua personalità) e oltraggio ai valori etici di cui si sostanzia ed alimenta il fenomeno religioso, oggettivamente riguardato".

D'altra parte, anche la recente sent. n.168/2005 (che ha dichiarato l'illegittimità costituzionale dell'art.403 c.p. nella parte in cui prevede, per le offese alla religione cattolica mediante vilipendio di chi la professa o di un ministro del culto, la pena della reclusione rispettivamente fino a due anni e da uno a tre anni, anziché la pena diminuita stabilita dall'art.406 dello stesso codice) ha fatto espresso riferimento alle "esigenze costituzionali di eguale protezione del sentimento religioso che sottostanno all'equiparazione del trattamento sanzionatorio per le offese recate sia alla religione cattolica, sia alle altre confessioni religiose", ribadendo che tutte le norme contemplate dal capo dei delitti contro il sentimento religioso "si riferiscono al medesimo bene giuridico del sentimento religioso, che l'art.403 c.p. tutela in caso di offese recate alla religione cattolica mediante vilipendio di chi la professa o di un ministro del culto".

Del resto, anche qualora potesse accogliersi la tesi del ricorrente secondo cui il bene tutelato dalla norma non è il sentimento religioso ma la persona (fisica o giuridica) offesa in quanto appartenente ad una determinata confessione religiosa, non si vedrebbe perché questa tesi dovrebbe comportare che, per aversi reato, il vilipendio dovrebbe rivolgersi verso determinate persone e non verso il gruppo indistinto dei fedeli di quella confessione religiosa nei cui confronti viene pubblicamente portata l'offesa.

È infine infondato anche il quarto motivo. Va preliminarmente osservato che il Tribunale del riesame ha revocato il sequestro del *forum* esistente nell'ambito del sito appartenente all'associazione ricorrente, lasciandolo esclusivamente sui singoli messaggi inviati da alcuni partecipanti al *forum* in questione, contenenti le frasi oggetto dei reati contestati. Ciò posto, il Collegio ritiene che esattamente il Tribunale del riesame ha dichiarato che nel caso di specie non trova applicazione l'art.21, comma 3, Cost., secondo cui "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", dato che la concreta fattispecie in esame non rientra nella più specifica disciplina della libertà di stampa, ma solo in quella più generale di libertà di manifestazione del proprio pensiero di cui all'art.21, comma 1, Cost..

Gli interventi dei partecipanti al *forum* in questione, invero, non possono essere fatti rientrare nell'ambito della nozione di stampa, neppure nel significato più esteso ricavabile dall'art.1 della legge 7 marzo 2001, n.62, che ha esteso l'applicabilità delle disposizioni di cui all'art.2 della legge 8 febbraio 1948, n.47 (legge sulla stampa) al "prodotto editoriale", stabilendo che per tale, ai fini della legge stessa, deve intendersi anche il "prodotto realizzato … su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico".

Il semplice fatto che i messaggi e gli interventi siano visionabili da chiunque, o almeno da coloro che si siano registrati nel *forum*, non fa sì che il *forum* stesso, che è assimilabile ad un

gruppo di discussione, possa essere qualificato come un prodotto editoriale, o come un giornale *online*, o come una testata giornalistica informatica. Si tratta quindi di una semplice area di discussione, dove qualsiasi utente o gli utenti registrati sono liberi di esprimere il proprio pensiero, rendendolo visionabile a tutti gli altri soggetti autorizzati ad accedere al *forum*, ma non per questo il *forum* resta sottoposto alle regole ed agli obblighi cui è soggetta la stampa (quale quello di indicazione di un direttore responsabile o di registrazione) o può giovarsi delle guarentigie in tema di sequestro che l'art.21, comma 3, Cost. riserva soltanto alla stampa, sia pure latamente intesa, ma non genericamente a qualsiasi mezzo e strumento con cui è possibile manifestare il proprio pensiero. D'altra parte, nel caso in esame, neppure si tratta di un *forum* strutturalmente inserito in una testata giornalistica diffusa per via telematica, di cui costituisca un elemento e su cui il direttore responsabile abbia la possibilità di esercitare il controllo (così come su ogni altra rubrica della testata).

Acutamente il difensore del ricorrente sostiene che la norma costituzionale dovrebbe esser interpretata in senso evolutivo per adeguarla alle nuove tecnologie sopravvenute ed ai nuovi mezzi di espressione del libero pensiero. Ma da questo assunto, non può farsi derivare che i nuovi mezzi di comunicazione del proprio pensiero (*newsletter*, *blog*, *forum*, *newsgroup*, *mailing list*, *chat*, messaggi istantanei, e così via) possano, tutti in blocco, solo perché tali, essere inclusi nel concetto di stampa ai sensi dell'art.21, comma 3, Cost., prescindendo dalle caratteristiche specifiche di ciascuno di essi.

In realtà i messaggi lasciati su un *forum* di discussione (che, a seconda dei casi, può essere aperto a tutti indistintamente, o a chiunque si registri con qualsiasi pseudonimo, o a chi si registri previa identificazione) sono equiparabili ai messaggi che potevano e possono essere lasciati in una bacheca (sita in un luogo pubblico, o aperto al pubblico, o privato) e, così come quest'ultimi, anche i primi sono mezzi di comunicazione del proprio pensiero o anche mezzi di comunicazione di informazioni, ma non entrano (solo in quanto tali) nel concetto di stampa, sia pure in senso ampio, e quindi ad essi non si applicano le limitazioni in tema di sequestro previste dalla norma costituzionale.

Il ricorso deve pertanto essere rigettato con conseguente condanna del ricorrente al pagamento delle spese processuali.

[…]

6. DIRITTI E LIBERTA' IN RETE: LIBERTA' DI INFORMAZIONE

6.1. Diffamazione su *blog* e responsabilità

Tribunale penale di Aosta, 26 maggio 2006, n.553

[…]

Due sono gli ordini di problemi che vanno risolti nel presente procedimento:

a) se gli articoli diffamatori pubblicati sul *blog* "ilbolscevicostanco.com" siano riconducibili all'attuale imputato (e quindi, per l'effetto, se l'attuale imputato si identifichi col Generale Zhukov e se questi fosse, in sostanza, il direttore del *blog*);

b) se gli articoli siano diffamatori.

Sono stati raggiunti gravi, precisi e concordanti indizi che consentono, con piena certezza, di affermare che il Generale Zhukov, proprietario del sito "il bolscevico stanco" è TIZIO.

Infatti:

1) Come si legge nell'allegato 8/A, fg 50, prodotto dal P.M. tale "soldatino popov" scrive alcune righe, che qui non interessano, al compagno generale.

A queste righe risponde TIZIO. Successivamente taluno si rivolge al compagno generale riprendendo il contenuto della risposta di TIZIO e dicendo a TIZIO: "proprio tu, generale, vai ad elemosinare." Si tratta di un indizio grave in quanto consente di dedurre un'equivalenza generale Zhukov = TIZIO, e preciso, derivando da due fonti diverse in modo univoco. Non è una prova, in quanto non vi è garanzia assoluta della rispondenza a realtà della firma TIZIO e di quanto indicato da altra non controllabile fonte, sicché non consente di raggiungere da sé solo la certezza del fatto che si vuole provare.

2) A casa di TIZIO è stato trovato l'*username* e la *password*, nonché ogni istruzione per la gestione del sito […].

Si è qui in presenza di un indizio gravissimo e ben preciso, atteso che *username* e *password* sono privati del soggetto cui pervengono. Non si tratta di prova diretta poiché da ciò solo non è possibile dedurre la penale responsabilità per gli articoli diffamatori (dando per un attimo già dimostrato che diffamatori essi siano). In sé, non è infatti impossibile che il foglio sia stato dimenticato da altri.

3) La *password* per l'accesso è "violaa". La figlia dell'imputato si chiama Viola […].

È un indizio grave, perché consente di dedurre che la *password* è verosimilmente stata elaborata dall'imputato, e preciso, limitatamente alla sua portata, in quanto non contraddetto da altri elementi intrinseci allo stesso.

4) Sono stati rinvenuti appunti manoscritti per l'accesso del sito, riconducibili all'imputato.

Trattasi di un ulteriore indizio dell'interessamento personale ai modi di accesso e gestione del sito, indizio grave in quanto direttamente legato ai fatti criminosi *de quibus* e preciso in quanto in sé coerente.

5) Una serie di articoli (precisamente messaggio di Capodanno e Velina Rosa 5 e 6) sono stati creati subito prima sul computer dell'imputato e poi pubblicati sul *blog de quo*.

La data era correttamente impostata sul computer del TIZIO […]. È, anche questo, un indizio gravissimo in quanto pone un pesante elemento di collegamento tra l'articolo (quella che interessa è la Velina Rosa 5) e l'imputato, e preciso in quanto dotato di intrinseca coerenza logica.

6) Pur di contorno è un elemento indiziario anche il fatto che si sia trovato presso il TIZIO un libro dal quale era tratta una foto pubblicata sul sito.

È fin troppo chiaro, e sembra quasi offensivo al senso comune spendere troppe parole al riguardo, che tali indizi sono assolutamente concordanti e permettono di collegare con certezza le affermazioni diffamatorie in imputazione (contenute nella "Velina Rosa 5") al TIZIO.

Ritenendo il contrario occorrerebbe immaginare che taluno, per caso, lasci a casa del TIZIO *password* e *username* per l'accesso come Zhukov e la gestione del *blog*; che, sempre per caso, la *password* coincida, con l'aggiunta di una A finale, col nome di battesimo della figlia dell'imputato (Viola - nome tutt'altro che comune); che il TIZIO preferisca subire personalmente le conseguenze penali delle condotte del generale Zhukov piuttosto che rivelare chi abbia lasciato tali documenti presso di lui; che, per motivi non individuabili nemmeno con sforzo di immaginazione, il TIZIO abbia poi deciso di prendere appunti per l'accesso e la gestione del *blog*; che, sempre per caso, 3 articoli, tra cui quello che interessa, siano stati creati col computer del TIZIO; che, ancora per caso,

un libro con una foto pubblicata sul *blog* fosse a casa del TIZIO e che infine soggetti scellerati, diversi dal TIZIO, abbiano usato il suo nome in un'occasione sul *blog*, per rispondere al soldatino Popov e che altri abbiano dato per scontata, senza ragione, l'identità Zhukov = TIZIO.

A corollario si aggiunga che il TIZIO esercita (o esercitava) la professione di giornalista, tanto da essere stato Vice Presidente del Consiglio dell'Ordine Valdostano e che era alquanto apprezzato […] per la sua vena ironica e che - infine - nella predetta qualità, era a conoscenza di procedimenti disciplinari a carico di colleghi per essersene occupato, tanto da detenere tutt'ora copie di atti in casa.

E trattasi di atti sui quali sono basate le considerazioni assunte diffamatorie a carico del Quinto e della Caia.

Da questo corposissimo coacervo di elementi, non credendo questo giudicante che la loro esistenza e coerenza possa essere dovuta a potenti forze esoteriche che perseguitano il TIZIO deve necessariamente concludersi che:

a) il generale Zhukov si chiama, all'anagrafe, TIZIO;

b) questi gestiva il *blog de quo*, tanto che tra le istruzioni da lui detenute vi è un foglio relativo alla cancellazione dei commenti;

c) la Velina Rosa 5 è stata scritta da TIZIO.

Il contenuto pubblicato su Internet e oggetto di contestazione *ex* art.595 c.p. è pacifico.

[…]

Da notare che la parte iniziale delle "osservazioni" sul XXXX è pubblicata sotto lo pseudonimo *Anonymous*.

Va subito rilevato che, essendosi provato *ut supra* che il TIZIO era il soggetto che aveva in disponibilità la gestione del *blog*, egli risponde *ex* art.596-*bis* c.p., essendo la sua posizione identica a quella di un direttore responsabile.

O, meglio, colui che gestisce il *blog* altro non è che il direttore responsabile dello stesso, pur se non viene formalmente utilizzata tale forma semantica per indicare la figura del gestore e proprietario di un sito Internet, su cui altri soggetti possano inserire interventi.

Ma, evidentemente, la posizione di un direttore di una testata giornalistica stampata e quella di chi gestisce un *blog* (e che, infatti, può cancellare messaggi) è - *mutatis mutandis* - identica.

Il gestore di un *blog* ha infatti il totale controllo di quanto viene postato e, per l'effetto, allo stesso modo di un direttore responsabile, ha il dovere di eliminare quelli offensivi.

Diversamente, vi è responsabilità penale *ex* art.596-*bis* c.p.

[…]

In ogni caso, tenuto conto del carattere satirico della pubblicazione e del fondo di verità in linea generale ravvisabile in quanto esposto, va applicata la pena pecuniaria.

[…]

P.Q.M.

Visti gli artt. 533-535 c.p.p. dichiara TIZIO colpevole dei reati a lui ascritti […] e lo condanna alla pena di euro 3.000 di multa, oltre spese processuali. Visti gli artt. 538 ss. c.p.p. condanna il medesimo al risarcimento dei danni tutti patiti dalle p.c., liquidati in euro 2.000 per ciascuno.

[…]

6.2. Testate giornalistiche *online* e registrazione

Tribunale penale di Modica, 8 maggio 2008

[…]

All'odierno imputato è stato contestato il reato di cui agli artt.5 e 16 della legge n.47 dell'8 febbraio 1948 per avere intrapreso la pubblicazione del giornale di informazione civile denominato "Accade in Sicilia" e diffuso, con registrazione avvenuta il 16 dicembre 2003, sul sito Internet *www.accadeinsicilia.net*. senza che fosse stata eseguita la registrazione presso la cancelleria del Tribunale di Modica, competente per territorio.

In diritto occorre preliminarmente osservare che l'art.5 della legge 47/1948 stabilisce che nessun giornale o periodico può essere pubblicato se non sia stato preventivamente registrato presso la cancelleria del Tribunale, nella cui circoscrizione la pubblicazione deve effettuarsi. Il successivo art.16 dello stesso testo normativo punisce penalmente chiunque intraprenda la pubblicazione di un giornale ovvero di un periodico, senza che sia stata eseguita la suddetta registrazione.

Va chiarito che il provvedimento di registrazione consiste in un mero controllo di legittimità della regolarità formale dei documenti prodotti e della rispondenza del loro contenuto alle disposizioni di legge. La registrazione di un periodico, quindi, non costituisce un limite preventivo alla libertà di stampa, essendo esclusa nell'emissione del suddetto provvedimento ogni valutazione discrezionale circa l'opportunità di consentire o meno la pubblicazione.

La finalità della registrazione è unicamente quella di garantire la repressione degli abusi e di individuare i soggetti responsabili di eventuali illeciti commessi a mezzo stampa. Essa rappresenta soltanto una condizione di legittimità della pubblicazione, la cui mancanza dà luogo al reato di stampa clandestina.

D'altro canto anche la Corte costituzionale con sent. n.2/1971 ha escluso che le disposizioni in esame compromettano le libertà riconosciute e garantite dall'art.21 Cost., avendo ivi affermato che l'obbligo della registrazione riguarda esclusivamente i giornali quotidiani o periodici, sicché non pone alcuno ostacolo a che un soggetto manifesti il proprio pensiero con singoli stampati o con numeri unici.

Peraltro deve precisarsi che, sulla scorta di fondamentali enunciati del Giudice costituzionale (sent. Corte cost. n.826 del 14 luglio 1988), la nozione di libertà di manifestazione del pensiero fa oggi riferimento non solo alla libertà di colui che intende avvalersene in senso attivo, ma anche al diritto dei destinatari del messaggio comunicativo.

Pertanto, al fine di assicurare un equilibrio tra queste due posizioni, entrambe costituzionalmente protette, appare legittimo l'intervento del legislatore volto a regolare l'esercizio dell'attività d'informazione.

Ciò posto, occorre rilevare che, sino all'entrata in vigore della legge 62/2001, il prevalente orientamento giurisprudenziale aveva adottato un'interpretazione restrittiva dell'art.1 della legge 47/1948, ritenendo che, affinché una pubblicazione potesse essere ricompresa nella nozione di prodotto editoriale di cui alla citata disposizione, dovesse necessariamente sussistere il requisito ontologico della riproduzione del giornale su supporto cartaceo.

Secondo tale orientamento veniva esclusa la possibilità di estendere ai giornali telematici le disposizioni relative alla registrazione previste per la stampa periodica.

Infatti la legge 47/1948 all'art.1 statuiva che, ai fini della suddetta legge, per stampa o stampati dovessero considerarsi tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico chimici, in qualsiasi modo destinate alla pubblicazione

Solo successivamente con la legge 62/2001 il legislatore ha esteso il concetto di prodotto editoriale, ricomprendendo in esso non solo il prodotto realizzato su supporto cartaceo, ma anche quello realizzato su supporto informatico destinato alla pubblicazione anche con mezzo elettronico, ed ha, conseguentemente, esteso l'applicazione degli artt.2 e 5 della legge 47/1948 anche ai giornali e periodici cd. telematici. Ed invero la nuova legge all'art.1, comma 1, statuisce che *per prodotto editoriale, ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o*

attraverso la radiodiffusione sonora e televisiva, con esclusione dei prodotti discografici o cinematografici" e stabilisce al successivo comma 3 che *"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 identìficativo del prodotto, è sottoposto, altresì, agli obblighi previsti dall'art.5 della medesima legge 47/1948".*

A seguito dell'entrata in vigore della suddetta legge si sono affermati due contrapposti orientamenti interpretativi circa l'ambito di applicazione del menzionato testo normativo. Secondo l'interpretazione fornita da alcuni autori il regime prescritto dall'art.1 della legge 62/2001 troverebbe applicazione solo per coloro i quali intendono usufruire delle agevolazioni previste dalla medesima legge. Diversamente secondo altra parte della dottrina e secondo la giurisprudenza di merito (Trib. Milano, II sez. civile, 16 maggio 2006 n.6127; Tribunale Salerno, 16 marzo 2001; Tribunale Latina, 7 giugno 2001) la norma, che accomuna in un sistema unitario la carta stampata e i nuovi *media,* ha valore generale, così da poter affermare l'assoluta equiparabilità di un sito Internet ad una pubblicazione a stampa, anche con riferimento ad un eventuale sequestro di materiale «incriminato».

Questo giudicante ritiene di aderire al secondo orientamento dianzi illustrato in quanto lo stesso, oltre che più razionale da un punto di vista sistematico, appare peraltro confermato dal fatto che il titolo della legge del 2001 reca *"Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n.416",* il che lascia intuire che l'intenzione del legislatore non fosse solo quella di dettare regole sulle provvidenze, ma anche di introdurre modifiche attinenti all'intero settore dell'editoria.

Pertanto l'inciso contenuto nell'art.1 della legge in esame "ai fini della presente legge" avrebbe valore generale e non limitato all'erogazione dei contributi.

Orbene, alla luce della suddetta normativa, al prodotto editoriale, per come definito dal comma 1 dell'art.1 della legge 62/2001, si applicano le disposizioni di cui all'art.2 della legge 47/1948, mentre i prodotti editoriali diffusi al pubblico con periodicità regolare e contraddistinti da una testata sono ulteriormente sottoposti agli obblighi previsti dall'art.5 della medesima legge 47/1948.

In sintesi devono essere inscritte, nell'apposito registro tenuto dai Tribunali civili, le testate giornalistiche *online* che abbiano le stesse caratteristiche e la stessa natura di quelle scritte o radio-televisive e che, quindi, abbiano una periodicità regolare, un titolo identificativo (testata) e che diffondano presso il pubblico informazioni legate all'attualità. In particolare, le testate telematiche da registrare e perciò sottoposte ai vincoli rappresentati dagli artt.2, 3 e 5 della legge 47/1948 sulla stampa sono quelle pubblicate con periodicità (quotidiana, settimanale, bisettimanale, trisettimanale, mensile, bimestrale) e caratterizzate dalla raccolta, dal commento e dall'elaborazione critica di notizie destinate a formare oggetto di comunicazione interpersonale, dalla finalità di sollecitare i cittadini a prendere conoscenza e coscienza di fatti di cronaca e, comunque, di tematiche socialmente meritevoli di essere rese note.

Ed è, altresì, ovvio che il richiamo contenuto nell'art.1, comma 3, della legge 62/2001 agli artt.2 e 5 della legge 47/1948 implica automaticamente il richiamo anche all'art.16 della stessa legge e, quindi, alle sanzioni penali prescritte per l'ipotesi di inottemperanza alle disposizioni di cui agli artt.2 e 5. Sicché l'art.16 della legge sulla stampa si applica anche ai giornali telematici non già in via analogica, come da alcuni sostenuto, ma perché è lo stesso legislatore che rinvia a detta disposizione nel momento in cui impone alle testate periodiche l'obbligo della registrazione.

D'altra parte diversamente opinando sarebbe irragionevole prevedere ed imporre anche ai periodici telematici gli stessi obblighi prescritti per la stampa ed escludere l'irrogazione delle sanzioni penali fissate per l'inosservanza dei suddetti obblighi.

Detto quadro normativo, per quello che in questa sede interessa, non è stato intaccato dall'entrata in vigore del d.lgs. 70/2003, il quale, per come risulta dalla stessa rubrica del decreto, disciplina esclusivamente "i servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico".

Le finalità della nuova normativa sono rese esplicite dal comma 1 dell'art.1 del d.lgs. 70/2003 e consistono nella promozione della libera circolazione dei servizi della società dell'informazione (SSI), e segnatamente nell'attività di commercio elettronico.

Tale normativa, da un punto di vista oggettivo e per come stabilito dall'art.2 dello stesso decreto, si riferisce a *"qualsiasi servizio della società dell'informazione, vale a dire qualsiasi*

servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi".

Sostanzialmente, rientra nell'ambito regolato dalla nuova disciplina il cd. commercio elettronico, inteso quale attività di contrattazione telematica e relative operazioni propedeutiche, oltre che qualsiasi tipo di servizio, che comunque costituisca un'attività economica.

In relazione, poi, all'ambito soggettivo di applicazione, tre sono le definizioni rilevanti. Il *«prestatore»,* che viene definito, sempre dall'art.2, come la persona fisica o giuridica che presta un servizio per la società dell'informazione (SSI); il *«destinatario del servizi»* quale soggetto che, a scopi professionali e non, utilizza un SSI, in particolare per ricercare o rendere accessibili informazioni; il *«consumatore»* come qualsiasi persona fisica o giuridica che agisca con finalità non riferibile all'attività commerciale, imprenditoriale o professionale eventualmente svolta.

Deve di conseguenza concludersi che il decreto legislativo in parola regola esclusivamente l'attività di prestazione di servizi di informazione, resa dalle società di informazione e da coloro che prestano servizi per le suddette società, mentre non si applica al singolo che svolge l'attività d'informazione non in forma commerciale e, quindi, non in qualità di prestatore di servizi nel senso dianzi delineato.

A tal fine va anche evidenziato che l'art.1, ultimo periodo, della legge 62/2001 risulta immutato e non è stato abrogato dal d.lgs. 70/2003, né la norma contenuta nel comma 3 dell'art.7 può essere considerata norma di interpretazione autentica del citato art.1 della legge 62/2001, essendo il decreto legislativo in commento applicativo, nell'ambito dell'ordinamento interno, di una direttiva comunitaria, la quale, al momento della sua emanazione, non poteva, evidentemente, avere a riferimento la legislazione interna preesistente.

L'orientamento che, al momento dell'entrata in vigore della legge 62/2001, interpretava restrittivamente l'art.1, comma 3, ultimo periodo, della legge 62/2001, affermando come in realtà tale norma sancisse l'obbligo di registrazione solo per le testate giornalistiche *online* che volessero accedere ai finanziamenti statali, non è, dunque, condivisibile proprio in ragione dell'emanazione del d.lgs. 70/2003, il quale ha dovuto introdurre, successivamente ed all'uopo, una disposizione *ad hoc*, che, si ribadisce, non è di interpretazione autentica e che esenta dalla registrazione le testate editoriali telematiche riferibili alle società di servizi.

Non può, quindi, sostenersi, *sic et simpliciter,* che l'art.7, comma 3, d.lgs. 70/2003 abbia sostanzialmente sancito l'inoperatività dell'art.1, comma 3, ultimo periodo, della legge 62/2001, facendo salva solo la marginale ipotesi dell'accesso al finanziamento pubblico. Semmai al contrario, avuto riguardo all'oggetto della disciplina del d.lgs. 70/2003 ed alla portata generale dell'art.1, commi 1 e 3, della legge 62/2001, il complesso sistematico delle norme impone un'esegesi delle medesime nel senso che al singolo giornalista, che non svolge la propria attività in forma economica e che non presta servizi in favore di una società di informazione, non può applicarsi la disposizione di cui all'art.7, comma 3, del d.lgs. 70/2003, che esonera dalla registrazione le testate editoriali telematiche che non intendono accedere alle provvidenze di cui alla legge 62/2001, perché tale disposizione riguarda solamente il cd. prestatore di servizi, rimanendo conseguentemente il singolo giornalista sottoposto all'obbligo di cui all'art.1, comma 3 ultimo periodo, della legge 62/2001.

A conferma di quanto sopra asserito (in operatività dell'art.1, comma 3, legge 62/2001) va ulteriormente chiarito che la registrazione cui fa riferimento l'art.7, comma 3, del d.lgs. 70/2003 non può che essere quella da effettuarsi presso il Registro Operatori della Comunicazione (ROC), istituito con la legge 249/1997 (art.16, legge 62/2001), e non quella da effettuarsi ai sensi dell'art.5 della legge 47/1948 (art.1, comma 3, legge 62/2001), essendo la prima sostitutiva della seconda, ai sensi dell'art.16 della legge 62/2001, ed essendo tenute le società dei servizi di informazione, cui si applica il d.lgs. 70/2003 e fatta salva l'esenzione di cui all'art.7, comma 3, del d.lgs. 70/2003, all'iscrizione presso il suddetto registro, anche in funzione sostitutiva della registrazione prevista dall'art.5 della legge 47/1948, quale obbligo connesso al singolo servizio *ex* art.7, comma 1, del d.lgs. 70/2003 e ai sensi del combinato disposto dell'art.16 della legge 62/2001 con l'art.1, comma 6, lett.a), numero 5) della legge 249/1997. Le stesse, infatti, rientrano tra i soggetti individuati all'uopo dalla legge del 1997 e cioè tra *"i soggetti destinatari di concessione ovvero di autorizzazione in base alla vigente normativa da parte dell'Autorità o delle amministrazioni competenti, le imprese concessionarie di pubblicità da trasmettere mediante impianti radiofonici o televisivi o da diffondere su giornali quotidiani o periodici, le imprese di produzione e distribuzione dei programmi radiofonici e televisivi, nonché le imprese editrici di giornali quotidiani, di periodici o*

riviste e le agenzie di stampa di carattere nazionale, nonché le imprese fornitrici di servizi telematici e di telecomunicazioni ivi compresa l'editoria elettronica e digitale".

In conclusione, alla stregua della normativa introdotta con il d.lgs. del 2003, devono iscriversi nel ROC soltanto i soggetti editori che pubblicano una o più testate giornalistiche diffuse al pubblico con regolare periodicità per cui è previsto il conseguimento di ricavi qualora intendono avvalersi delle provvidenze previste dalla legge n.62 del 7 marzo 2001 o che, comunque, ne facciano specifica richiesta.

Tale differenziazione di trattamento per le società di servizi di informazione e per il prestatore di servizi che opera in favore della stessa, i quali qualora non intendano beneficiare del finanziamento pubblico sono esonerati dall'obbligo di iscrizione al ROC, si giustifica in considerazione del fatto che detti enti collettivi sono già sottoposti ad una normativa che consente facilmente di individuarli e, dunque, garantisce la trasparenza ed il controllo sullo svolgimento della loro attività (vedi appunto d.lgs. 70/2003 e segnatamente lo stesso art.7, commi 1 e 2, che impone al prestatore l'obbligo di fornire una serie di dettagliate informazioni circa la propria attività).

Una diversa interpretazione delle disposizioni in commento, a parere di questo Decidente, sarebbe suscettibile di irragionevolezza ed in contrasto con il principio di eguaglianza sancito dall'art.3 Cost..

Difatti, qualora dovesse ritenersi che la disposizione di cui all'art.7, comma 3, del d.lgs. 70/2003 abbia escluso l'obbligo della registrazione di cui all'art.5 della legge 47/1948 per tutti coloro i quali pubblicano un periodico tramite la rete Internet, si creerebbe un'ingiustificata disparità di trattamento tra i giornalisti della carta stampata, i quali soli sarebbero costretti a rispettare il dettato della legge del 1948 sulla stampa, ed i giornalisti telematici i quali, invece, potrebbero pubblicare in rete senza alcuna limitazione e senza alcuna forma di controllo.

Si aggiunga che proprio la pubblicazione di una pagina *web* rappresenta la forma più efficace e potenzialmente più insidiosa di diffusione di una notizia, dato o informazione, giacché tale "luogo" virtuale può essere visitato non solo da colui che è specificamente e direttamente interessato a conoscere una certa notizia, ma può essere visitato anche da soggetti che, inserendo uno o più termini in un motore di ricerca, vengono indirizzati al sito in oggetto.

Al riguardo proprio la Suprema Corte in una recente sentenza ha rilevato come nel caso in cui un utente di Internet "crei o utilizzi uno spazio *web,* la comunicazione deve intendersi effettuata potenzialmente *erga omnes* (sia pure nel ristretto -ma non troppo - ambito di tutti coloro che abbiano gli strumenti, la capacità tecnica e, nel caso di siti a pagamento, la legittimazione a connettersi)" (Cass. pen., 27 dicembre 2000).

Tanto premesso in diritto, nel caso in esame risulta acclarata la sussistenza del reato contestato all'odierno imputato.

Dalla documentazione in atti emerge inequivocabilmente che l'imputato ha pubblicato sul sito Internet denominato *www.accadeinsicilia.net*, un giornale che rientra nel paradigma del prodotto editoriale descritto dall'art.1, comma 3, legge 62/2001.

In primo luogo è lo stesso imputato che, intitolando il proprio prodotto *"Accade in Sicilia giornale di informazione civile",* ha definito e qualificato il proprio prodotto come "giornale diretto a svolgere attività di informazione" e, dunque, come prodotto editoriale.

Ad ulteriore conferma che quanto pubblicato dal Ruta sul sito in parola sia un prodotto editoriale proviene dal contenuto degli articoli in esso pubblicati, i quali hanno ad oggetto fatti di cronaca locale, inchieste giudiziarie, testimonianze dirette e fatti storici (vedi: "omicidi Tumino e Spampinato"; "affare acqua e mafia"; 8 agosto 2003 "emergenze e giustizia il questore Casabona viene trasferito da Ragusa"; 29 giugno 2003 "caso Carbone-Antonveneta. Nell'est siciliano si vilipende la legge fino alla vergogna"; 15 aprile 2003 "Operazione *privè* negli iblei").

In secondo luogo, l'attività istruttoria ha consentito di accertare che il sito Internet creato dall'imputato presentava le caratteristiche di un periodico per la sistematicità con cui veniva aggiornato e con cui venivano pubblicati gli articoli.

Dalle pagine del suddetto giornale rinvenute dalla Polizia Postale di Catania e da quelle già acquisite al fascicolo per il dibattimento si evince chiaramente che gli articoli venivano pubblicati con cadenza giornaliera, dato peraltro confermato, come già anticipato, anche dalla denominazione data dallo stesso imputato di "Giornale" che letteralmente significa quotidiano di informazione" […].

In conclusione, il prodotto pubblicato dal Ruta sul sito Internet denominato *www.accadeinsicilia.net* si inquadra esattamente nell'ambito del prodotto editoriale di cui all'art.1,

commi 1 e 3 del d.lgs. 62/2001 per la cui pubblicazione era necessaria la registrazione presso la cancelleria del Tribunale, non operando nel caso di specie l'esenzione di cui all'art.7, comma 3, d.lgs. 70/2003 perché l'imputato non ha svolto l'attività d'informazione per cui è processo in forma commerciale o comunque economica, né ha operato quale prestatore di servizi per le società di servizi d'informazione.

L'inottemperanza al predetto obbligo, in applicazione di principi di diritto sopra enunciati, integra il reato di cui all'art.16 della legge 47/1948.

In ultimo va chiarito che non assume rilevanza, al fine di escludere la penale responsabilità dell'imputato, l'affermazione resa dallo stesso in sede di spontanee dichiarazioni, secondo cui il prodotto dallo stesso pubblicato non fosse un quotidiano, ma semplicemente un "*blog*" inteso come diario di informazione civile.

Al riguardo giova innanzitutto evidenziare che il "*blog*" è principalmente uno strumento di comunicazione ove chiunque può scrivere ciò che vuole e come tale può anche essere usato per pubblicare un giornale.

Infatti un "*blog*" può anche essere utilizzato come metodo di presentazione di un giornale, cioè di una testata registrata con una sua linea editoriale, per coinvolgere il pubblico.

Pertanto diverso può essere l'uso che si fa del *blog* nel senso che lo si può utilizzare semplicemente come strumento di comunicazione ove tutti indistintamente possono esprimere le proprie opinioni sui più svariati argomenti ed in tal caso non ricorre certamente l'obbligo di registrazione, ovvero come strumento tramite il quale fare informazione.

Nella fattispecie *de qua*, come risulta dalle pagine acquisite agli atti e come ha riferito il teste […], per pubblicare degli articoli sul sito creato dal Ruta era necessario contattare costui e sottoporre alla sua preventiva valutazione l'articolo che si intendeva pubblicare.

Pertanto appare evidente come il sito in questione non fosse un *blog*, al quale chiunque potesse accedere e partecipare al dibattito, ma era un vero e proprio giornale dotato di una testata e di un editore responsabile.

A suggello e conferma di quanto sopra va, del resto, richiamato che lo stesso imputato ha definito la propria pubblicazione come "Giornale di informazione civile".

L'imputato va, quindi, condannato in ordine al reato allo stesso contestato. L'imputato appare meritevole della concessione delle attenuanti generiche attesa la sua incensuratezza.

[…]

6.3. Informazione e istigazione a delinquere in Rete

Tribunale penale di Rovereto, 29 novembre 2007, n.300

[…]

A F.M. viene contestato:

- di aver creato e gestito i domini Internet *Semini.it* e *Mariuana.it* ed i relativi siti attraverso i quali vendeva semi di *cannabis indica* e diffondeva consigli su come utilizzarli per la coltivazione, inneggiando al relativo uso;

- di aver creato il sito *shop.mariuana.it* attraverso cui pubblicizzava e vendeva attrezzature per la coltivazione di piante di *cannabis*;

- di aver creato e gestito il *forum* di discussione all'interno del sito *mariuana.it* attraverso cui gli utenti si scambiavano consigli, immagini ed esperienze relative alla coltivazione.

Attraverso tali condotte, sempre secondo l'accusa, il F. avrebbe posto in essere un'attività di istigazione all'uso illecito di sostanze stupefacenti, inducendo all'uso di *mariuana* ed hashish gli utenti dei siti e gli acquirenti dei prodotti commercializzati. La fattispecie che si assume violata è quindi quella di cui all'art.82 del d.p.r. 309/1990 che sanziona chi pubblicamente istiga all'uso illecito di sostanze stupefacenti ovvero svolge, anche in privato, attività di proselitismo o ancora induce altri all'uso medesimo.

La presente vicenda processuale ha avuto la sua origine da una più ampia indagine (avviata dalla Procura della Repubblica presso il Tribunale di Santa Maria Capua Vetere) generata da una segnalazione relativa ai siti *Semini.it* e *Mariuana.it*. In merito alle attività di indagine sono stati sentiti, nel corso del dibattimento, gli agenti […] i quali hanno riferito che:

- nel sito *Semini.it.* riconducibile all'imputato, erano illustrati e posti in vendita vari tipi di semi di cannabis indica, senza indicazioni o consigli per la relativa coltivazione;

- nel sito *Mariuana.it*., parimenti riconducibile all'imputato, oltre all'illustrazione delle proprietà della cannabis ed alle indicazioni dei contributi scientifici e giuridici connessi erano posti in vendita numerosi oggetti, tra cui strumenti per la coltivazione, termometri, materiale per la realizzazione di serre e *gadgets* sempre riconducibili alla materia;

- nello stesso sito era attivo un *forum* nel cui ambito, previa registrazione, i vari interlocutori si cambiavano idee ed opinioni anche sull'uso di sostanze derivate dalla *cannabis*;

- l'attività del *forum* era regolata da moderatori, tra i quali a volte lo stesso F.;

- attraverso appositi *links* era possibile passare dal sito *Semini* al sito *Mariuana*.

Sulla struttura del sito *Mariuana.it* ha riferito il teste M., il quale ha dichiarato che:

- mentre l'accesso al sito era libero, l'accesso al *forum* era possibile solo previa registrazione;

- l'*home page* del sito aveva un contenuto solo informativo e conteneva estratti di riviste ed articoli in materia di derivati della *cannabis*;

- il *forum* era diviso in sezioni in ciascuna delle quali era possibile, previa registrazione, intervenire e manifestare le proprie opinioni;

- l'intervento del moderatore sulla singola sezione non era di tipo preventivo ma solo successivo.

Si tratta, a questo punto, di verificare se attraverso le attività riconducibili ai siti Internet sopra indicati venissero svolte attività illecite.

Partendo dall'analisi del sito *Semini.it*, risulta acclarato che in esso venivano posti in vendita semi di *cannabis*, oltre ad altri oggetti (termometri, prodotti generici ecc.); la vendita dei semi, come noto, non è in alcun modo sanzionata dalla legge che, viceversa, prevede come ipotesi di reato la coltivazione delle piante, sempre che (come affermato dalla più recente giurisprudenza) non si tratti di mera coltivazione domestica ad uso strettamente personale. L'attività di tal sito, come dichiarato dagli stessi operanti, era peraltro limitata alla semplice esposizione ed illustrazione dei semi e delle relative proprietà (con i relativi costi) e non venivano in quella sede forniti consigli o indicazioni per la successiva coltivazione.

Nel sito *Mariuana.it*, invece, venivano illustrati nella *home page* tematiche di carattere generale attinenti i derivati della *cannabis*; si trovavano pubblicati articoli, sia di carattere scientifico che sociologico, nei quali erano fornite informazioni sul tipo di sostanza, sulla riconosciuta o meno

dannosità per la salute, sull'affermata differenza tra la stessa le droghe cd. "pesanti", sulle proprietà terapeutiche di tipo analgesico, ecc. Nello stesso sito si trovava un *forum* di discussione, aperto ad utenti registrati, nel quale ciascuno dei partecipanti esponeva le proprie opinioni in merito alla tematica dell'uso di *mariuana* o *hashish*; ciascuna delle sezioni era seguita da un moderatore che, di volta in volta, interveniva anche attraverso la rimozione di messaggi.

Ciò posto in fatto, la norma di cui all'art.82 del d.p.r. 309/1990 sanziona le condotte di istigazione all'uso, di proselitismo o di induzione all'uso medesimo. L'unica interpretazione costituzionalmente orientata di tali disposizioni (peraltro fatta propria dalla giurisprudenza di legittimità) è nel senso che assumono penale rilevanza tutte quelle manifestazioni (verbali, scritte, comportamentali) che appaiono oggettivamente dirette a fornire consigli o indicazioni sull'uso o a convincere altri o ancora a far si che il destinatario della comunicazione sia portato ad accettare come valore positivo ed a praticare l'utilizzo di stupefacenti; una lettura più ampia si risolverebbe nel ritenere illecita in radice qualsiasi manifestazione di pensiero circa la non dannosità (o la limitata dannosità) dell'uso, anche come mera affermazione di principio, e finirebbe con il confliggere irrimediabilmente con il canone dettato dall'art.21 Cost.. In una società improntata a principi di laicità quale è quella in cui viviamo risulterebbe difatti impensabile considerare penalmente illecita la semplice manifestazione di un convincimento, ancorché discutibile o non condivisibile, che per l'appunto può assumere tale carattere solo allorché si traduca nel promuovere l'uso di stupefacenti nel senso sopra evidenziato. In altri termini, a giudizio di chi scrive, il carattere di offensività della fattispecie penale di cui si tratta va rinvenuto nel fatto che le condotte descritte siano oggettivamente connotate dalla promozione dell'uso di suggerimenti, consigli (sia per la coltivazione che per l'assunzione) indicazioni e quant'altro denoti che la condotta è posta in essere per determinare o convincere altre persone, ancorché tale finalità non venga in concreto a realizzarsi.

Se questa è l'unica lettura possibile della norma incriminatrice, non può che ritenersi che l'attività del sito *Semini.it* non sia stata connotata nel senso sopra indicato. È difatti accertato che nessun tipo di indicazione veniva in quella sede fornito per la coltivazione di piante né, tanto meno, per la successiva preparazione del prodotto stupefacente ricavabile, né veniva svolta attività di promozione della successiva coltivazione; la conclusione può apparire paradossale, essendo del tutto ragionevole ritenere che l'acquisto di semi di *cannabis* sia diretto alla successiva coltivazione di piante, ma l'ordinamento non attribuisce carattere di penale rilevanza alla vendita (e rispettivamente all'acquisto) di semi per cui, sino a che l'operatore si limiti meramente a porli in vendita, illustrandone le caratteristiche ma senza fornire indicazioni di dettaglio sulla coltivazione, si è in presenza di un'attività del tutto lecita.

La parte generale (*home page*) del sito *Mariuana.it,* come detto, era caratterizzata da un contenuto informativo in cui venivano, in sostanza, pubblicati interventi e contributi improntati alla cultura del cd. antiproibizionismo; per quanto sopra rilevato è del tutto palese che tale tipo di attività, così caratterizzata, è del tutto estranea all'ambito di operatività della fattispecie penale ma resta contenuta nell'ambito della libera manifestazione del pensiero che a ciascuno va doverosamente riconosciuta. La scelta culturale ed ideologica dell'antiproibizionismo (che ciascuno è libero di condividere, contestare od avversare) resta un fatto del tutto estraneo all'ambito di operatività del diritto penale ma resta circoscritta al campo delle opzioni etiche, morali e politiche; di conseguenza il mero fatto di illustrare le ragioni poste a fondamento di tale scelta e di dibatterne non può essere considerato penalmente rilevante.

Nell'ambito del sito *Mariuana.it,* come detto, era altresì operante un *forum* di discussione articolato su sezioni nel quale chiunque, dopo essersi registrato, poteva intervenire, esprimere le proprie idee e talvolta anche condividere, con altri utenti, impressioni ed esperienze relative all'uso personale di derivati della *cannabis*. Si tratta, quindi, di uno spazio aperto al dibattito ed alle opinioni ed esperienze personali (come è nella generalità dei *forum*), in cui ciascuno poteva intervenire ed illustrare il proprio punto di vista, ma in nessun modo è emerso che attraverso tale spazio venissero forniti consigli, indicazioni, suggerimenti o svolta attività di promozione dell'uso di terzi da parte dell'imputato o di soggetti allo stesso riconducibili. Se così è (e le risultanze dibattimentali non consentono altre conclusioni) deve anche in questo caso ritenersi che si resta nell'ambito di attività di manifestazione del pensiero (condivisibili o meno) non sussumibili tra le condotte di istigazione, induzione o proselitismo caratterizzanti la fattispecie di cui all'art.82 del d.p.r. 309/1990.

L'accertamento dibattimentale, in conclusione, ha dimostrato che l'imputato era referente di un sito (*Semini.it*) attraverso cui venivano commercializzati semi di cannabis senza indicazioni sulla successiva coltivazione, attività di per sé lecita; ha inoltre evidenziato che il sito *Mariuana.it* aveva un contenuto di carattere informativo in cui trovavano espressione scelte ed opzioni culturali proprie del movimento antiproibizionistico, attività che, non essendosi tradotta in promozione all'uso di derivati della *cannabis*, non può ritenersi illecita. Nel *forum* di discussione, infine, venivano ospitate le opinioni in materia da parte degli utenti, anch'esse limitate all'ambito dell'espressione del pensiero di per sé non riconducibile alle condotte sanzionate dall'art.82 del d.p.r. 309/1990. Esulando il carattere di illiceità penale, l'imputato va mandato assolto per insussistenza del fatto.

[…]

7. DIRITTI E LIBERTA' IN RETE: DIRITTI ECONOMICI

7.1. 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*.

33. La *Telefónica* ha proposto opposizione avverso tale ordinanza sostenendo che, in conformità alla LSSI, la trasmissione dei dati richiesti dalla *Promusicae* è autorizzata esclusivamente nell'ambito di un'indagine penale o per la tutela della pubblica sicurezza e della difesa nazionale, e non nel contesto di un procedimento civile o a titolo di accertamento preliminare relativo ad un siffatto procedimento. Da parte sua, la *Promusicae* ha affermato che l'art.12 della LSSI deve essere interpretato in conformità a varie disposizioni delle direttive 2000/31/CE, 2001/29/CE e 2004/48/CE, nonché agli artt.17, n.2, e 47 della Carta, ossia testi che non consentono agli Stati membri di limitare l'obbligo di comunicazione dei dati in oggetto solamente ai fini previsti dal disposto di tale legge.

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:

«Se il diritto comunitario, e specificamente gli artt.15, n.2, e 18 della direttiva 2000/31/CE, l'art.8, nn.1 e 2, della direttiva 2001/29/CE, l'art.8 della direttiva 2004/48/CE, nonché gli artt.17, n.2, e 47 della Carta (...), consentano agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale – ad esclusione, quindi, dei processi civili – l'obbligo di conservare e mettere a disposizione i dati sulle connessioni ed il traffico generati dalle comunicazioni effettuate durante la prestazione di un servizio della società dell'informazione, che incombe agli operatori di rete e di servizi di comunicazione elettronica, ai fornitori di accesso alle reti di telecomunicazione ed ai fornitori di servizi di archiviazione di dati».

[…]

Sulla questione pregiudiziale

41. Con la sua questione, il giudice del rinvio chiede in sostanza se il diritto comunitario, e in particolare le direttive 2000/31/CE, 2001/29/CE e 2004/48/CE, lette anche alla luce degli artt.17 e 47 della Carta, vadano interpretati nel senso che impongono agli Stati membri di istituire, al fine di garantire l'effettiva tutela del diritto d'autore, l'obbligo di comunicare taluni dati personali nel contesto di un procedimento civile.

[…]

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 paragrafi 2, 3 e 5 dello stesso articolo e l'art.15, n.1, di tale direttiva.

48. Per quanto riguarda, da un lato, i paragrafi 2, 3 e 5 del detto art.6, inerenti al trattamento dei dati sul traffico riguardo alle prescrizioni connesse alle attività di fatturazione dei servizi, di commercializzazione di questi ultimi o di fornitura di servizi a valore aggiunto, va rilevato che tali disposizioni non riguardano la comunicazione di siffatti dati a persone diverse da quelle che agiscono sotto l'autorità dei fornitori di reti pubbliche di comunicazione elettronica e di servizi di comunicazione elettronica accessibili al pubblico. Quanto alle disposizioni dell'art.6, n.6, della direttiva 2002/58/CE, esse non riguardano controversie diverse da quelle, insorgenti tra i fornitori e gli utilizzatori, relative ai motivi della memorizzazione dei dati avvenuta per attività previste dalle altre disposizioni di tale articolo. Pertanto, poiché le disposizioni del detto articolo, con tutta evidenza, non concernono una situazione come quella in cui si trova la *Promusicae* nel contesto della causa principale, esse non possono essere prese in considerazione per valutare tale situazione.

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 utilizzi 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 utilizzi, 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 garantiscano, 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 paragrafo 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.

59. Neppure il testo degli artt.15, n.2, e 18 della direttiva 2000/31/CE, né quello dell'art.8, nn.1 e 2, della direttiva 2001/29/CE, richiedono che gli Stati membri istituiscano un siffatto obbligo.

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.

62. A tale riguardo va ricordato che il diritto fondamentale di proprietà, di cui fanno parte i diritti di proprietà intellettuale, come il diritto d'autore (v., in tal senso, sent. 12 settembre 2006, causa C-479/04, *Laserdisken* […] p.to 65), e il diritto fondamentale alla tutela giurisdizionale effettiva costituiscono principi generali del diritto comunitario (v. in tal senso, rispettivamente, sentt. 12 luglio 2005, cause riunite C-154/04 e C-155/04, *Alliance for Natural Health e a.* […] p.to 126 e giurisprudenza ivi citata, nonché 13 marzo 2007, causa C-432/05, *Unibet* […] p.to 37 e giurisprudenza ivi citata).

63. Tuttavia, occorre rilevare che nella controversia in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolto, 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 Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, il quale garantisce il diritto al rispetto della vita privata, mentre l'art.8 della Carta proclama espressamente il diritto alla tutela dei dati personali.

65. Pertanto, la domanda di pronuncia pregiudiziale in esame solleva la questione della necessaria conciliazione degli obblighi connessi alla tutela di diversi interessi fondamentali: da una

parte, il diritto al rispetto della vita privata e, dall'altra, i diritti alla tutela della proprietà e ad un ricorso effettivo.

66. I meccanismi che consentono di trovare un giusto equilibrio tra questi diversi diritti e interessi sono contenuti, da un lato, nella stessa direttiva 2002/58/CE, in quanto essa prevede norme che stabiliscono in quali situazioni ed in qual misura il trattamento dei dati personali è lecito e quali salvaguardie devono essere previste, nonché nelle tre direttive menzionate dal giudice del rinvio, che fanno salvo il caso in cui le misure adottate per tutelare i diritti che esse disciplinano inciderebbero sulla tutela dei dati personali. Dall'altro lato, tali meccanismi devono risultare dall'adozione, da parte degli Stati membri, di disposizioni nazionali che garantiscano la trasposizione di queste direttive e dall'applicazione di queste da parte delle autorità nazionali (v. in tal senso, per ciò che riguarda la direttiva 95/46/CE, sent. *Lindqvist*, cit., p.to 82).

67. Per quanto riguarda le dette direttive, le loro disposizioni presentano un carattere relativamente generico, in quanto devono applicarsi a un gran numero di situazioni diverse che possono presentarsi nell'insieme degli Stati membri. Esse contengono quindi logicamente norme che lasciano agli Stati membri il necessario margine di discrezionalità per definire misure di recepimento 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.,* non ancora pubblicata nella Raccolta, 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 paragrafo 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.

[…]

7.2. Diritti d'autore, ruolo del *provider* e tutela della riservatezza

Tribunale di Roma, sez. specializzata in materia di proprietà industriale ed intellettuale, ord. 14 aprile 2010

[…]

Fapav ha agito nei confronti di Telecom Italia s.p.a. (per brevità: Telecom) a tutela dei diritti di autore delle imprese produttrici e distributrici di opere audiovisive in essa associate, esponendo di avere individuato, grazie a ricerche commissionate per accertare la dimensione del fenomeno dell'illecita messa a disposizione in Internet di opere audiovisive protette, siti *web* che vengono utilizzati per tale scopo, alcuni dei quali sono stati oggetto di condanne in altri ordinamenti per la loro attività illecita.

Fapav ha indicato un elenco di tredici siti, attraverso i quali ha riferito essersi verificati, nel periodo settembre 2008 - marzo 2009, per sole 9 pellicole, oltre 2.200.000 accessi illeciti, la gran parte di quali avvenuta mediante connessioni fornite da Telecom.

La ricorrente ha quindi riferito di avere notificato a Telecom, il 25 maggio 2009, una diffida con la quale le ha chiesto di porre in essere le misure tecniche, amministrative e giuridiche necessarie per impedire l'abuso della convenzione Internet da parte di propri abbonati (in particolare, di bloccare l'accesso ai siti usati per l'illecita riproduzione delle opere e di comunicare alle autorità di Pubblica Sicurezza i dati idonei a consentire l'adozione delle misure di competenza di quest'ultima), ricevendo risposta negativa.

Nel perdurare degli accessi illeciti alle opere protette di titolarità dei suoi associati, Fapav ha dunque proposto la presente azione cautelare. Le misure richieste (in vista dell'eventuale proposizione di azione di risarcimento danni nei confronti di Telecom) sono le seguenti:

1. ordine a Telecom di comunicare all'autorità di P.S. tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette dagli artt.171 ss. della legge 633/1941;

2. ordine a Telecom di adottare tutte le misure per impedire ovvero ostacolare l'accesso ai siti in questione;

3. ordine a Telecom di informare i propri utenti in ordine alla natura illecita delle condotte di riproduzione, comunicando altresì che tali condotte costituiscono condotte contrattualmente vietate ai sensi del contratto di accesso ad Internet e, per l'effetto, che la prosecuzione di tali condotte potrà dar luogo alla risoluzione del contratto medesimo;

4. ogni altro provvedimento idoneo a salvaguardare il buon diritto della ricorrente.

Si è costituita in giudizio Telecom contestando il ricorso sotto diversi profili, pregiudiziali e di merito. Sono intervenuti nel procedimento la SIAE, con intervento adesivo al ricorso, e AIP, Assotelecomunicazioni, nonché il Garante per la protezione dei dati personali (Garante) con interventi adesivi alla difesa di Telecom. […]

La contestazione della liceità, *ex* d.lgs. 196/2003, del metodo usato da Fapav per l'accertamento delle violazioni dedotte in giudizio e, pertanto, della possibilità di utilizzare le informazioni riferite dalla ricorrente a fondamento della domanda, formulata dal Garante e dalle resistenti, non è fondata.

Le indagini commissionate da Fapav, il cui risultato è stato dedotto a prova delle violazioni commesse attraverso l'accesso ai siti *web* indicati, hanno ad oggetto dati aggregati (numero degli accessi a ciascuna opera in un determinato periodo di tempo) che non consentono la identificazione di alcun indirizzo IP degli utenti. Gli stessi indirizzi IP usati per fornire il dato aggregato sono stati resi anonimi nel procedimento mediante l'obliterazione di parte del codice che li forma. Quindi non vi è stata, da parte della ricorrente, alcuna acquisizione di conoscenza di dati personali degli utenti, il che è sufficiente ad escludere - in difetto di prova contraria - che vi sia stato alcun "trattamento" di dati, *ex* art.4, lett.a), d.lgs. 196/2003.

Non è fondata nemmeno la contestazione dell'ammissibilità, *ex* d.lgs. 196/2003, della prima delle misure richieste dalla ricorrente (ordine a Telecom di comunicare all'autorità di P.S. tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette dagli artt.171 ss. della legge 633/1941) dal momento che i dati da comunicare non sono indicati e che la ricorrente ha espressamente specificato di non avere inteso includere nella domanda la comunicazione di dati personali.

Fapav ha dedotto, nel ricorso, la responsabilità di Telecom *ex* art.17, comma 3, d.lgs. 70/2003, per la propria condotta agevolatrice delle violazioni dei diritti di autore, derivante dall'inadempimento agli obblighi di protezione nei confronti dei titolari dei diritti sulle opere illecitamente riprodotte in rete sanciti dallo stesso decreto legislativo, ed ha prospettato la successiva instaurazione di un giudizio di risarcimento danni nei confronti della stessa Telecom, in vista del quale ha formulato, attraverso l'azione cautelare in oggetto, la richiesta di far cessare ogni condotta di agevolazione dei diritti delle sue associate.

Le disposizioni normative specificamente invocate dalla ricorrente nell'atto introduttivo del presente procedimento sono le seguenti: art.14, comma 3, art.17, commi 2 e 3, del d.lgs. 70/2003, art.163 della legge 633/1941.

All'esito della discussione, nelle note autorizzate, la ricorrente ha affermato non essere in controversia l'accertamento della responsabilità di Telecom, ma la disponibilità di misure cautelari idonee a tutelare medio tempore il buon diritto della ricorrente - dal momento che la direttiva 2000/31 CE e il d.lgs. 70/03 pongono a carico dei soggetti astrattamente esonerati da responsabilità, perché non si trovano in una situazione di controllo, precisi obblighi di precauzione/protezione - ed ha invocato, altresì, la violazione dell'art.16, comma 1, del decreto legislativo citato.

È necessario chiarire innanzitutto che l'inadempimento agli obblighi di protezione genera responsabilità del prestatore (ossia il soggetto giuridico che presta un servizio della società dell'informazione, nella terminologia del d.lgs. 70/2003, di attuazione della direttiva 2000/31/CE, relativa a taluni aspetti giuridici della società dell'informazione nel mercato interno con particolare riferimento al commercio elettronico) come sancito dall'art.17, ultimo comma, del d.lgs. 70/2003. Quindi è certamente ammissibile una domanda volta ad ottenere la cessazione della violazione degli obblighi di protezione, in quanto agevolatrice dell'illecito commesso dagli utenti, ma occorre stabilire quali siano le misure irrogabili a tal fine, in relazione alla violazione dedotta.

Gli obblighi del prestatore e i limiti delle relative responsabilità in relazione alle violazioni commesse attraverso il servizio prestato sono delineati dagli articoli da 14 a 17 del d.lgs. 70/2003.

Si ricava, dalle disposizioni normative suddette, che il prestatore non ha un obbligo di sorveglianza sulle informazioni trasmesse o memorizzate né un obbligo di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite (art.17, comma 1). Gli articoli 14, commi 1 e 2, 15, comma 1, e 16, commi 1 e 2, limitano a particolari casi la responsabilità, sia civile che penale, del prestatore (rispettivamente di servizi di mero trasporto o di memorizzazione temporanea o permanente di informazioni) per il contenuto delle informazioni trasmesse o memorizzate.

Inoltre tutti i prestatori:

1. sono tenuti ad informare prontamente l'autorità giudiziaria o amministrativa avente funzioni di vigilanza qualora siano a conoscenza di presunte attività o informazioni illecite riguardanti un loro destinatario del servizio della società dell'informazione (art.17, comma 2, lett.a);

2. sono tenuti a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione del destinatario dei loro servizi con cui hanno accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite (art.17, comma 2, lett.b);

3. possono essere destinatari di provvedimenti dell'autorità giudiziaria o amministrativa di vigilanza che richiedano loro, anche in via d'urgenza, di impedire le violazioni commesse (ultimi commi degli artt.14, 15 e 16);

4. sono civilmente responsabili del contenuto dei servizi forniti qualora non abbiano prontamente ottemperato alla richiesta dell'autorità giudiziaria o amministrativa di vigilanza di impedire l'accesso al suddetto contenuto oppure se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicurano l'accesso, non abbiano provveduto ad informarne l'autorità competente (art.17, comma 3).

Gli obblighi appena elencati (da 1 a 3) sono accomunati dall'essere relativi a tutti i prestatori e dall'avere ad oggetto comportamenti di collaborazione con l'autorità giudiziaria o amministrativa di vigilanza investite dell'accertamento delle violazioni commesse attraverso il servizio reso, al fine di prevenire o reprimere tali violazioni. Si tratta di quegli obblighi che possono essere sinteticamente definiti come obblighi di protezione dei diritti suscettibili di violazioni commesse da utenti attraverso il servizio reso dal prestatore. Ad essi possono essere assimilati i particolari obblighi relativi alla prestazione dei servizi di memorizzazione di informazioni (*caching* e *hosting*)

che, pur essendo collocati dal legislatore tra le prescrizioni relative alle modalità di prestazione dei servizi (art.15, comma 1, lett.e, art.16, comma 1), hanno la finalità di impedire la commissione o perpetuazione di illeciti da parte degli utenti del servizio.

Gli obblighi di protezione sorgono, prevalentemente, dalla richiesta della competente autorità giudiziaria o amministrativa con funzioni di vigilanza, la quale chieda che il prestatore impedisca le violazioni commesse (ultimi commi degli artt.14, 15 e 16 cit.) oppure chieda al prestatore di fornire le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione di dati, al fine di individuare o prevenire attività illecite (art.17, comma 2, lett.b).

Tra gli obblighi di protezione peraltro vi è l'obbligo del prestatore di informare senza indugio l'autorità giudiziaria o amministrativa di vigilanza, che sorge in assenza di un provvedimento dell'autorità, dalla "conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione" (art.17, comma 2, lett.a). È un obbligo che evidentemente ha la finalità di rendere effettiva la possibilità di intervento dell'autorità giudiziaria o amministrativa e quindi di sollecitare l'attività di accertamento delle violazioni, nell'ambito della quale potranno eventualmente essere attivati, questa volta dall'autorità stessa, gli ulteriori obblighi di protezione sopra menzionati.

Nel quadro normativo delineato dagli artt.14-17 del d.lgs. 70/2003, le disposizioni applicabili a Telecom, quale fornitrice di un servizio di mera connessione alla rete Internet, sono solamente quelle di cui agli artt.14 e 17, come peraltro puntualmente indicato dalla stessa Fapav nel ricorso introduttivo. Gli artt.15 e 16 sono infatti riferiti ai prestatori di servizi di memorizzazione di informazioni.

Occorre in particolare escludere, a confutazione di quanto dedotto da Fapav nelle note autorizzate, che Telecom abbia l'obbligo di sospendere il servizio di accesso ai siti in questione *ex* art.16, comma 1, per essere stata portata a conoscenza di fatti o circostanze che rendevano manifesta l'illiceità dell'attività dell'informazione. Tale disposizione è infatti applicabile solamente al prestatore di servizi di *hosting*, ossia di memorizzazione permanente di informazioni, consistente nella messa a disposizione di una parte delle risorse di spazio di memoria digitale contenute all'interno di un *server* al fine di rendere visibile su Internet materiale informativo del destinatario del servizio, mentre Telecom fornisce solamente il servizio di connessione, come è pacifico.

Limitato il quadro normativo di riferimento agli artt.14 e 17 d.lgs. 70/2003, deve essere escluso (perché nemmeno dedotto) che Telecom si sia resa responsabile delle informazioni trasmesse per avere svolto nell'illecita trasmissione delle informazioni in questione alcuna delle attività indicate dal comma 1 dell'art.14 come fonte di responsabilità del prestatore (dare origine alla trasmissione, selezionare il destinatario, selezionare o modificare le informazioni trasmesse) che implicano lo svolgimento di un ruolo attivo del prestatore nella specifica comunicazione.

Deve essere anche escluso (perché pure non dedotto) che Telecom abbia ricevuto alcun ordine dell'autorità giudiziaria o amministrativa volto ad impedire le violazioni commesse dagli utenti *ex* art.14, comma 3, e che quindi avesse l'obbligo di sospendere il servizio di accesso ai siti in questione.

Deve essere infine escluso (per la stessa ragione) che Telecom abbia ricevuto dall'autorità giudiziaria o amministrativa alcuna richiesta di informazioni al fine di individuare e prevenire attività illecite *ex* art.17, comma 2, lett.b. Peraltro tale disposizione fa riferimento ai soli dati dell'utente con cui il prestatore abbia accordo di memorizzazione di dati e quindi non è applicabile al prestatore di servizi di mero trasporto.

Pertanto l'unica violazione che sembra potersi ascrivere a Telecom è quella dell'obbligo di informare senza indugio l'autorità giudiziaria (o quella amministrativa avente funzioni di vigilanza) circa le informazioni ricevute attraverso la diffida di Fapav del 25 maggio 2009.

Si trattava infatti di informazioni sufficientemente motivate per essere attendibili e per fornire a Telecom quella conoscenza di "presunte" attività o informazioni illecite riguardanti un suo destinatario del servizio dalla quale l'art.17, comma 1, lett.a) fa scaturire l'obbligo di immediata comunicazione all'autorità competente all'accertamento e repressione dell'illecito.

Ciò significa peraltro che, in presenza della sola informazione ricevuta attraverso la suddetta diffida, Telecom non solo non avrebbe dovuto, ma nemmeno avrebbe legittimamente potuto interrompere il servizio, non essendo responsabile delle informazioni trasmesse, ai sensi dell'art.14, comma 1, citato, ed essendo obbligata contrattualmente alla prestazione.

La responsabilità di Telecom conseguente a tale violazione è la responsabilità civile per il contenuto del servizio sancita dall'art.17, comma 3.

Si tratta di una responsabilità solidale con quella dei titolari dei siti *web* in questione e degli utenti che vi accedono, ma fondata sulla sola violazione dell'obbligo di protezione, quindi su un titolo diverso dall'illecito che gli obblighi di protezione sono finalizzati ad impedire, con quanto ne consegue anche in ordine alla misura della responsabilità (*ex* artt.1223 e 2056 c.c.).

Dalla differenza del titolo da cui deriva la responsabilità di Telecom rispetto a quello da cui deriva la responsabilità dei titolari dei siti *web* in questione e dei relativi utenti discende, come logica conseguenza, l'impossibilità di adottare nei confronti della prima, ed al di fuori di un procedimento di accertamento della violazione commessa dai secondi, quindi necessariamente instaurato nei confronti di questi, le misure finalizzate alla repressione della violazione stessa.

Si deve in particolare escludere che possano essere, in questa sede, adottati i provvedimenti di cui all'ultimo comma dell'art.14, che impongono al prestatore di impedire le violazioni commesse da altri mediante la comunicazione di informazioni attraverso il servizio da esso reso o di porre fine alle violazioni da esso stesso commesse attraverso il servizio (allorché reso in violazione del disposto del comma 1 dell'art.14 o in violazione di un precedente ordine dell'autorità).

Tali provvedimenti, per la natura delle violazioni che sono finalizzati a prevenire o reprimere, sono da ritenere di competenza dell'autorità giudiziaria investita dell'accertamento delle stesse.

Pertanto solo se, nell'ambito dell'attività di accertamento delle violazioni descritte nella diffida di Fapav, l'autorità giudiziaria o amministrativa richieda a Telecom informazioni ulteriori o le richieda di interrompere il servizio di accesso ai siti implicati nelle violazioni, Telecom sarà tenuta a fornire le informazioni ulteriori o a sospendere il servizio di accesso ai siti, e sarà ulteriormente responsabile verso i titolari dei diritti lesi in caso di inottemperanza a tali ordini o richieste delle autorità.

Infine si osserva che l'art.163 della legge 633/1941 (che consente al titolare di un diritto di utilizzazione economica di opere di chiedere che sia disposta l'inibitoria di attività che costituiscano violazione del diritto stesso anche se consistenti in servizi prestati da intermediari) non sancisce *ex novo* le responsabilità dell'intermediario per le violazioni dei diritti di autore commesse attraverso i servizi da lui resi, ma si limita a prevedere la possibilità di inibire la prestazione del servizio da parte dell'intermediario, nell'ambito dell'attività di repressione della violazione del diritto di autore commessa dagli utenti o dal prestatore stesso. Quindi dall'art.163 citato non deriva alcun obbligo di Telecom di interrompere o sospendere il servizio in questione ulteriore rispetto a quelli desumibili dal d.lgs. 70/2003, né alcun potere dell'autorità giudiziaria di inibire la prestazione del servizio nell'ambito di un procedimento giudiziario che non abbia ad oggetto l'accertamento e la repressione delle violazioni dei diritti di autore commesse attraverso il servizio.

In relazione alla responsabilità di Telecom sommariamente accertata, la sola misura cautelare irrogabile al fine di far cessare l'illecito di cui essa si è resa responsabile a danno degli associati Fapav è quella che imponga alla resistente di porre in essere l'attività di informazione sinora omessa, trasmettendo all'autorità giudiziaria ed amministrativa le informazioni ottenute attraverso la diffida di Fapav.

La terza misura cautelare richiesta (ordine a Telecom di informare gli utenti) non può essere invece emessa perché non è in nessun modo rivolta ad ovviare alla specifica violazione ascrivibile a Telecom.

La misura da emanare, in relazione alla violazione sommariamente accertata a carico di Telecom, è l'ordine a quest'ultima di comunicare all'autorità giudiziaria che possa promuovere un procedimento di accertamento delle violazioni dei diritti di autore denunciate da Fapav, ossia la Procura della Repubblica presso il Tribunale di Roma, ed all'autorità amministrativa competente in materia di comunicazioni, ossia il Ministero delle Comunicazioni, tutte le informazioni ricevute da Fapav attraverso la diffida del 23 maggio 2009 relative alle violazioni dei diritti di autore su opere cinematografiche commesse attraverso accessi ai siti *web* indicati nel ricorso, corredate, per completezza dell'informazione, dei dati in possesso di Telecom, diversi dai dati identificativi dei destinatari del servizio, che possano eventualmente essere utili ad integrare le notizie contenute nella diffida.

[…]

7.3. Tutela dei diritti di proprietà intellettuale e anonimato

Tribunale di Roma, sez. specializzata per la proprietà industriale e intellettuale, ord. 17 marzo 2008

[…]

Ritenuto

Sul procedimento: che la *Techland sp.z.o.o*., società con sede in Polonia, di produzione e commercializzazione di *computer games*, e in particolare del gioco *Call of Juarez*, nonché la *Peppermint Jam Records GmbH,* società con sede in Germania, di produzione musicale, in particolare con fonogrammi degli artisti cantanti Mousse, Warren, Roachford e Kakande, agiscono contro Tiscali Italia s.p.a., società *provider* di servizi informatici, domandando al Tribunale un ordine a quest' ultima di fornire le generalità dei soggetti utenti del servizio che hanno effettuato sul sistema Internet il cosiddetto *file-sharing* delle citate opere coperte dal diritto di autore, identificati mediante numeri di protocollo da un'indagine di parte commessa all'impresa svizzera *Logistep*;

- che Tiscali, costituita, chiede la reiezione della domanda, eccependo: in via pregiudiziale l'inammissibilità della domanda per difetto di strumentalità e anticipatorietà rispetto a una domanda nei confronti del *provider*, e l'ineseguibilità del provvedimento in violazione del diritto alla privacy dei consumatori; in via preliminare il difetto di possibilità giuridica della domanda come proposta, di pericolo nel ritardo e di legittimazione del gestore della rete; nel merito la non proteggibilità dei giochi elettronici secondo il diritto di autore e l'inammissibilità della prova del *downloading*, acquisita da parte ricorrente illecitamente in violazione delle regole sulla privacy, nonché il concorso di colpa delle società ricorrenti che non hanno agito nei confronti dei produttori e fornitori dei programmi di *file-sharing*;

- che nel procedimento spiegano intervento autonomo il Garante per la Protezione dei dati personali (d'ora in poi "Garante"), il Codacons (Coordinamento delle Associazioni a tutela dell'Ambiente e dei diritti dei consumatori e degli utenti) e l'Adiconsum (Associazione Difesa Consumatori e Ambiente), associazioni rappresentative dei consumatori (d'ora in poi "Associazioni dei Consumatori"), che tutti domandano la reiezione della domanda, lesiva del diritto alla privacy dei consumatori utenti;

[…];

- che il programma-mezzo per partecipare al P2P è scaricabile dal sistema Internet, e la partecipazione al programma-mezzo permette di accedere ad appositi siti ove praticare il cosiddetto *file-sharing*, e cioè la condivisione diretta di programmi e *files*, contenenti anche opere protette dal diritto di autore, in particolare opere musicali, mediante operazioni di *uploading* e *downloading* degli stessi in rete;

- che l'identificazione degli utenti è data da un *username*, o *nickname*, a cui corrisponde un codice GUID, quella dei *files* mediante il cosiddetto valore *hash* e quella del computer mediante l'indirizzo IP, dati tutti in possesso dei gestori della rete, così come le generalità degli utenti consumatori, che altrimenti restano anonimi;

- che le parti ricorrenti hanno commissionato alla *Logistep*, società di monitoraggio antipirateria, un'indagine, eseguita la quale questa ha identificato una serie di valori *hash*, codici GUID e indirizzi IP, corrispondenti ad altrettanti utenti e *files* contenenti le opere di proprietà delle due società condivise in rete a una data ora;

- che per contro non sono in possesso delle parti ricorrenti le informazioni relative alle generalità dei medesimi utenti, che la parte resistente non contesta essere nella propria disponibilità di fatto, contestandone invece la disponibilità di diritto per essere tali dati riservati, e su questo punto specifico è sorto il conflitto tra le parti portato avanti a questo Tribunale;

- Sulle questioni: che il caso pone numerose questioni, sia pregiudiziali, sia preliminari, rilevabili d'ufficio e sollevate con eccezioni delle parti resistenti e dei terzi intervenuti, e su cui si registrano precedenti, anche contrastanti tra loro di questo Tribunale;

- In particolare sulla questione pregiudiziale di ammissibilità della *discovery*: che la prima questione, pregiudiziale e di rito e rilevabile d'ufficio, è quella dell'ammissibilità della domanda, così come proposta dalla parte ricorrente, collegata altresì alla questione preliminare della

possibilità giuridica dell'azione così come esercitata dalla parte ricorrente, sollevata da parte resistente;

- che la parte ricorrente propone una domanda, da essa qualificata come domanda di *discovery* in via cautelare, il cui *petitum* è costituito dalle informazioni sui dati di consumatori utenti del servizio informatico e utilizzatori dei programmi di *file sharing*, e la *causa petendi* dalla lesione dei diritti di proprietà intellettuale delle società di produzione sulle opere scambiate gratuitamente in rete, e che la parte fonda sugli artt.8.3 della direttiva CE 2001/29/CE (sulla armonizzazione di taluni aspetti del diritto di autore e dei diritti connessi nella società dell'informazione), sugli artt.8, 9 e 11 della direttiva 2004/48/CE (cd. direttiva *enforcement*) e sugli artt.156 e 156-*bis* e 156-*ter* della legge 633/1941 sul diritto di autore;

[…]

- Sulla questione dell'uso della *discovery* per la comunicazione di dati personali, che la questione fondamentale posta dal caso in esame, che è alla base dell'interesse a intervenire del Garante e delle Associazioni dei Consumatori, è quella del conflitto apparente tra la norma dell'art.8 della direttiva *enforcement* e le norme nazionali di recepimento di questa e dunque gli artt.156-*bis* e 156-*ter* richiamati, a tutela dei diritti di proprietà industriale, da un lato, e alcune norme delle direttive CE in materia di società dell'informazione e del d.lgs. 30 giugno 2003 n.196 (codice in materia di protezione dei dati personali, d'ora in poi " Codice della privacy);

- che tale questione è stata risolta con varie oscillazioni dalla giurisprudenza di questo Tribunale ed è stata ora affrontata dalla sentenza della Corte di Giustizia del 29 gennaio 2008 nel procedimento C-275/06 (*Productores de Musica de Espana. Promusicae* contro *Telefonica de Espana SAU*, d'ora in poi caso *Promusicae*), su rinvio pregiudiziale del *Juzgado de lo Mercantil* n.5 de Madrid, pronuncia vincolante per la Corte, quale giudice europeo;

- che il contesto normativo comunitario rilevante può essere ricostruito come segue: l'art.2 della direttiva *enforcement* fa salva l'applicazione delle direttive 95/46/CE, 1999/93/CE e 2000/31/CE; l'art.3 della medesima direttiva prevede che le misure per assicurare il rispetto dei diritti di proprietà intellettuale debbano essere effettive e proporzionate, e il paragrafo 3 dello stesso art.8 fa salve le disposizioni che "e) disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali" e l'art.156, comma 3, prevede che con l'ordine di *discovery* siano adottate "le misure idonee a garantire la tutela delle informazioni riservate";

- che la direttiva 45/96/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, all'art.2 definisce quali " dati personali" "qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata)" anche indirettamente, "mediante riferimento a un numero di identificazione"; e quale "trattamento dei dati personali" ogni forma di messa a disposizione dei dati stessi;

- che la medesima direttiva all'art.7 permette il trattamento dei dati personali "se necessario per il perseguimento dell'interesse legittimo … dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata" e l'art.13, lett.d), permette agli Stati membri di limitare la portata delle norme a protezione dei dati personali se misura necessaria alla salvaguardia "della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate";

- che l'art.1 della direttiva 2000/31/CE, relativa ad alcuni aspetti giuridici dei servizi della società dell'informazione (cd. direttiva sul commercio elettronico) all'art.15.2 prevede la facoltà per gli Stati membri di prescrivere un obbligo dei prestatori di servizi di comunicare "alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati", facoltà di cui lo Stato italiano non si è valso, e all'art.18 prevede misure urgenti anche provvisorie atte "a porre fine alle violazioni e a impedire ulteriori danni agli interessi in causa";

- che la direttiva 2001/29/CE, sulla tutela giuridica del diritto di autore e dei diritti connessi nell'ambito del mercato interno, con particolare riferimento alla società dell'informazione, che all'art.8.3 prevede l'inibitoria nei confronti "degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto di autore o diritti connessi", all'art.9 fa salva l'applicazione delle disposizioni sul rispetto della vita privata;

- che la direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni (direttiva sulla privacy) all'art.5 sancisce il principio di tutela della riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e

all'art.15 prevede limiti alla tutela, con misure che, ai sensi della citata direttiva 1995/46/CE, siano necessarie, opportune, e proporzionate all'interno di una società democratica per la salvaguardia, tra gli altri interessi, di quelli lesi da reati, e quindi per la prevenzione, la ricerca e l'accertamento degli stessi;

- che infine gli artt.17 e 47 della Carta di Nizza tutelano rispettivamente quali diritti fondamentali il diritto di proprietà, a cui può ascriversi anche il diritto di proprietà intellettuale (CGCE, sent. 12 settembre 2006, C-479/2004, *caso Lasedisken*) e il diritto a un ricorso effettivo, mentre gli artt.7 e 8 della medesima Carta garantiscono rispettivamente il diritto al rispetto della vita privata e il diritto alla tutela dei dati personali, riproducendo l'art.8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e sono richiamati dal secondo considerando della citata direttiva 2002/58/CE;

- che in questo contesto normativo, nell'ambito di una controversia pendente tra la *Promusicae*, associazione senza scopo di lucro, che agisce per conto dei titolari dei diritti di proprietà intellettuale che ne fanno parte, e la *Telefonica*, in cui quest' ultima si rifiuta di fornire alla prima dati personali relativi all'utilizzo di Internet mediante connessioni da essa fornite, il *Judzgado Mercantil* ha sospeso il processo e rinviato alla Corte di Giustizia per pronuncia pregiudiziale;

- che dunque la Corte europea da un lato richiama le corti nazionali a un'interpretazione delle disposizioni di diritto interno di recepimento delle direttive comunitarie conforme al diritto comunitario e dall'altro a un'interpretazione delle direttive stesse che ne adegui il significato alla protezione dei diritti fondamentali e ai principi generali del diritto comunitario, quale quello di proporzionalità, rimettendo di fatto al giudice nazionale, in sede di ricostruzione del sistema, di effettuare il bilanciamento tra gli interessi in conflitto e dunque tra l'interesse alla protezione del diritto di autore quale diritto di proprietà intellettuale e il diritto alla protezione dei dati personali;

- che il contesto normativo interno in cui si muove il giudice italiano è il seguente: l'art.4 del d.lgs. 30 giugno 2003, n.196 (Codice in materia di protezione dei dati personali, d'ora in poi Codice) definisce il trattamento dei dati come "qualunque operazione o complesso di operazioni … concernenti la raccolta, … la conservazione … la comunicazione", essendo chiaro che le tre operazioni elencate tra altre sono legate tra loro da un nesso di consequenzialità e strumentalità, giacché i dati sono raccolti e conservati per essere eventualmente comunicati alle condizioni di legge;

- che l'art.24.1 f) permette il trattamento dei dati senza consenso "per far valere un diritto in sede giudiziaria", l'art.123 del Codice, in attuazione della direttiva 2002/58/CE, porta un generale divieto di conservazione dei dati relativi al traffico nelle comunicazioni elettroniche e l'art.132 dello stesso codice vi deroga per un tempo massimo di 24 mesi nel caso di finalità di accertamento e repressione dei reati, e di ulteriori 24 mesi per le medesime finalità in relazione ai delitti di cui all'art.407.2 a), c.p.p., nonché ai delitti in danno di sistemi informatici e telematici valendosi dunque il legislatore nazionale della facoltà di disporre l'obbligo di comunicazione anche per l'uso non autorizzato del sistema di comunicazione elettronica per la commissione di illeciti non penali ma civili;

- che la norma permissiva dell'art.24.1 f) ha portata generale e rispetto a essa quella dell'art.132 ha natura speciale, ancorché non possa predicarsene l'eccezionalità, in una ricostruzione del sistema conforme al diritto comunitario, che attribuisce pur sempre agli Stati membri la facoltà di derogare al divieto assoluto di trattamento dei dati, ancorché lo Stato italiano non se ne sia valso;

- ma per effetto del mero principio di specialità può ritenersi che la deroga al divieto di trattamento dei dati senza consenso sia ristretta al caso di azioni giudiziarie penali, in cui solo vige l'obbligo di conservazione dei dati per un limitato periodo, parametrato sulla gravità del reato, al fine della comunicazione e utilizzazione dei dati stessi come prova nel processo penale;

- che quindi il legislatore nazionale, attuando tutte le direttive sopra citate, ha effettuato la scelta di limitare le deroghe alle norme protettive della riservatezza al caso di illeciti penali, senza estenderle al caso di illeciti civili, scelta compatibile con il diritto comunitario come interpretato dalla Corte di Giustizia con la pronuncia sopra esaminata, che esclude il vincolo per gli Stati a prevedere un obbligo di comunicazione dei dati in processi civili;

- che dunque il legislatore nazionale ha già effettuato il bilanciamento tra i due diritti, entrambi fondamentali, di proprietà intellettuale e alla riservatezza, ritenendo che la prevalenza del primo sul secondo sia giustificata unicamente se unita alla lesione di interessi della collettività

protetti dal diritto penale, invertendosi i termini del rapporto qualora sia leso soltanto l'interesse individuale del titolare del diritto di esclusiva pur protetto dal diritto della proprietà intellettuale;

- che la Corte costituzionale con sent. 372/2006 ha respinto l'eccezione di legittimità costituzionale dell'art.132 nella parte in cui permette la conservazione dei dati di traffico per ulteriori 24 mesi per finalità di repressione soltanto di determinati reati, giustificando la ragionevolezza del diverso trattamento con la gravità dei reati stessi e richiamando la necessità di un bilanciamento tra il diritto alla riservatezza e gli interessi tutelati dal diritto penale;

- che la Corte costituzionale, con le recenti sentt. 348 e 349/2007 ha affermato il principio secondo cui la violazione degli obblighi derivanti dalla CEDU (n.d.e. che all'art.8 tutela appunto il diritto alla riservatezza) costituisce altresì violazione dell'art.117 Cost.;

- che il giudice italiano, quale interprete del diritto interno in conformità al diritto comunitario e di questo nel rispetto dei diritti fondamentali e del principio di proporzionalità deve prendere atto della scelta legislativa di non avvalersi della facoltà di estendere alle azioni civili l'uso di misure a protezione del diritto di autore se queste violano il diritto alla riservatezza, in ragione della ritenuta non proporzionalità di tali mezzi di *enforcement* alla lesione del diritto proprietario, di fuori dell'ipotesi di reati, e del bilanciamento di interessi così effettuato dal legislatore;

- che ciò il giudice nazionale può fare, tenuto in conto che, in difetto di un vincolo in senso contrario da parte delle direttive in materia siffatta scelta può ritenersi conforme al diritto comunitario secondo la pronuncia della Corte di Giustizia esaminata e che la giurisprudenza comunitaria stessa rimette alla discrezionalità delle Autorità competenti degli Stati membri il giudizio di proporzionalità;

- che inoltre sotto il profilo dell'efficacia delle misure per l'*enforcement* dei diritti di proprietà intellettuale, principio richiamato dall'art.3 della relativa direttiva insieme a quello di proporzionalità, la conseguenza sul sistema della ritenuta prevalenza del diritto di privacy dei consumatori sul diritto proprietario non costituisce sottrazione di ogni tutela a fronte del fenomeno del *downloading*, ben potendosi ragionare in termini di responsabilità dei gestori della rete *peer-to-peer* e dei produttori e fornitori dei servizi di *file sharing*, come avvenuto nella giurisprudenza statunitense, in cui si registrano i primi *leading cases* in materia (vedi primo tra tutti il caso *Napster*);

- che in conclusione nel caso di specie, in cui l'esecuzione dell'ordine di *discovery* si risolverebbe in una comunicazione dei dati personali dei consumatori senza alcun consenso dei medesimi, che operano sulla rete sulla presunzione di anonimato, la misura violerebbe il diritto alla riservatezza dei medesimi e pertanto ne difetta il requisito di ammissibilità;

- che il ricorso dunque deve essere respinto […]

8. LE COMUNICAZIONI ELETTRONICHE

8.1. Confidenzialità della posta elettronica e limiti dell'analogia

Tribunale penale di Milano, ord. 10 maggio 2002

[…]

In fatto l'esponente deduceva che la A. in data 13 agosto 2001 aveva ricevuto da parte del proprio datore di lavoro […] presso la quale aveva svolto in qualità di impiegata mansioni di *consultant/account* sin dalla data di assunzione avvenuta l'1 settembre 2000) raccomandata datata 6 agosto 2001 del seguente letterale tenore: "il giorno 31 luglio u.s., la sua responsabile, durante le normali e periodiche operazioni di lettura della casella aziendale di posta elettronica (cui fanno riferimento i clienti di […], per i progetti a Lei assegnati) al fine di verificare eventuali messaggi ricevuti durante il Suo periodo di assenza per ferie, si imbatteva in comunicazioni inerenti soluzioni Internet inequivocabilmente relative a progetti estranei a quelli attualmente gestiti da […]".

Con successiva missiva del 29 agosto 2001 la A. veniva licenziata dalla ditta […] per presunta violazione dei doveri inerenti al rapporto di lavoro (licenziamento che la lavoratrice impugnava con rivendicazioni economiche).

Nella denuncia-querela l'esponente deduceva che la condotta della C. e del R. presentava aspetti di rilevanza penale (art.616 c.p.) avendo i medesimi fatto accesso alla corrispondenza della lavoratrice; corrispondenza – quella contenuta all'interno della sua casella di posta elettronica, al pari di quella effettuata per via epistolare, telegrafica, telefonica ovvero effettuata con ogni altra forma di comunicazione a distanza – la cui segretezza è garantita costituzionalmente. Né si poteva ritenere la ricorrenza di una causa di giustificazione (esercizio di un diritto o adempimento di un dovere) dal momento che in nessun caso – con l'ovvia eccezione, nella specie non ricorrente, dell'ipotesi in cui si abbia motivo di ritenere che in essa siano contenuti elementi comprovanti fatti illeciti che interessino in modo diretto l'agente – è consentito al datore di lavoro di controllare il contenuto dei messaggi di posta elettronica. Ad ogni buon conto occorreva evidenziare che:

- i messaggi inviati dai clienti erano, senza dubbio identificabili tra quelli contenuti nella casella postale (e ciò si deduceva dal fatto che la stessa società aveva assegnato tali clienti alla A. e le relative comunicazioni erano state oggetto di altri e precedenti controlli da parte della responsabile sig.ra C.);
- il controllo delle missive dei clienti era superfluo considerato che gli stessi erano in ferie;
- il controllo dei messaggi a carattere privato fu compiuto quanto la A. era in ferie evidentemente a sua insaputa e con l'avallo dei responsabili della società;
- non vi era alcuna fondata ragione, al momento del controllo della corrispondenza destinata alla A., da parte della società, per ritenere che in essa vi fossero contenuti elementi comprovanti fatti illeciti interessanti in modo diretto la società stessa.

In data 21 gennaio 2002 il P.M. avanzava richiesta di archiviazione del procedimento con la seguente motivazione: "le caselle di posta elettronica recanti quali estensioni nell'indirizzo *email @(…).it,* seppur contraddistinte da diversi "*username*" di identificazione e *password* di accesso, sono da ritenersi equiparate ai normali strumenti di lavoro della società e quindi soltanto in uso ai singoli dipendenti per lo svolgimento dell'attività aziendale agli stessi demandata; considerando quindi che la titolarità di detti spazi di posta elettronica debba ritenersi riconducibile esclusivamente alla società […]".

L'opposizione risulta inaccoglibile mentre, di contro, l'archiviazione deve essere disposta ritenuta l'infondatezza della notizia di reato.

Dopo aver sgombrato il campo da impropri riferimenti alla normativa contenuta nella legge 675/1996 relativa al ben diverso (ed assolutamente inconferente) problema della tutela del trattamento dai dati personali, una breve ma doverosa premessa s'impone.

La fattispecie dedotta avanti a questo giudice presenta aspetti di novità nell'ambito di una disciplina che solo da tempi relativamente assai recenti ha iniziato a fare la propria comparsa nelle aule giudiziarie.

Non può negarsi come la nascita e la diffusione di una nuova tecnologia precedono sempre e significativamente l'affermarsi di una cultura comune e standardizzata nell'utilizzo ad ogni livello del nuovo strumento. La preoccupazione della prima fase è solo quella di acquisire la padronanza, a volte anche solo parziale, dell'uso tecnico del nuovo mezzo o strumento senza alcun interesse (o

attenzione) nel valutare le modalità di integrazione semiotica o antropomorfa dalla nuova tecnologia (cfr. il recente esempio della telefonia mobile). A questa regola non è certamente sfuggita la "posta elettronica" di Internet.

In attesa di una codificazione dei comportamenti ai fini dell'omologazione e dell'accettazione di un uso standardizzato dello strumento, molte sono le problematiche che si sono affacciate con la nascita della "buca delle lettere elettronica", tra queste dividendole per aree tematiche e cono specifico riferimento all'utilizzo di tale strumento da parte del lavoratore si possono elencare le seguenti:

a) utilizzo anche per fine privato dell'indirizzo di posta elettronica da parte del lavoratore con eventuale esposizione dello stesso sulla carta da visita intestata a proprio nome;

b) possesso di un indirizzo "generalista" e cui la posta ivi indirizzata può avere come destinatario un qualunque altro dipendente con conseguente incertezza sulla "consegna";

c) mancata individuazione del mittente (in possesso di un indirizzo in codice o con sigla) che non provvede a sottoscrivere il messaggio ovvero che non si preoccupa di farsi riconoscere rendendosi di fatto anonimo.

Limitando sostanzialmente la nostra analisi alla prima problematica, va detto innanzitutto come non possa mettersi in dubbio il fatto che l'indirizzo di posta elettronica affidato in uso al lavoratore, di solito accompagnato da un qualche identificativo più o meno esplicito, abbia carattere personale, nel senso cioè che lo stesso viene attribuito al singolo lavoratore per lo svolgimento delle proprie mansioni.

Tuttavia, "personalità" dell'indirizzo non significa necessariamente "privatezza" del medesimo dal momento che, salve le ipotesi in cui la qualifica del lavoratore lo consenta o addirittura lo imponga in considerazione dell'impossibilità o del divieto di compiere qualsiasi tipo di controllo/intromissioni da parte di altri lavoratori che rivestano funzioni o qualifiche sovraordinate (fattispecie che potrebbe effettivamente indurre a qualche dubbio), l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario (ma sempre appartenenti all'azienda) a prescindere dall'identità o diversità di qualifica o funzione: ipotesi, frequentissima, è quella del lavoratore che "sostituisce" il collega per qualunque causa (ferie, malattia, gravidanza) e che va ad operare, per consentire la continuità aziendale, sul *personal computer* di quest'ultimo anche per periodi di tempo non limitati.

Così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti è inconfigurabile in astratto, salve eccezioni di cui sopra, un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale.

Pertanto il lavoratore che utilizza – per qualunque fine – la casella di posta elettronica, aziendale, si espone al "rischio" che anche altri lavoratori della medesima azienda che, unica, deve considerarsi titolare dell'indirizzo – possano lecitamente entrare nella sua casella (ossia in suo uso sebbene non esclusivo) e leggere i messaggi (in entrata e in uscita) ivi contenuti, previa consentita acquisizione della relativa *password* la cui finalità non è certo quella di "proteggere" la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società;

E che detto rischio, per essere "operativo", non debba essere preventivamente ed espressamente ricordato al lavoratore è un'evenienza che può ritenersi conseguenziale alle doverose ed imprescindibili conoscenze informatiche del lavoratore che, proprio perché utilizzatore di detto strumento, non può ignorare questa evidente e palese implicazione.

Né si può ritenere che l'assimilazione della posta elettronica alla posta tradizionale, con consequenziale affermazione "generalizzata" del principio di segretezza, si verifichi nel momento in cui il lavoratore utilizzi lo strumento per fini privati (ossia extralavorativi), atteso che giammai un uso illecito (o, al massimo, semplicemente tollerato ma non certo favorito) di uno strumento di lavoro può far attribuire a chi, questo illecito commette, diritti di sorta.

A questo punto, peraltro, il problema muta prospettiva perché non riguarda più l'individuazione ed il diritto di chi "entra" nel computer (e nell'indirizzo di posta elettronica) altrui avendo possibilità di leggere i messaggi di posta elettronica non specificamente a lui destinati, bensì diventa quello di "tutelare" il diritto di chi invia il messaggio (a qualunque contenuto: ossia a contenuto privato ovvero lavorativo) credendo che il destinatario dello stesso sia e possa essere esclusivamente una determinata persona (o una cerchia determinata di persone). È evidente che questa situazione può trovare tutela rendendo chiaro al proprio interlocutore che l'indirizzo di posta elettronica è esclusivamente aziendale (e, quindi, al di là dell'uso di intestazioni apparentemente

personali del lavoratore-principale utilizzatore, lo stesso non è un indirizzo privato secondo quanto precedentemente detto); cosa che può avvenire o usando un inequivoco identificativo aziendale (indirizzato ad un destinatario virtuale) in aggiunta ad altro identificativo personale-nominativo ovvero provvedendo a segnalare adeguatamente al proprio interlocutore (destinatario reale) la circostanza del carattere "non privato" dell'indirizzo.

Né può ritenersi conferente ogni ulteriore argomentazione che, facendo apoditticamente leva sul carattere di assoluta assimilazione della posta elettronica alla posta tradizionale, cerchi di superare le strutturali diversità dei due strumenti comunicativi (si pensi, in via esemplificativa, al carattere di "istantaneità" della comunicazione informatica – operante come un normale terminale telefonico – pur in presenza di un prelievo necessariamente legato all'accensione del personal e, quindi, sostanzialmente coincidente con la presenza stanziale del lavoratore nell'ufficio ove è presente il *desktop* del titolare dell'indirizzo) per giungere a conclusioni differenti da quelle ritenute da questo giudice.

Tanto meno può ritenersi che leggendo la posta elettronica contenuta sul *personal computer* del lavoratore si possa verificare un non consentito controllo sulle attività di quest'ultimo atteso che l'uso dell'*email* costituisce un semplice strumento aziendale a disposizione dell'utente-lavoratore al solo fine di consentire al medesimo di svolgere la propria funzione aziendale (non si possono dividere i messaggi di posta elettronica: quelli "privati" da un lato e quelli "pubblici" dall'altro) e che, come tutti gli altri strumenti di lavoro forniti dal datore di lavoro, rimane nella completa e totale disponibilità del medesimo senza alcuna limitazione (di qui l'inconferenza dell'assunto in ordine all'asserito preteso divieto assoluto del datore di lavoro di "entrare" nelle cartelle "private" del lavoratore ed individuabili come tali, che verosimilmente contengano messaggi privati indirizzati o inviati al lavoratore e che solo ragioni di discrezione ed educazione imporrebbero al datore di lavoro/lavoratore non destinatario di astenersi da ogni forma di curiosità…).

Parimenti irrilevante appare l'ulteriore rilievo che anche la posta tradizionale che presenti caratteri inequivoci di "privatezza", non cessi di assumere detto carattere se fatta recapitare al suo destinatario sul posto di lavoro anziché al proprio domicilio dal momento che in questo caso l'inconfondibilità del carattere di privatezza-esclusività (busta chiusa con nominativo del solo destinatario) della corrispondenza non consente di operare un simile confronto!

Venendo alla fattispecie dedotta in giudizio, si evidenzia come le indagini esperite […] abbiano consentito di acclarare che:

- all'interno della […] il lavoratore è depositario di un *username* e di una *password* (conosciuti dal solo responsabile tecnico) che vengono utilizzati per entrare nel sistema informatico: identificativi che il singolo lavoratore può in qualsiasi momento modificare;
- l'accesso a tutti gli strumenti aziendali (*email* compresa) è funzionale all'occupazione del dipendente;
- la funzione svolta dagli identificativi non è quella di proteggere i dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì quella di proteggere i predetti strumenti dall'accesso di persone estranee alla società;
- è prassi comune fra i dipendenti dell'azienda fornire volontariamente i propri dati d'accesso ad altri lavoratori con funzioni societarie equivalenti onde permettere la continuazione delle relative funzioni in propria assenza;
- nel normale uso dello strumento viene anche tollerato un uso extra-lavorativo dell'*email* senza tuttavia che si verifichi un mutamento della destinazione dello strumento, che è quello esclusivo della comunicazione con colleghi e clienti: in ogni caso non viene consentito, anzi è assolutamente vietato, l'utilizzo dello spazio di posta elettronica per motivi personali;
- l'indirizzo di posta elettronica dei dipendenti della società si compone, da sinistra a destra, del nome e del cognome del lavoratore seguiti dal simbolo @ e dal nome della società (…).it.

Tutte queste circostanze di fatto attestanti le consuetudini lavorative all'interno dell'azienda e le condotte dei dipendenti sono conformi alle premesse sopra esposte e consentono di escludere la configurabilità a carico degli indagati di fattispecie delittuose.

Fermo quanto precede, si può concludere ritenendo che:

- la A., così come gli altri lavoratori con mansioni e qualifica pari o assimilabili, era tenuta, secondo una consuetudine che non abbiamo difficoltà a ritenere universale, a segnalare (ovvero a non mantenere segreta nel caso di successiva modificazione) la propria *password* per consentire a qualunque altro suo collega di poterla adeguatamente sostituire durante la sua assenza dal lavoro;

- la A., nell'utilizzazione della casella di posta elettronica della società, non poteva non sapere che alla medesima, indipendentemente dalla sua presenza in società, vi poteva avere lecito accesso qualunque altro suo collega (e, ovviamente, il datore di lavoro) al fine del disbrigo delle incombenze lavorative connesse alle mansioni (invio e ricezione di comunicazioni di lavoro con colleghi e clienti). Fermo quanto precede, da ultimo va detto che quand'anche - per assurdo, atteso quanto sin qui esposto - si volesse ritenere che con la loro condotta la C. e il R. nelle rispettive diverse qualità, entrando nella casella di posta elettronica in uso alla lavoratrice abbiano commesso nei confronti della stessa un'illecita intromissione in una sfera personale privata, nondimeno la configurabilità del reato di cui all'art.616 c.p. verrebbe ugualmente esclusa sotto il profilo soggettivo attesa la totale mancanza di dolo nella loro condotta;

- l'accesso alla casella di posta elettronica dell'A. è avvenuta per motivi assolutamente connessi allo svolgimento dell'attività aziendale, oltre che in assenza della lavoratrice: in una situazione, cioè, nella quale non vi era altro modo per accedere a quelle necessarie informazioni e comunicazioni che, diversamente, se non ricevute ovvero recepite con ritardo, avrebbero potuto arrecare un evidente danno (economico e non solo) per la società.

Da qui il rigetto dell'opposizione e l'archiviazione del procedimento.

[…]

8.2. Corrispondenza elettronica collettiva e confidenzialità

TAR Lazio, Roma, sez.I, 15 novembre 2001, n.9425

[…]

I tre ricorsi devono essere riuniti e decisi contestualmente poiché sono collegati da un evidente nesso di consequenzialità.

Il punto di diritto che appare rilevante nel contesto dell'intera vicenda è rappresentato dalla qualificazione del comportamento tenuto dall'amministrazione nell'acquisire cognizione delle affermazioni del ricorrente, espresse nell'ambito di una "*mailing list*", nonché dalla valutazione dei limiti di utilizzabilità delle notizie acquisite. In fatto, riferisce il ricorrente che nel primo semestre del 1998, in relazione ad un argomento di grande interesse fra i diplomatici, rappresentato dallo status degli Uffici XXX […] all'estero, lo stesso esprimeva a titolo personale nel circuito privato "Diplomazia", alcune valutazioni critiche che traevano spunto da perplessità, a sua volta espresse a livello ufficiale dall'Ambasciatore a Varsavia nei riguardi delle soluzioni proposte dal Ministero. Venuto a conoscenza del messaggio tramite un funzionario appartenente a tale circuito, il direttore generale del personale ha deplorato il comportamento del ricorrente con la nota, oggetto del primo ricorso. In particolare l'atto di deplorazione, adottato in quanto il ricorrente avrebbe violato i doveri di lealtà e di fedeltà ai sensi dell'art.11 del d.p.r. 3/1957 ed il dovere di assidua e solerte collaborazione previsto dal successivo art.13, farebbe riferimento: - alla violazione delle regole della riservatezza (art.142 del d.p.r. 18/1967), in relazione all'intervento del ricorrente su una questione d'ufficio ed alla divulgazione con strumento informatico di una comunicazione d'ambasciata; - al linguaggio usato, ritenuto "di basso ed inaccettabile livello" e con "forme gratuitamente sarcastica", con conseguente "grossolano tentativo si screditare l'amministrazione"; - ad un episodio precedente di qualche mese, consistito nell'aver criticato "pubblicamente ed aspramente" la YYYY, fatto che avrebbe procurato non poco imbarazzo al Ministero per la superficialità delle asserzioni e per "l'indecorosità di un'aperta pronuncia fatta da un diplomatico in servizio all'estero contro un ente pubblico del proprio Paese".

Ad avviso del ricorrente, l'amministrazione, divulgando e strumentalizzando il contenuto riservato del messaggio, avrebbe violato le norme anche di livello costituzionale poste a garanzia delle comunicazioni di pensiero a carattere intersoggettivo. L'amministrazione obietta che la rete di posta elettronica "Diplomazia" non potrebbe essere assimilata alla corrispondenza privata, poiché sarebbe aperta a tutti i funzionari diplomatici, in qualsiasi momento gli stessi intendessero iscriversi, che l'amministrazione non avrebbe intercettato la comunicazione del ricorrente, ma sarebbe stata edotta del contenuto delle considerazioni da questi espresse tramite un funzionario appartenente al circuito, circostanza che avrebbe reso le dichiarazioni assimilabili ad una "comunicazione cartacea liberamente circolante", divenuta di pubblico dominio; che, inoltre, attesa la gravità delle affermazioni contenute nella comunicazione, l'amministrazione avrebbe avuto il dovere di intervenire.

In merito alla natura giuridica del circuito ed alla natura della corrispondenza ivi circolante è sufficiente fare riferimento all'art.5 della legge 23 dicembre 1993, n.547 ed all'art.3 del d.p.r. 10 novembre 1997, n.513. In conformità a tali norme, la corrispondenza trasmessa per via informatica e telematica, cd. posta elettronica, deve essere tutelata alla stregua della corrispondenza epistolare o telefonica ed è quindi caratterizzata dalla segretezza.

La Rete "Diplomazia", secondo quanto chiarito dal Garante per la protezione dei dati personali (cfr. nota 16 giugno 1999), è un servizio di indirizzario automatico che consente la trasmissione a più persone di comunicazioni su determinati argomenti di interesse comune. Per far parte della *mailing list*, costituita su iniziativa personale di alcuni diplomatici, è necessario essere un diplomatico ed ottenere, su questa base, l'apposita *password* prevista per accedervi. I messaggi che vi circolano devono essere quindi considerati alla stregua della corrispondenza privata e ciò "sia che si tratti, come sembra di una vera e propria '*mailing list*', sia che si trattasse, in ipotesi di un *newsgroup* ad accesso condizionato dalla disponibilità di una *password*, fornita ad una pluralità di soggetti determinati". Il numero degli iscritti, potenzialmente molto numeroso, ma sempre definito e non indifferenziato, è dunque irrilevante ai fini dell'equiparabilità o no della comunicazione telematica a quella epistolare, contrariamente a quanto sostenuto

dall'amministrazione, posto che la tipologia della comunicazione resta comunque a carattere intersoggettivo e non diffuso. Né rileva, ai fini della qualificazione, la potenziale permeabilità dall'esterno del circuito informatico, poiché tale rischio è proprio di tutte le altre forme comuni di comunicazione e non ne altera le caratteristiche od il livello di garanzia.

Quanto ai destinatari di messaggi, di corrispondenza o di una comunicazione, si conviene che l'ordinamento non impone agli stessi vincoli espressi di riservatezza, salvo il caso di specifici obblighi o cautele disciplinati da particolari norme. Nella specie, è comunque irrilevante, ai fini della decisione, ricercare se tali vincoli sussistessero in relazione al comportamento dei funzionari che hanno diffuso la comunicazione del ricorrente, né giova alla soluzione della controversia accertare se gli stessi abbiano o no agito per fini esclusivamente personali. Il loro comportamento rileva solo per escludere che il modo in cui l'amministrazione ha avuto conoscenza dei fatti, ritenuti disciplinarmente rilevanti, possa configurare un'abusiva e quindi illecita intercettazione di un messaggio informatico tutelato come corrispondenza privata. L'amministrazione, tuttavia, una volta resa edotta dell'oggetto della corrispondenza, non avrebbe dovuto utilizzarlo a fondamento di un formale atto di deplorazione gravemente lesivo della carriera del ricorrente, poiché si trovava alla presenza di una comunicazione, contenente l'espressione di un libero pensiero, destinata originariamente a soggetti definiti, il cui autore non avendo operato alcuna scelta consapevole volta a diffonderne il contenuto in modo indifferenziato, non si era comportato in modo contrario alle regole della riservatezza. Pur essendo occasionale e non intenzionale il modo di conoscenza di tali comunicazioni, le opinioni ivi espresse non erano perciò suscettibili di censura da parte dell'amministrazione alla stessa stregua di notizie scientemente diffusa alla generalità, dovendo invece essere apprezzato nella giusta misura il fatto che l'autore, nella specie, si era servito di un mezzo di diffusione garantito dalla segretezza.

Non si ravvisano in altri termini nella fattispecie i presupposti per l'applicazione dell'art.142, secondo il quale il personale dell'amministrazione degli Affari esteri è tenuto a comportarsi con particolare discrezione e riservatezza. La sindacabilità da parte dell'amministrazione del comportamento in privato degli appartenenti alla carriera diplomatica incontra infatti il limite del diritto alla tutela della loro sfera personale, sicché le opinioni espresse in tale ambito dal ricorrente non potevano divenire oggetto di sindacato disciplinare. Una volta definito l'ambito entro il quale sono maturate le espressioni ed i giudizi ritenuti lesivi e denigratori, si stempera anche la possibilità di attribuire valore negativo al linguaggio usato nella comunicazione censurata. Per la minima parte in cui il messaggio contiene osservazioni personali, infatti, le stesse sono formulate con il tipico linguaggio per iperbole e con espressioni informali e dirette, quasi da conversazione verbale, che caratterizzano in genere tale tipo di comunicazione riservata. Né la violazione della riservatezza, od un comportamento non improntato a lealtà o fedeltà possono essere identificati nella presunta illegittima diffusione del contenuto di atti, già resi pubblici e per di più non coperti da segreto, od in episodi pregressi a suo tempo giudicati irrilevanti a fini disciplinari.

[…]

Per queste ragioni, i due ricorsi, aventi ad oggetto lo stesso procedimento di promozione, devono essere accolti […].

8.3. *Mailing lists* e segreto epistolare

Tribunale civile di Milano, 5 giugno 2007, n.8037

[…]

Con atto di citazione notificato in data 20 novembre 2002, R.A., magistrato con funzioni di presidente della Corte di Assise presso il Tribunale di Novara, conveniva in giudizio, dinanzi a questo Tribunale la Spa Società xxxxxxxxxxx, quale editrice del quotidiano xxxxxxxxxx, Mxxxxx Bxxxxxx, quale direttore responsabile e Sxxxxxx Fxxxxxxxx quale autore dell'articolo ivi pubblicato in data 14 gennaio 2002, intitolato "Il partito dei giudici si ritrova in *chat* per condannare sempre il Cavaliere".

Esponeva l'attore che l'articolo predetto conteneva stralci dei messaggi di posta elettronica scambiati fra gli utenti della *mailing list*, unitamente ai nomi dei magistrati autori di alcuni di questi messaggi ed altri dettagli della loro attività, quali la posizione ricoperta e la sede dell'ufficio; che nella stessa pagina dello stesso numero del quotidiano xxxxxxxxxx compariva altro articolo sottoscritto con uno pseudonimo abbreviativo xxxxx, nel quale la *mailing list* veniva descritta come "una *mailing list* via Internet … con la quale si possono mettere in contatto i giudici da tutta Italia" strumento creato dalle "due correnti di sinistra dei giudici", Movimenti riuniti e Magistratura democratica per parlarsi tra loro; che nell'articolo del Fxxx era indicata una sola corrente, "Magistratura democratica, la corrente di sinistra dei giudici"; che in seguito alla pubblicazione del servizio in questione aveva subito una serie di disavventure personali e professionali; che la *mailing list* in esame è una lista di spedizione di posta elettronica e la pubblicazione dei messaggi di posta elettronica è avvenuta in violazione di legge; che i messaggi così inviati costituiscono corrispondenza riservata, tutelata dall'art.15 Cost. ("La libertà e la segretezza della corrispondenza sono inviolabili …"); che nella nozione di corrispondenza rientrano "la corrispondenza epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza", ai sensi dell'art.5 legge 547/1993; che anche i messaggi di posta elettronica costituiscono corrispondenza epistolare personale, anche se invece di avere un solo destinatario, sono diretti ad una pluralità di soggetti; che la pubblicazione da parte di xxxx di corrispondenza epistolare costituisce un illecito, in violazione dell'art.15 Cost. e del disposto di cui agli artt.616 e 618 c.p.; che la violazione del segreto epistolare non può trovare esimente nella libertà di stampa e nel diritto di cronaca; che il diritto alla riservatezza delle vicende private è riconosciuto dagli artt.2 e 3 Cost., sui diritti inviolabili del cittadino, e dagli artt.15 e 16 Cost. sull'inviolabilità del domicilio e la libertà e segretezza della corrispondenza; che la tutela del segreto si riferisce ai soggetti estranei, diversi rispetto a quelli tra i quali si svolge la comunicazione; che la giurisprudenza tende ad operare un raccordo fra l'art.21 Cost., che sancisce il diritto di opinione, di critica, di cronaca quali estrinsecazione della libertà di manifestazione del pensiero, rilevando che oltre al rispetto della verità, della pertinenza e dell'interesse sociale, incontri un ulteriore limite nella tutela dei diritti inviolabili dell'individuo garantita dagli artt.2 e 3 Cost.; che l'autore della pubblicazione che si fonda sulla violazione delle norme sopra citate è tenuto al risarcimento del danno causato; che l'articolo in esame viola anche la legge 675/1996 sulla tutela dei dati personali, in quanto vengono pubblicati nome e cognome, posizione e luogo di lavoro dei vari autori delle missive in esame; che tali dati personali non sono essenziali rispetto all'informazione oggetto dell'articolo, come dimostrato dal fatto che l'articolo di spalla a firma xxxxx, contiene stralci di missive, senza l'indicazione degli autori; che nel caso di specie ricorre la violazione dell'art.9 legge 675/1996, anche in relazione all'art.20, comma 1, lett.d) ed all'art.25, comma 1, nel trattamento dei propri dati personali, per mancanza dei requisiti di legittimità, correttezza e violazione, nonché dell'essenzialità dell'informazione;

[…]

Tanto premesso, l'attore chiedeva che i convenuti fossero dichiarati responsabili della violazione del segreto epistolare, tutelato dagli arti. 2, 3 e 15 Cost., nonché dagli artt.615-*ter*, 616 e 618 c.p. e della violazione della normativa in tema di trattamento dei dati personali, art.9, art.20, comma 1, lett.d) e art.25, comma 1, legge 675/1996 e condannati al risarcimento di tutti i danni subiti quantificati in euro 200.000,00.

La Società xxxxxxxx Spa, Mxxxx Bxxx e Sxxx Fxxx costituitisi, contestavano le deduzioni formulate dall'attore osservando:

- che il contenuto dei messaggi in esame non era coperto dal segreto epistolare, essendo i messaggi stessi indirizzati ad una schiera indeterminata di aderenti alla *mailing list*, non previamente conoscibile dal mittente; che tale *mailing list*, aperta a tutti coloro volessero iscriversi, costituiva una "bacheca virtuale";
- che il mittente non poteva non essere consapevole dell'eventualità che qualcuno dei destinatari ne divulgasse il contenuto, come accaduto nel caso di specie;
- che non erano configurabili i reati di cui agli artt.616 c.p. (violazione, sottrazione e soppressione della corrispondenza), nonché 618 c.p. (rivelazione del contenuto di corrispondenza) e 615-*ter* c.p. (accesso abusivo ad un sistema informatico e telematico), considerato che il giornalista aveva ricevuto i messaggi in esame da una legittima fonte di informazione; che la diffusione dei dati relativi a nome e cognome, posizione lavorativa e sede dell'ufficio, non costituiva lesione della normativa in materia di riservatezza, ma legittimo esercizio del diritto di cronaca e di critica;
- che infatti erano stati rispettati i criteri della verità dei fatti, dell'interesse pubblico alla conoscenza dei fatti e dell'essenzialità dell'informazione;
- che l'esigenza di comunicare ai lettori i dati utili alla precisa individuazione del mittente derivava dal ruolo pubblico dell'attore, dalla particolare gravità del contenuto dei messaggi e dalla sgradevolezza del linguaggio utilizzato;
- che la pubblicazione dei messaggi di posta elettronica è avvenuta nel pieno rispetto del codice di deontologia ed in particolare secondo il criterio dell'essenzialità dell'informazione, da valutare anche tenendo conto che le persone note o che svolgono funzioni pubbliche godono di una sfera di riservatezza attenuata rispetto alle persone comuni;

[…]

Motivi della decisione

La domanda formulata dall'attore risulta fondata e pertanto, deve trovare accoglimento.

Occorre premettere che nel caso di specie i messaggi di posta elettronica inviati nell'ambito della *mailing list* denominata "In Movimento" costituiscono corrispondenza epistolare privata.

Ed invero, tale tipo di scambio di corrispondenza si qualifica per le modalità di invio, telematiche, e per il fatto di avere, per ogni messaggio, un mittente ed una pluralità di destinatari.

Pluralità di destinatari che non comporta, però, l'indeterminatezza degli stessi, in quanto il messaggio, grazie alla rete informatica, viene inoltrato contestualmente a più soggetti, i quali sono esattamente individuati negli aderenti alla *mailing list* medesima.

Le modalità di accesso alla *mailing list* sono regolate attraverso un'iscrizione, previa comunicazione dei propri dati personali, e relativa accettazione da parte del moderatore […].

Solo gli iscritti, esattamente individuati, possono accedere alla lista e deve, invece, negarsi che l'accesso sia consentito a chiunque lo desideri o si connetta alla rete telematica in un determinato momento.

Sussiste, pertanto la personalità della comunicazione, che non si identifica con l'unicità, ma consiste nella predeterminazione dei destinatari, cui il mittente intende inviare il proprio messaggio di posta elettronica, quelli e non altri.

Contrariamente a quanto dedotto da parte convenuta, nel caso di specie non si ha una comunicazione diretta a soggetti indeterminati, ma rivolta a tutti gli iscritti alla lista, i quali hanno fornito i propri dati personali risultando identificabili e sono stati accettati dal moderatore.

Da quanto detto, ne consegue che i messaggi scambiati nell'ambito della *mailing list* in esame sono caratterizzati dalla segretezza e godono della tutela di cui all'art.15 Cost., agli artt.616 e 618 c.p., nonché all'art.13 del dpr n.513/1997.

L'art.15 Cost. chiarisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge". All'art.616, comma 4, viene precisato che "Agli effetti delle disposizioni di questa sezione, per 'corrispondenza' si intende quella epistolare, telegrafica, telefonica; informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

L'art.13 sopra citato, regola la "segretezza della corrispondenza trasmessa per via telematica".

I convenuti si difendono richiamando una pronuncia del Garante per la tutela dei dati personali del 12 luglio 1999 […], che avrebbe stabilito che la presa di conoscenza di un'*email* da parte di un soggetto estraneo al circuito di posta elettronica, non contrasta con la normativa relativa ai dati personali, quando "il messaggio non sia stato indebitamente acquisito, ma comunicato da uno dei destinatari del messaggio stesso".

Tale pronuncia, però, come evidenziato da parte attrice, non pare pertinente nella presente fattispecie, nella quale non si è verificata la mera presa di conoscenza dell'*email*, ma è stata effettuata la divulgazione a mezzo pubblicazione su di un quotidiano a diffusione nazionale.

Del resto, come dichiarato da questo Tribunale (sentenza del 5 marzo 1998 […]), "La pubblicazione di corrispondenza epistolare che abbia carattere confidenziale o si riferisca all'intimità della vita privata, in mancanza del consenso dell'autore … costituisce violazione del diritto alla riservatezza, anche qualora la diffusione avvenga con il consenso del destinatario".

Ne consegue che non risulta sufficiente il consenso di uno dei destinatari per la divulgazione dei messaggi inviati, sembrando prevalente il diritto alla riservatezza dell'autore, riconosciuto e tutelato dalle fonti normative sopra citate.

Nel caso di specie sussiste pertanto, la violazione della riservatezza dell'attore, con riferimento al segreto epistolare.

Il fatto per cui è causa comporta, altresì, la sussistenza di altra violazione, che riguarda la pubblicazione dei dati personali dell'attore e cioè nome e cognome, posizione lavorativa e sede dell'ufficio.

A tal proposito, i convenuti si difendono osservando che tale condotta era scriminata dal legittimo esercizio del diritto di cronaca, sulla base dei noti requisiti, relativi alla verità del fatto narrato, all'interesse pubblico della notizia in questione ed alla continenza dello scritto, ai quali va affiancato nel presente caso essenzialità dell'informazione.

Reputa peraltro il Tribunale che risulti assorbente la trattazione del requisito dell'essenzialità dell'informazione, che nel caso di specie difetta.

Si osserva, infatti, che la notizia in esame dovrebbe consistere nella comunicazione ai lettori che, nell'ambito della magistratura esistono alcuni giudici che hanno manifestato particolare avversione per una parte politica e lo abbiano comunicato nell'ambito di una platea piuttosto ampia, la *mailing list*.

Parte convenuta sostiene che l'informazione è stata resa nella sua essenzialità e che non si poteva prescindere dall'individuazione dei giudici criticati, per il ruolo pubblico del giudice, per la gravità del fatto e per la sgradevolezza del linguaggio utilizzato.

Reputa peraltro il Tribunale che tale impostazione non possa condividersi e che vada fatta una diversa riflessione.

Ed infatti, la completezza dell'informazione in questione, come sopra individuata, pare raggiunta con la (sola) indicazione dei fatti narrati, mentre la precisazione dei nominativi dei giudici autori dei messaggi pubblicati non sembra costituire un elemento aggiuntivo significativo, comportando, invece, un'esposizione degli stessi ai lettori del quotidiano Il xxxxxx, con le conseguenze, in termini di disagi, che l'attore ha documentato.

Né risulta consigliata la pubblicazione dei dati personali in questione dal ruolo ricoperto dalla magistratura, considerato che tale ruolo va apprezzato nel riferimento alla categoria ed ha meno valore nell'indicazione del singolo.

Anche la dedotta gravità del fatto non sembra essere pertinente, considerato che l'informazione in questione risultava completa anche senza i dati personali in esame, consentendo al lettore di formarsi una propria opinione.

Da quanto detto ne consegue che la diffusione dei dati personali in questione (nome e cognome, posizione ricoperta e sede dell'ufficio) costituisce un trattamento dei relativi dati non lecito o comunque eseguito in maniera non corretta, come evidenziato in altra vicenda da questo Tribunale con la sentenza del 13 aprile 2000 […].

Sussiste pertanto la lamentata lesione del diritto alla riservatezza, che si affianca alla violazione del segreto epistolare.

[…]

P.Q.M.

Il Tribunale definitivamente pronunciando sulla domanda proposta da Rxxx Axxx con atto di citazione notificato in data 20 novembre 2002, nei confronti della Società xxxxx Edizioni Spa, Mxxx Bxxx e Sxxx Fxxx, ogni contraria istanza, eccezione o deduzione disattesa, così provvede:

1) accerta la lesione del diritto alla riservatezza dell'attore, commessa attraverso la pubblicazione dell'articolo in data 14 gennaio 2002, intitolato " Il partito dei giudici si ritrova in *chat* per condannare sempre il Cavaliere";

2) condanna i convenuti xxxxxxxxxxxxxxx al pagamento in solido, in favore dell'attore, della somma di euro 15.000,00 per la lesione del diritto alla riservatezza;

[…]

8.4. Posta elettronica non sollecitata

Garante per la protezione dei dati personali, provv. generale 29 maggio 2003

***Spamming*. Regole per un corretto invio delle *email* pubblicitarie**

[…]

2. Invio lecito di posta elettronica pubblicitaria

Gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia (art.1, comma 1, lett.c), legge n.675).

La loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato.

Il consenso è necessario anche quando gli indirizzi sono formati ed utilizzati automaticamente con un *software* senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

Questo assetto, basato su una scelta dell'interessato cd. di *opt-in*, è stato ribadito nel 1998 (con il d.lgs. n.171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea […].

Questa Autorità si è pronunciata più volte in materia ribadendo che la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari (cfr., tra l'altro, la decisione dell'11 gennaio 2001 […]).

In particolare, i dati dei singoli utenti che prendono parte a gruppi di discussione in Internet sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico (art.9, comma 1, lettere a) e b), legge n.675).

Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista "anagrafica" degli abbonati ad un Internet *provider* (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure pubblicati su siti *web* di soggetti pubblici per fini istituzionali.

Tali considerazioni valgono anche con riferimento ai messaggi pubblicitari inviati a gestori di siti *web* -anche di soggetti privati- utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio. In quest'ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n.675) e non anche a rendere l'interessato disponibile all'invio di messaggi pubblicitari.

In tutti questi casi, l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad adottare "filtri", a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico.

Il fenomeno interessa anche piccole e grandi imprese destinatarie di un elevato numero di messaggi, le quali devono farsi carico di misure interne e di costi anche organizzativi per contrastarlo.

Questo ingiustificato riversamento sugli utenti dei costi pubblicitari si verifica anche relativamente a messaggi inviati da singole persone fisiche che, in vari casi esaminati, non si limitano ad una comunicazione episodica, ma intraprendono una comunicazione sistematica per fini personali o, addirittura, una diffusione di dati cui è applicabile la disciplina in materia di protezione dei dati personali (art.3, legge n.675).

3. Il quadro giuridico su informativa e consenso

La legge individua il contenuto dell'informativa agli interessati, nonché i casi in cui è necessario il consenso espresso dell'interessato o è possibile prescinderne (artt.10, 11, 12 e 20 legge n.675).

Al riguardo va nuovamente rilevato che non può farsi a meno del consenso ritenendo che i dati personali relativi all'indirizzo di posta elettronica – e all'indirizzo in particolare - siano "pubblici" in quanto conoscibili da chiunque.

Le disposizioni normative che si riferiscono a questo aspetto (artt.12, comma 1, lett.c) e 20, comma 1, lett.b), legge cit.) sono infatti applicabili solo quando vi è un pubblico registro, elenco, atto o documento conoscibile da chiunque perché vi è una specifica disciplina che ne impone la conoscibilità indifferenziata da parte del pubblico, e non anche quando i dati personali sono conoscibili da chiunque per mere circostanze di fatto (si pensi, oltre ai casi già richiamati di raccolta su siti *web* o di messaggi trasmessi su *newsgroup* o su *mailing list*, agli indirizzi di posta elettronica raccolti in rete tramite appositi *software* o mediante comuni motori di ricerca).

Il principio del consenso è quindi già operante nel nostro ordinamento prima ancora di essere affermato senza eccezioni su scala europea, dalla menzionata direttiva 2002/58/CE in fase di recepimento, a tutta la posta elettronica comunque inviata per fini di commercializzazione diretta (si vedano in particolare l'art.13 e il considerando n.40).

Il quadro evidenziato trova conferma nella disciplina sulla protezione dei consumatori nei contratti a distanza che, in riferimento al rapporto sottostante ai fini del quale si procede al trattamento di dati personali, vieta ai fornitori l'impiego della posta elettronica in mancanza del consenso preventivo del consumatore, in relazione a determinati scopi tra i quali rientrano anche quelli pubblicitari (art.10, comma 1, d.lgs. 22 maggio 1999, n.185).

Per gli aspetti relativi alla protezione dei dati personali non devono essere peraltro considerate le disposizioni del recente d.lgs. 9 aprile 2003, n.70, sul commercio elettronico, dichiarate in proposito espressamente inapplicabili (art.1, comma 2, lett.b) d.lgs. n.70 cit.).

Il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi (art.11, legge n.675).

Tale disciplina non può essere elusa inviando una prima *email* che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario, oppure riconoscendo solo un diritto di tipo cd. "*opt-out*" al fine di non ricevere più messaggi dello stesso tenore.

Al contrario, è opportuna e va incoraggiata la prassi di alcuni fornitori i quali, dopo aver ottenuto realmente un valido consenso dei destinatari, danno semplice conferma della sua manifestazione, attraverso un messaggio volto unicamente ad annunciare il successivo inoltro di materiale pubblicitario. Tale prassi, se utilizzata correttamente, consente tra l'altro di verificare l'effettiva corrispondenza dell'indirizzo di posta elettronica ai soggetti che avevano espresso il consenso, nonché di accertare il permanere di tale volontà.

L'insieme dei diritti riconosciuti dalla legge agli utenti determina, in caso di loro violazione, un trattamento illecito dei dati che:

- è già vietato direttamente dalla legge, senza che sia necessario adottare uno specifico provvedimento interdittivo del Garante dell'autorità giudiziaria; determina, a seconda dei casi, l'applicazione di sanzioni amministrative pecuniarie, in particolare per omessa informativa od omessa notificazione (artt.10, 34 e 39, legge n.675; art.12, d.lgs. 185/1999);
- comporta il rimborso delle spese e dei diritti relativi al procedimento attivato da un fondato ricorso al Garante, oppure da un'azione dinanzi al giudice civile, come pure il risarcimento dei danni, specie di tipo patrimoniale, che derivino dai fatti illeciti e siano comprovati dall'interessato in relazione ai disagi sopra illustrati;
- rende applicabile anche una sanzione penale qualora il trattamento illecito dei dati sia effettuato al fine di trarne per sé o per altri un profitto o per arrecare ad altri un danno, con la pena accessoria della pubblicazione della sentenza di condanna (artt.35 e 38, legge n.675).

4. Messaggi pubblicitari a propri clienti

Per effetto del recepimento della direttiva 2002/58/CE sarà peraltro possibile integrare, nel prossimo futuro, la disciplina sopra illustrata, permettendo a talune società di far conoscere a propri clienti prodotti o servizi analoghi a quelli per i quali si è già stabilito un rapporto, con i medesimi clienti, di vendita di prodotti o servizi.

In tali casi, la società titolare del trattamento (dopo aver informato preventivamente e adeguatamente il cliente) potrà procedere all'invio del messaggio pubblicitario, offrendo però al cliente, in modo chiaro e distinto (sia al momento della raccolta dei suoi dati, sia in occasione di ciascun messaggio) il diritto di rifiutare sin dall'inizio tale uso dei dati o di obiettare, gratuitamente e in maniera agevole, anche successivamente (art.13, par. 2, direttiva 2002/58/CE cit.)

5. Messaggi per conto terzi e acquisto di banche dati

In alcuni casi portati all'attenzione del Garante, l'invio di messaggi pubblicitari era stato effettuato, per conto di terzi committenti, da società specializzate che utilizzano indirizzi di posta elettronica contenuti in proprie banche dati.

Tali società, da considerarsi "titolari" o contitolari del trattamento dei dati a seconda del rapporto che si instaura con il committente e delle modalità di concreta utilizzazione dei dati, sono tenute a rispettare le disposizioni in tema di informativa e specifico consenso, anche per quanto riguarda l'eventuale comunicazione di dati personali ai committenti medesimi e le relative finalità.

Ciò comporta un quadro di obblighi e possibili responsabilità anche penali che gli operatori devono verificare con attenzione, anche quando la società specializzata incaricata sia stabilita fuori dell'Unione europea.

Dall'esame dei reclami e delle segnalazioni pervenuti al Garante è risultato, altresì, che alcuni dei soggetti che hanno utilizzato la posta elettronica per l'invio di messaggi pubblicitari avevano acquisito da terzi le banche dati contenenti gli indirizzi dei destinatari. In questi casi, chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito alla comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario; al momento in cui registra i dati deve poi inviare in ogni caso, a tutti gli interessati, un messaggio di informativa che precisi gli elementi indicati nell'art.10 della legge n.675, comprensivi di un riferimento di luogo - e non solo di posta elettronica - presso cui l'interessato possa esercitare i diritti riconosciuti dalla legge.

6. Diritti degli interessati

Indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi, chi detiene i dati deve assicurare in ogni caso agli interessati la possibilità di far valere in ogni momento i diritti riconosciuti dalla legge, i quali sono spesso esercitati per conoscere da quale fonte sono stati tratti i dati, o per far interrompere gratuitamente la loro ulteriore utilizzazione ai fini commerciali-pubblicitari, oppure per far cancellare i dati trattati in violazione di legge (art.13, comma 1, lett.e), della legge).

Nel sito Internet del Garante è riportato un modello-tipo per esercitare tali diritti in maniera agevole, gratuitamente e senza particolari formalità, anche verbalmente o mediante posta elettronica, dimostrando la propria identità (art.17, comma 1, d.p.r. 501 del 31 marzo 1998). Tale modello è utilizzabile in luogo di altri reperibili in reti telematiche che non sono pienamente validi in quanto si riferiscono anche ad aspetti non riconosciuti dall'art.13 della legge n.675 (ad esempio, chiedono il rilascio di attestazioni o la copia di autorizzazioni non previste).

I diritti vanno esercitati sulla base di tale modello direttamente presso l'indirizzo conoscibile del titolare o del responsabile del trattamento, riservando solo ad un eventuale momento successivo l'instaurazione di una procedura contenziosa dinanzi al Garante o all'autorità giudiziaria.

Anche ai fini dell'esercizio di tali diritti, deve ritenersi che l'invio anonimo di messaggi pubblicitari senza l'indicazione di un mittente identificabile concreti già oggi un trattamento illecito di dati personali, a prescindere da quanto dispone il citato d.lgs. 70/2003 sul commercio elettronico (come si è visto, fuori della materia della protezione dei dati personali) e da quanto, in riferimento ai dati personali, sarà previsto con il recepimento della direttiva 2002/58/CE (la quale non consente l'invio di messaggi pubblicitari quando l'identità del mittente viene camuffata o addirittura celata e quando non viene fornito un indirizzo valido che consenta al destinatario di richiedere la cessazione delle comunicazioni: art.13, par. 4, direttiva cit.).

I mittenti dei messaggi devono quindi indicare già oggi, in modo chiaro, la fonte di provenienza del messaggio, nonché il soggetto e l'indirizzo – non solo di posta elettronica - presso cui i destinatari possono esercitare i propri diritti (si veda, in proposito, l'art.10, comma 1, lett.f) della legge n.675). Appare altresì conforme al principio di correttezza indicare nell'oggetto del messaggio la sua tipologia pubblicitaria-commerciale (art.9, comma 1, lett.a), legge n.675).

7. Elenchi di possibili destinatari

L'eventuale elenco predisposto da operatori, contenente i nominativi dei soggetti che non hanno manifestato il consenso o che lo hanno revocato (cd. *black list*) non può essere utilizzato per porre a carico degli interessati, anche indirettamente, un onere di iscrizione nell'elenco medesimo.

Come si è illustrato, il consenso ha un connotato autorizzatorio "positivo" in base al quale l'eventuale silenzio dell'interessato comporta il diniego del consenso eventualmente richiesto e non rileva come assenso tacito all'invio dei messaggi.

Consta peraltro che alcuni operatori intendono adottare la diversa prassi di redigere anche tramite siti *web* appositi elenchi di persone che hanno manifestato il consenso, distinti in base alle diverse categorie di messaggi commerciali-pubblicitari che gli interessati hanno acconsentito a ricevere. Tale prassi, se correttamente seguita, può rappresentare una misura utile, sul piano organizzativo, per garantire un più effettivo rispetto della volontà espressa dai singoli. A tale riguardo, costituirà una pratica utile quella di garantire agli interessati la possibilità di inserire direttamente il proprio nome nelle diverse liste o di cancellarlo dalle stesse, magari attraverso un'apposita pagina *web*, ferma restando l'esigenza di identificarli.

8. *Email* provenienti dall'estero

Ad alcuni messaggi, in quanto provenienti dall'estero, non è applicabile la legge italiana sulla protezione dei dati personali.

Ciò non comporta l'assoluta mancanza di rimedi o tutela, potendo l'utente chiedere una verifica da parte della competente autorità nazionale di protezione dei dati personali, ove istituita nel Paese eventualmente individuabile dal messaggio.

In altri casi, come quelli relativi alle leggi degli Stati federali, l'invio di messaggi pubblicitari di posta elettronica può essere illecito in base alla legge di alcuni Stati, per cui è parimenti possibile, per gli utenti, chiedere alle competenti autorità pubbliche degli Stati di valutare la perseguibilità degli illeciti.

Va infine tenuto presente che alcune *email* indesiderate possono essere lo strumento per commettere reati comuni (ad esempio di truffa) che devono considerarsi commessi nel territorio italiano quando, sebbene l'azione è avvenuta all'estero, l'evento-reato che ne deriva si è verificato in Italia.

Questa Autorità si riserva di valutare la posizione dei singoli fornitori di servizi i cui trattamenti sono stati oggetto di segnalazione, anche alla luce dell'ulteriore documentazione eventualmente pervenuta.

In questo quadro, con separati provvedimenti relativi all'esame dei singoli reclami e segnalazioni, si provvederà, oltre alle eventuali trasmissioni di atti all'autorità giudiziaria penale:

a) a contestare la violazione amministrativa relativa agli obblighi di informativa di cui all'art.10 della legge 31 dicembre 1966, n.675;

b) ad avviare il procedimento per l'applicazione delle ulteriori sanzioni amministrative previste dal d.lgs. 185/1999;

Tutto ciò premesso il Garante:

1. ai sensi dell'art.31, comma 1, lett.l) della legge 31 dicembre 1996, n.675, vieta l'ulteriore trattamento illecito di dati personali realizzato a scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, effettuato in violazione delle disposizioni sopra richiamate da parte dei soggetti cui si riferiscono le segnalazioni e i reclami pervenuti;
2. ai sensi dell'art.31, comma 1, lett.c) della legge 31 dicembre 1996, n.675, segnala ai titolari del trattamento di cui agli atti del procedimento la necessità di conformare i trattamenti di dati personali ai principi richiamati nel presente provvedimento.

9. L'USO DI INTERNET SUL LUOGO DI LAVORO

9.1. Controlli in Rete sul lavoratore e privacy

Corte Europea dei Diritti dell'Uomo, 3 aprile 2007 - *Application* no. 62617/00

[…]

Procedure

1. The case originated in an application (no. 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, email 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"). The College is a statutory body administered by the State and possessing powers under sections 18 and 19 of the Further and Higher Education Act 1992 relating to the provision of further and higher education.

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, email 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 email at work when her step-daughter was contacted by the College and asked to supply information about emails 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 emails only were being investigated. By an email dated 24 November 1999 the CP advised the applicant that, whilst all email activity was logged, the information department of the College was investigating only her emails, following a request by the DP.

13. The Government submitted that monitoring of emails took the form of analysis of email addresses and dates and times at which emails were sent and that the monitoring occurred for a few months prior to 22 November 1999. According to the applicant the monitoring of emails

occurred for at least six months from May 1999 to November 1999. She provided documentary evidence in the form of printouts detailing her email usage from 14 May 1999 to 22 November 1999 which set out the date and time of emails sent from her email account together with the recipients' email addresses.

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] email traffic.

Subsequent to the applicant becoming aware that someone from the College had been following up her emails, 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 email 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, email 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."

30. The Government contested that argument.

[…]

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-, no.27798/95, §43, […]). It follows logically that emails 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 email 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 email 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, email 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, email 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;

[…]

9.2. Posta elettronica aziendale e conoscenza della *password*

Corte di Cassazione, sez.V penale, 11 dicembre 2007, n.47096

[…]

Con la sentenza impugnata il Tribunale di Torino, sezione di Chivasso, ha prosciolto G.T. perché il fatto non sussiste dall'imputazione di avere abusivamente preso cognizione della corrispondenza informatica aziendale della dipendente R.M., licenziata poi sulla base delle informazioni così acquisite.

Ricorre per Cassazione il pubblico Ministero e deduce violazione dell'art.616 c.p., lamentando che il Giudice del merito si sia fondato sull'erroneo presupposto della rilevanza della proprietà aziendale del mezzo di comunicazione violato, senza considerare il profilo funzionale della destinazione del mezzo telematico non solo al lavoro ma anche alla comunicazione, tutelata dall'art.15 Cost.

Il ricorso è infondato.

L'art.616, comma 1, c.p. punisce infatti la condotta di "chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime".

Sicché, quando non vi sia sottrazione o distrazione, la condotta di chi si limita a "prendere cognizione" è punibile solo se riguarda "corrispondenza chiusa". Chi "prende cognizione" di "corrispondenza aperta" è punito solo se l'abbia a tale scopo sottratta al destinatario ovvero distratta dalla sua destinazione.

Ciò posto, e indiscussa l'estensione della tutela anche alla corrispondenza informatica o telematica (art.616, comma 4, c.p.), deve tuttavia ritenersi che tale corrispondenza possa essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o di ricezione dei singoli messaggi. Infatti, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite. Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. E quando in particolare il sistema telematico sia protetto da una *password*, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso. Anche quando la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso.

Nel caso in esame è indiscusso, e ne dà atto lo stesso ricorrente, che le *passwords* poste a protezione dei computer e della corrispondenza di ciascun dipendente dovevano essere a conoscenza anche dell'organizzazione aziendale, essendone prescritta la comunicazione, sia pure in busta chiusa, al superiore gerarchico, legittimato a utilizzarla per accedere al computer anche per la mera assenza dell'utilizzatore abituale.

Ne consegue che del tutto lecitamente G.T. prese cognizione della corrispondenza informatica aziendale della sua dipendente, utilizzando la chiave di accesso di cui legittimamente disponeva, come noto alla stessa R.M.. Infatti, secondo le prescrizioni del provvedimento del Garante per la protezione dei dati personali n.13 dell'1 marzo 2007, i dirigenti dell'azienda accedono legittimamente ai computer in dotazione ai propri dipendenti, quando delle condizioni di tale accesso sia stata loro data piena informazione.

P.Q.M.

La Corte rigetta il ricorso.

[…]

9.3. Tolleranza dell'uso personale della posta elettronica aziendale

Tribunale Firenze, sez. lavoro, 7 gennaio 2008, n.1218

[…]

Con ricorso al Tribunale di Firenze, in funzione di giudice del lavoro, il sig XY ha convenuto in giudizio Z Cooperativa a r.l. impugnando il licenziamento disciplinare intimatogli con lettera 28 ottobre 2004 dalla datrice di lavoro e chiedendone la condanna al pagamento di complessivi euro 90.000.000 a titolo di risarcimento del danno biologico, esistenziale, all'immagine, da dequalificazione; costituitasi in giudizio, parte convenuta ha contestato la domanda, chiedendone il rigetto.

[…]

Con lettera 28 ottobre 2004, Z Cooperativa a r.l. ha contestato al ricorrente il seguente addebito disciplinare: "Dal mese di gennaio 2004 lei ha quotidianamente usato in modo improprio e per fini ed interessi personali gli strumenti informatici aziendali in sua dotazione accedendo, durante l'orario di lavoro, a diversi siti non attinenti alla sua attività lavorativa. A titolo meramente esemplificativo citiamo qui alcuni dei siti che lei ha aperto e visionato e dai quali, in alcuni casi, ha scaricato dati: […]". A seguito di tale contestazione, il ricorrente è stato licenziato con lettera in data 15 novembre 2004.

Ad avviso del giudicante, parte convenuta non ha provato la sussistenza di giusta causa di recesso, per le seguenti considerazioni:

- la consulenza tecnica espletata, sulla base dei dati raccolti in sede di accertamento tecnico preventivo, ha concluso, se pure con il margine di approssimazione che deriva dalla difficoltà di distinguere con esattezza i siti Internet attinenti all'attività lavorativa da quelli a essa estranei, che il ricorrente ha utilizzato il computer a lui assegnato per accedere alla rete Internet per complessive 276,53 ore, su 163 giorni nei quali ha effettuato almeno un collegamento;
- per il 70% circa tali accessi sono stati relativi a siti non attinenti l'attività lavorativa;
- considerato che il tempo medio di accesso alla rete Internet ammonta, per il ricorrente, a circa 80 minuti giornalieri […], l'utilizzo del computer per ragioni extralavorative può essere mediamente determinato in circa 56 minuti giornalieri;
- peraltro, è emerso dall'istruttoria espletata che era consentito un accesso alla rete Internet per motivi extralavorativi, sia pure nei limiti della ragionevolezza e purché il sistema non fosse tenuto occupato per tempi eccessivi;
- in tale contesto, benché gli accessi del ricorrente siano stati superiori a quelli di colleghi assegnati a mansioni affini […], non può ritenersi la proporzionalità della sanzione espulsiva (cfr., da ultimo, Cass. 30 marzo 2006, n.7543), in quanto l'intensità dell'elemento soggettivo della condotta del lavoratore è sminuito dalla tolleranza aziendale all'accesso, da parte dei dipendenti, alla rete Internet anche per motivi extralavorativi;
- va inoltre rilevato che è estranea alla contestazione disciplinare la questione circa la mancata prestazione lavorativa del ricorrente durante l'accesso alla rete Internet, in quanto il licenziamento è motivato con l'uso improprio degli strumenti informatici aziendali;
- tale fattispecie è assimilabile al danneggiamento di beni aziendali, per il quale l'art.81 CCNL prevede la sanzione conservativa della sospensione, e anche sotto tale profilo va ritenuta la carenza di proporzionalità della sanzione espulsiva.

Ne consegue l'annullamento del licenziamento, con la condanna della convenuta alla reintegrazione nel posto di lavoro e al risarcimento del danno *ex* art.18 legge 300/1970, in difetto di prova circa l'*aliunde perceptum* […].

9.4. Rilevazione dei dati di traffico Internet sul luogo di lavoro

Corte di Cassazione, sez. lavoro, 23 febbraio 2010, n.4375

[…]

Con sent. n.1048/2003 il Giudice del lavoro del Tribunale di Milano, in accoglimento della domanda proposta da YYYY nei confronti della XXXX S.p.a., dichiarava l'illegittimità dei due licenziamenti alla stessa intimati in data (…), con le conseguenze di cui all'art.18 dello Statuto dei lavoratori.

Il Tribunale, quanto al primo licenziamento, riferibile a fatti commessi fra il (…), riteneva che i fatti contestati, sintetizzabili nell'accesso a Internet per ragioni non di servizio in contrasto con il regolamento aziendale del 4 maggio2001, fossero stati rilevati e registrati da un programma di controllo informatico centralizzato (*Super Scout*), in violazione della legge 300/1970, art.4, comma 2, con la conseguente inutilizzabilità dei dati acquisiti. In ogni caso riteneva violate le regole di proporzionalità e gradualità delle sanzioni disciplinari.

Quanto, poi, al secondo licenziamento, intimato a seguito di lettera di contestazione del (…), il primo giudice riteneva la contestazione tardiva, poiché i fatti contestati, relativi al periodo (…), erano in parte antecedenti alla prima contestazione disciplinare e in parte una duplicazione dei fatti già contestati e per i mesi precedenti la prima contestazione, sicuramente conoscibili con il programma *Super Scout*.

Inoltre essi erano stati ricavati direttamente dal *personal computer* della YYYY senza che la società avesse dimostrato l'inaccessibilità dello stesso fra il (…) e il momento del rilievo dei dati alla fine di agosto, come riferito dal teste M., con il dubbio della manipolazione dei dati stessi e di una conoscenza o comunque conoscibilità dei dati in epoca antecedente.

[…]

La Corte d'Appello di Milano, con sentenza depositata il 30 settembre 2005, confermava la sentenza appellata e condannava l'appellante al pagamento delle spese.

[…]

Motivi della decisione

[…]

Con il primo motivo la ricorrente lamenta che la Corte di merito, in sostanza trasformando essa "parte offesa" in "parte offendente", ha omesso di considerare l'enorme quantitativo di accessi ad Internet di svariato tipo, con rilevante sottrazione al tempo di lavoro e con pericolo per la sicurezza della rete aziendale e, pur avendo accertato che per regolamento interno, conosciuto dalla YYYY, tali accessi erano autorizzati solo per le esigenze di servizio, non ne ha tratto le relative conseguenze, in ordine alla proporzionalità del licenziamento, anche sotto il profilo della configurabilità del reato di cui all'art.615-*ter* c.p..

Il motivo è in parte inammissibile e in parte infondato.

Mentre la "censura di fondo" è del tutto generica, il quantitativo degli accessi ad Internet, come risultato dai tabulati prodotti in corso di causa, e non anche come emerso dal sistema di controllo *Super Scout* (i cui dati sono stati ritenuti legittimamente non utilizzabili, come si vedrà), è stato attentamente esaminato e valutato (con riferimento al primo licenziamento, stante la tardività del secondo) dalla Corte d'Appello, la quale, con motivazione congrua e priva di vizi logici, ha rilevato la sproporzione tra addebito e sanzione, in base ai rilievi che il collegamento a Internet nel periodo in osservazione (…) si era verificato in otto giornate oltre all'apertura, quotidiana dal (…), di un indirizzo di posta elettronica non aziendale al portale (…), che pur non essendovi contestazione sul tipo di sito visitato e sulla potenziale dannosità per il sistema informatico aziendale, nella specie non era stato contestato in modo specifico il tempo che sarebbe stato sottratto alla prestazione lavorativa, non essendo indicati né l'orario né la durata dei singoli collegamenti, i quali potevano essere avvenuti anche in pausa lavorativa, che dai citati tabulati era emerso che la durata dei collegamenti (salvo uno) era stata di pochi minuti e che l'accesso ad Internet era avvenuto, non di rado, in pausa pranzo, che peraltro non era emerso che in precedenza vi fosse stato da parte della azienda un particolare richiamo sulla rigidità del divieto di uso promiscuo, che, infine, la lavoratrice non aveva precedenti disciplinari.

Né all'uopo può ritenersi sufficiente il generico richiamo, tra l'altro, anche alla legge 547/1993, contenuto nel Regolamento in "ordine al corretto utilizzo dei sistemi informatici aziendali" contenuto nel ricorso. Peraltro non può ignorarsi che i fatti contestati erano "sintetizzabili nell'accesso a Internet per ragioni non di servizio in contrasto con il regolamento aziendale" e non anche nell'"accesso abusivo al sistema informatico" della società.

Con il secondo motivo la ricorrente, denunciando violazione dell'art.8 dello Statuto dei lavoratori e del d.lgs. 196/2003, art.4 lett.a) e d), nonché vizio di motivazione, in sostanza lamenta che erroneamente la Corte di merito avrebbe ritenuto nella fattispecie la violazione della legge 300/1970, art.8, e della normativa sulla privacy (all'epoca legge 675/1996, ora d.lgs. 196/2003).

Osserva il Collegio che la censura non coglie nel segno l'impugnata decisione, la quale, seppure nelle premesse ha, tra l'altro, prospettato la questione della utilizzabilità o meno delle informazioni acquisite anche sotto i profili dell'art.8 dello Statuto dei lavoratori e della tutela della privacy, in sostanza ha poi fondato la decisione, circa l'inutilizzabilità dei dati risultati dal sistema di controllo adottato (*Super Scout*), soltanto sulla violazione dell'art.4 dello stesso Statuto (ritenendo, peraltro, utilizzabili i tabulati rilevati direttamente dal computer). Il motivo, quindi, in quanto non attinente al reale *decisum*, […] risulta inammissibile.

Con il terzo motivo la ricorrente, denunciando violazione dell'art.4 citato e vizio di motivazione, in sostanza censura la sentenza impugnata nella parte in cui ha, appunto, ritenuto che nella fattispecie vi fosse stata una violazione della detta norma. Al riguardo, in particolare, la ricorrente in primo luogo deduce che "i dati posti a base della seconda contestazione non erano stati rilevati da alcun sistema di controllo, bensì dal diretto esame del computer della YYYY", per cui superflua era "qualsiasi dissertazione" sull'art.4.

Tale censura risulta inammissibile, in quanto anch'essa non attinente al *decisum*, giacché la violazione dell'art.4 dello Statuto è stata affermata in relazione al primo licenziamento, mentre per il secondo licenziamento la decisione è stata incentrata sulla tardività della contestazione. In secondo luogo, ed in generale, la ricorrente, premesso che "i controlli rivolti a esclusiva finalità di tutela del patrimonio aziendale ricadono al di fuori del campo di applicazione dell'art.4″ citato, lamenta che la Corte di merito avrebbe male interpretato ed applicato il detto articolo, in sostanza "parificando i controlli difensivi a quelli sull'attività lavorativa". Tale censura è infondata.

Come è stato affermato da questa Corte "ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dalla legge 300/1970, art.4, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o gli apparecchi di rilevazione di telefonate ingiustificate" (v. Cass. 3 aprile 2002, n.4746).

Il detto art.4, infatti, sancisce, al suo comma 1, il divieto di utilizzazione di mezzi di controllo a distanza sul presupposto – espressamente precisato nella Relazione ministeriale – che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

Lo stesso articolo, tuttavia, al comma 2, prevede che esigenze organizzative, produttive ovvero di sicurezza del lavoro possano richiedere l'eventuale installazione di impianti ed apparecchiature di controllo, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

In tal caso è prevista una garanzia procedurale a vari livelli, essendo l'installazione condizionata all'accordo con le rappresentanze sindacali aziendali o con la commissione interna, ovvero, in difetto, all'autorizzazione dell'Ispettorato del lavoro. In tal modo, come è stato evidenziato da Cass. 17 luglio 2007, n.15892, "il legislatore ha inteso contemperare l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro, o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi".

Con la stessa sentenza, è stato però precisato che la "insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore", per cui "tale esigenza non consente di espungere dalla fattispecie astratta i casi dei cd. controlli

difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso".

In tale ipotesi si tratta, infatti, comunque di un controllo cd. "preterintenzionale" che rientra nella previsione del divieto "flessibile" di cui all'art.4 citato, comma 2. Del resto, come già affermato da Cass. 18 febbraio 1983 n.1236, l'articolo in esame "disciplina distintamente le due ipotesi" delle apparecchiature finalizzate al controllo a distanza dell'attività dei lavoratori (comma 1) e delle apparecchiature richieste da esigenze organizzative e produttive ovvero della sicurezza del lavoro, "ma tali comunque da presentare la possibilità di fornire anche il controllo a distanza del dipendente", le prime assolutamente vietate, le seconde consentite "soltanto a condizione che il datore di lavoro osservi quanto tassativamente previsto".

Orbene sul punto l'impugnata sentenza si è attenuta a tali principi e con motivazione congrua e priva di vizi logici ha affermato che "i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento (se non altro, nel nostro caso, sotto il profilo del rispetto delle direttive aziendali)".

La Corte territoriale ha, altresì, aggiunto che "ciò è evidente laddove nella lettera di licenziamento i fatti accertati mediante il programma *Super Scout* sono utilizzati per contestare alla lavoratrice la violazione dell'obbligo di diligenza *sub specie* di aver utilizzato tempo lavorativo per scopi personali (e non si motiva invece su una particolare pericolosità dell'attività di collegamento in rete rispetto all'esigenza di protezione del patrimonio aziendale").

Sulla base di tali considerazioni la Corte legittimamente ha ritenuto applicabile nella fattispecie l'art.4, comma 2 citato, negando la utilizzabilità dei dati acquisiti dal citato programma in violazione di tale norma.

Con il quarto motivo la ricorrente, denunciando violazione delle disposizioni di cui al p.to 3 dell'allegato 2 al d.lgs. 626/1994, e all'art.615-*ter* c.p.c., nonché vizio di motivazione, in sostanza, posto che la YYYY era a conoscenza "sia del divieto di accesso ad Internet non giustificato da esigenze d'ufficio sia della riserva di controllo sulla osservanza del divieto formulata dalla società", in sostanza ritiene il controllo in esame legittimo in quanto effettuato non "all'insaputa" dei lavoratori e lamenta che erroneamente la sentenza impugnata avrebbe dato prevalenza alla norma dello Statuto dei lavoratori e non alla norma successiva del 1994.

La ricorrente, poi, assume che analogo argomento potrebbe ricavarsi dall'art.615-*ter* c.p.. Il motivo è infondato.

La normativa a tutela della sicurezza e della salute dei lavoratori sul luogo di lavoro del 1994 non ha in alcun modo modificato la disciplina "di base" a tutela della libertà e dignità del lavoratore, fissata dalla legge 300/1970, art.4. Le uniche regole in materia di "controlli a distanza" sono rimaste quelle dettate dall'art.4 dello Statuto, che, peraltro, è stato poi anche espressamente richiamato dal d.lgs. 196/2003, art.114.

Tanto meno, poi, ha inciso sulla norma statutaria la legge 547/1993, art.4, che ha introdotto il reato di cui all'art.615-*ter* c.p..

[…]

Il ricorso va, pertanto, respinto e la ricorrente va condannata al pagamento delle spese in favore della controricorrente.

[…]

9.5. 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 *email* 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, secondo comma, 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; par. 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. par. 3*);

c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art.11, comma 1, lett.b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza* (*par. 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 (*par. 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, secondo comma, Statuto dei lavoratori; allegato VII, par.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 *files* 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 *files 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 *files 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, secondo comma, l. n.300/1970*); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro 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, primo comma, legge 300/1970*), tra cui sono certamente comprese 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. É 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 *email*;
- 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 modificazione 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 utilizzi 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 *files*, 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; Provv.* 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 inconferenti 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 *files 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

Il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i *file* allegati – 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; 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, quarto comma, c.p.; art.49 Codice dell'amministrazione digitale*).

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;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, 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. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano 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 eventuale 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.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art.4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art.24, comma 1, lett.f, del Codice*);

b) in caso di valida manifestazione di un libero consenso;

c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul cd. bilanciamento di interessi (*art.24, comma 1, lett.g,, del Codice*).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art.26).

7.2. *Datori di lavoro pubblici*

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (*artt.18-22 e 112*).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (*art.7, comma 4, lett.a, del Codice*).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (*art.29 del Codice*).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. allegato B al Codice, regola n.19.6; Parere n.8/2001 cit., p.to 9).

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:

a) l'adozione e la pubblicizzazione di un disciplinare interno (p.to 3.2.);

b) l'adozione di misure di tipo organizzativo (p.to 5.2.) affinché, segnatamente:

- 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 *email*;

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;

[…]

10. INTERNET E PUBBLICA AMMINISTRAZIONE

10.1. Uso non corretto di Internet nella p.a. e danno erariale

Corte dei Conti, sez. giurisd. Piemonte, 13 novembre 2003, n.1856

[…]

In data 8 gennaio 2002, perveniva presso la Procura regionale di questa Corte per la Regione Piemonte denuncia da parte del Comune di Arona, in merito all'asserita condotta trasgressiva serbata dall'odierno convenuto, all'epoca dei fatti in servizio nel citato ente locale in qualità di Dirigente del 1° Settore "Gestione e sviluppo risorse".

Per quanto concerne la dinamica degli avvenimenti, giova evidenziare che, secondo quanto riferito nella menzionata segnalazione di danno, il Centro di elaborazione dati del Comune in parola aveva appurato, già da qualche tempo, che la rete informatica era stata oggetto di incursioni di virus provenienti da collegamenti Internet su siti non istituzionali.

Le registrazioni disponibili consentivano di individuare non soltanto la postazione lavorativa incriminata, quella del dr. R.M., ma anche il dettaglio di tutti gli accessi ad Internet nel periodo compreso tra l'1 giugno 2001 ed il 30 novembre 2001, con approfondita e specifica descrizione del tipo di sito visitato; i dati elaborati indicavano che il funzionario in narrativa si sarebbe collegato, ripetutamente e con sistematicità, a siti non istituzionali.

[…]

Diritto

[…]

Passando alla disamina delle motivate argomentazioni di merito poste a fondamento dell'azione di responsabilità da parte dell'Ufficio Requirente, e delle correlate controdeduzioni formulate dai difensori dell'odierno convenuto, il Collegio deve focalizzare la propria attenzione sulle considerazioni addotte dalla difesa circa il disconoscimento, l'inutilizzabilità e l'inefficacia probatoria dei documenti e dei dati posti a base della domanda di risarcimento della Procura regionale, l'estraneità del proprio assistito ai fatti che gli vengono addebitati, nonché l'arbitrarietà del criterio con il quale è stata quantificata la somma afferente al danno patrimoniale e la carenza di prova circa il contestato danno all'immagine.

Per quanto concerne la prima censura, incentrata sul divieto di utilizzare, da parte del datore di lavoro, impianti audiovisivi ed altre apparecchiature finalizzate a svolgere un controllo a distanza dei lavoratori, con conseguente violazione della normativa a tutela della privacy, questi Giudici ritengono che la stessa debba essere disattesa.

Il Collegio, infatti, non ravvisa nell'operato del Comune di Arona alcun comportamento invasivo preordinato al controllo recondito dell'attività del proprio dipendente, ma semplicemente l'impiego, con verifiche svolte *ex post*, di un tipo di *software* in uso a molte Pubbliche amministrazioni in grado di registrare i dati inerenti agli accessi degli utenti collegati alla rete, non solo per finalità di repressione di comportamenti illeciti, ma anche per esigenze statistiche e di controllo della spesa.

Del resto, non risulta che i controlli siano stati concomitanti all'attività lavorativa dell'odierno convenuto, ma sono stati disposti soltanto *a posteriori*, in funzione di significative e ripetute anomalie rappresentate da incursioni di virus provenienti da siti non istituzionali; l'utilizzabilità e l'efficacia nel presente giudizio dell'intero materiale probatorio raccolto, quindi, non può essere, ad avviso di questi Giudici, posta in discussione.

Relativamente alla seconda censura, quella concernente l'asserito difetto di responsabilità del proprio assistito, la difesa propugna la tesi secondo la quale altre persone ignote diverse dal convenuto avrebbero potuto avere facile accesso al PC in dotazione a quest'ultimo; il dr. R.M., ripercorrendo quanto esposto analiticamente nell'atto defensionale, era solito accendere il PC al mattino, per approntare subito tutti gli strumenti di lavoro, con spegnimento del medesimo alla sera, prima di lasciare l'ufficio. Durante la giornata, il Dirigente in parola era costretto, per motivi di servizio, ad assentarsi dalla postazione di lavoro, anche per diverse ore, allo scopo di recarsi in altri uffici o partecipare a riunioni, lasciando conseguentemente il PC in funzione ed abilitato al collegamento alla rete di Internet, essendo la "*password*" personale già inserita.

Le richiamate considerazioni si appalesano infondate e non possono trovare accoglimento.

Sulla specifica questione, il Collegio non condivide le conclusioni prospettate dalla difesa, relativamente all'asserita possibilità per la quale chiunque avrebbe potuto navigare in Internet con il PC in dotazione all'odierno convenuto e la "*password*" avrebbe potuto essere conosciuta da altri soggetti, quali gli addetti al C.E.D., sul rilievo che, se ciò non si può certamente escludere in via di fatto, residua, tuttavia, un comportamento negligente, inescusabile e gravemente colposo del dr. R.M., il quale, per sua espressa ammissione, si allontanava dal proprio ufficio per diverse ore al giorno lasciando il locale aperto ed il PC acceso, incustodito e con la parola chiave inserita. Il contegno serbato con sistematicità dal citato Dirigente, connotato dal mancato esercizio di quelle minime, possibili e semplici cautele procedimentali che la situazione richiedeva, da considerarsi oltremodo censurabile, poiché posto in essere da una figura lavorativa che ricopriva un ruolo di vertice nell'organigramma dell'ente locale, depone a favore di una diretta imputabilità del danno, sotto il profilo eziologico, all'odierno convenuto.

Tale assunto appare suffragato anche da un ulteriore particolare, non scevro di un elevato valore sintomatico: se, infatti, gli accessi ai siti non istituzionali effettuati dalla postazione del prefato dirigente non fossero stati dal medesimo compiuti, egli, in qualità di legittimo possessore del PC, avrebbe dovuto, verosimilmente, avvedersi dell'uso improprio da parte di ignoti dell'apparecchio in dotazione, comunicando le anomalie riscontrate ai competenti servizi dell'ente di appartenenza, considerato che l'utilizzo illecito si è protratto costantemente per alcuni mesi; risulta, al contrario, che i primi accertamenti sono stati avviati a seguito delle rilevazioni e delle conseguenti segnalazioni del C.E.D. del Comune di Arona.

Venendo all'esame della terza censura afferente alla presunta inattendibilità dei criteri utilizzati per la quantificazione del danno patrimoniale, occorre precisare che la Procura regionale, partendo dal dato richiamato in narrativa, che individua, alla luce della perizia tecnica del Prof. M. e degli accertamenti compiuti dal C.E.D. del Comune di Arona, in circa 250 ore il tempo di utilizzo non istituzionale di Internet da parte del dr. R.M., ha inteso avvalersi per la menzionata attività volta alla determinazione del danno, sebbene in forma stimata e forfetaria, di elementi obiettivi, quali l'ammontare della retribuzione in godimento ed il numero delle ore di navigazione sui vari siti non istituzionali. Atteso che lo stipendio mensile lordo del convenuto ammontava a lire 8.500.000 e che lo stesso risulta aver effettuato nel periodo considerato, in media, 36 ore settimanali, con una retribuzione oraria pari a lire 59.000, l'Ufficio requirente ha quantificato il danno patrimoniale, ottenuto moltiplicando la predetta misura oraria per il totale delle ore trascorse collegandosi a siti non istituzionali (250), in lire 14.750.000, cui sono state aggiunte, applicando sempre un procedimento induttivo, lire 500.000 a titolo di costo del servizio telefonico *pro quota*.

Ribatte la difesa che le rilevazioni dei *files* di "*log*", se da un lato consentono di verificare l'esistenza e la durata di un collegamento alla rete, non sono ovviamente in grado di dimostrare che il soggetto connesso sia, in quel determinato intervallo temporale, dedito esclusivamente alla consultazione del sito ricercato, ben potendo dedicarsi ad ogni altra attività lavorativa rientrante nelle proprie mansioni, pur se il PC rimane, durante le ore medesime, collegato ad Internet; in altre parole, non sarebbe in alcun modo possibile ritenere accertata e provata la precisa coincidenza tra ore di collegamento e ore prive di qualsivoglia prestazione lavorativa, per trarre l'esistenza e l'entità di un danno che, in base soltanto ai suddetti elementi, non è determinato, né logicamente determinabile.

In merito al profilo della determinazione del danno patrimoniale, il Collegio muove da un dato oggettivo, nonostante le osservazioni critiche inerenti al grado di sicurezza della rete formulate nella perizia di parte privata stilata da […], da reputarsi sufficientemente preciso, acclarato con dovizia di argomentazioni tecniche dalla relazione del Prof. M. e dai rilevamenti elaborati dal C.E.D. del Comune di Arona: dal PC in uso all'odierno convenuto sono stati effettuati accessi a siti non istituzionali della rete Internet pari a circa 250 ore di collegamento nel periodo interessato; tali connessioni, in ragione di quanto precedentemente esposto circa il comportamento gravemente colposo del dr. R.M., associato alla circostanza corroborante attinente all'esame incrociato del riepilogo delle giornate di presenza e degli orari di entrata e di uscita dello stesso, sono da ritenersi direttamente imputabili al dirigente in parola.

In tale quadro complessivo, inoltre, il Collegio intende dissentire con forza dall'affermazione della difesa secondo la quale non sarebbe rilevante, ai fini del danno, il tempo trascorso da un Dirigente in attività non attinenti al proprio servizio, in quanto le figure in parola negli enti locali, a differenza degli altri dipendenti, non devono rendere una prestazione lavorativa quantificabile con orario minimo, ma sono tenuti esclusivamente ad un'obbligazione di risultato. Se è vero, infatti, che

la funzione del Dirigente è improntata ad una certa flessibilità nell'orario di lavoro, non può sottacersi la circostanza che l'attività di tali soggetti comporta, indubbiamente, una maggiore responsabilità che si riflette in modo diretto sulla stessa durata ed articolazione delle prestazioni lavorative, diversamente dagli altri dipendenti che agiscono, in linea di massima, sulla base di una programmazione lavorativa predefinita; il riferimento all'espletamento di un'obbligazione di risultato, non affranca certamente il Dirigente dall'obbligo giuridico di utilizzare il tempo trascorso in ufficio per il conseguimento dei fini istituzionali, anche in virtù della posizione di vertice ricoperta che deve fungere da esempio per i propri collaboratori.

In altri termini, e con maggiore ampiezza esplicativa, questi Giudici reputano non rispondente ai canoni dell'efficienza e dell'efficacia della prestazione lavorativa da rendere a fronte della retribuzione percepita, lo svolgimento del lavoro di ufficio che presenti continue parentesi temporali dedicate alla connessione a siti non istituzionali della rete Internet, quantomeno in relazione alle ore interessate dall'attività in rassegna.

Ciò premesso, partendo dai cennati presupposti emersi nell'ambito dell'evocata cornice ricostruttiva, il Collegio, pur valutando corretto il parametro dedotto dalla Procura regionale, poiché appare quello che più di ogni altro conserva nel suo alveo un fondamento di natura oggettiva, laddove si richiama alla retribuzione oraria del soggetto, non condivide, tuttavia, la quantificazione del danno patrimoniale derivante dalla correlata operazione di calcolo matematico effettuata dalla parte pubblica, in quanto il criterio prescelto non è idoneo a provare in modo inoppugnabile, come prospettato dalla difesa del convenuto, la perfetta corrispondenza tra le ore di collegamento alla rete Internet rilevate, il cui numero può considerarsi pressoché certo, e le ore prive di prestazione lavorativa; la stessa Procura regionale definisce tale valutazione stimata e forfetaria. A tal proposito, infatti, non si può escludere che alcune connessioni ai siti non istituzionali siano rimaste attive per diversi minuti nel corso di ciascuna giornata, anche per mera dimenticanza, nel periodo in cui il predetto Dirigente svolgeva le proprie funzioni istituzionali in ufficio o presso altri luoghi, lasciando il PC sempre acceso sin dalla mattina come evidenziato nell'atto defensionale.

In relazione alle delineate osservazioni in ordine alla quantificazione del danno, il Collegio ravvisa la necessità di ricorrere, nella fattispecie in esame, al potere equitativo demandato dall'art.1226 c.c., riducendo l'importo contestato dalla Procura regionale a tale titolo e ritenendo raggiunta la prova a carico dell'odierno convenuto di un danno patrimoniale per l'importo di euro 5.000,00, comprensivi di rivalutazione monetaria ed interessi, in base alle risultanze del procedimento penale, della perizia tecnica redatta dal Prof. M. e dei rilevamenti elaborati dal C.E.D. del Comune di Arona.

[…]

Quanto alla contestazione afferente al supposto danno all'immagine, prescindendo dal vaglio relativo alla prova dello stesso, individuabile nei noti criteri oggettivi, soggettivi e sociali e nei canoni di carattere generale contenuti nella recente decisione delle Sezioni Riunite di questa Corte n.10/QM/2003, il Collegio valuta la pretesa avanzata dalla parte pubblica infondata, sul rilievo assorbente che le notizie dell'episodio concernente la connessione a siti non istituzionali da parte dell'odierno convenuto sono state divulgate agli organi di stampa dal Comune danneggiato, per cui difetta, a monte, una delle stesse condizioni per promuovere l'azione di responsabilità per tale voce di danno, atteso che la diffusione delle informazioni potenzialmente pregiudizievoli è riconducibile esclusivamente all'ente locale che dovrebbe essere risarcito.

Per quanto esposto in narrativa, il Collegio condanna l'odierno convenuto al pagamento in favore dell'Erario della somma di euro 5.000,00, comprensivi di rivalutazione monetaria ed interessi.

[…]

10.2. Uso non corretto di Internet nella p.a. e danno da disservizio

Corte dei Conti, sez. giurisd. Basilicata, 22 marzo 2006, n.83

[…]

Con atto di citazione del 14 dicembre 2004, preceduto da rituale invito a dedurre *ex* art.5, comma 1 della legge 19/1994, la Procura regionale della Corte dei conti per la Basilicata conveniva in giudizio i signori Tizio e Caio, nella qualità di Operatori amministrativi in servizio presso la Direzione provinciale del lavoro di Potenza, chiedendo che gli stessi venissero condannati al risarcimento, in favore dell'Erario, della somma complessiva di euro 22.953,66, corredata da interessi legali, rivalutazione monetaria e spese di giudizio.

Il danno contestato agli odierni convenuti traeva origine da una segnalazione da parte dell'amministrazione di appartenenza, per fatti, riferibili al periodo 2001/2003, e così sintetizzabili. Nell'autunno del 2003 veniva accertata la presenza di un "virus" nella rete informatica della Direzione provinciale del lavoro di Potenza; la successiva opera di "bonifica" svolta dalla ditta specializzata incaricata e dalla Polizia postale al fine di eliminare il predetto "virus" ed, altresì, accertare la causa dei problemi insorti, aveva consentito di verificare che i *computers* erano stati infettati a seguito dell'installazione di giochi e software non autorizzati e a causa dell'illecita navigazione su "siti Internet" a carattere pornografico, effettuata da "*workstations*" operanti all'interno dell'ufficio; la contrazione del virus risultava coincidere, peraltro, con la data di apertura di tabelle di Excel utilizzate per la non autorizzata esecuzione di operazioni non pertinenti con l'attività lavorativa ovvero per la creazione di "*files*" riguardanti fatture relative a ditte private. Il "virus" successivamente, si era poi propagato nell'ambito della *LAN* dell'amministrazione ed aveva infettato i sistemi operativi.

[…]

Diritto

La Sezione è oggi chiamata ad adottare una decisione su una vicenda che involge, da un lato, la tematica diffusa della corretta utilizzazione di beni strumentali in dotazione alla pubblica amministrazione e, da altro lato, la ricerca di precisi ed attendibili momenti di collegamento causale tra verificazione dell'evento dannoso e condotta personale serbata in un settore operativo, quale è quello informatico, in cui il rischio di una "multifattorialità" causale, letta in chiave di pluralità ed indeterminabilità di apporti soggettivi, nell'impropria utilizzazione dello strumento informatico, è indubbiamente elevato.

La validità di tale premessa "introduttiva" è confermata dalla circostanza che vede tanto la relazione tecnica di parte convenuta, quanto la memoria difensiva che quella recepisce, adombrare la possibilità, manifestandosi come incontrovertibile la prova dell'intervenuto collegamento attraverso Internet con siti non istituzionali, che altri soggetti abbiano potuto utilizzare le postazioni di lavoro degli odierni convenuti sì da attribuire formalmente ad essi la responsabilità dell'illecita condotta.

Nella ricerca risolutoria di tale delicata e complicata premessa operativa, utile viatico appare essere a questo Giudice il contenuto delle relazioni amministrative e tecniche che si sono soffermate sulla vicenda oggi all'esame, e redatte in sede di denuncia disciplinare e di procedimento penale.

Prima, tuttavia, di esaminarne e valutarne i tratti significativi e rilevanti ai fini della compiuta definizione del procedimento giurisdizionale rimesso a questo Giudice, occorre precisare entità e dinamica del danno contestato dalla Procura regionale agli odierni convenuti, onde agevolare la successiva attività attributiva in termini di personale responsabilità.

Dalla narrativa che precede in fatto può così ricavarsi che l'attore pubblico ha individuato tre distinte partite di danno, ritenute tutte riconducibili all'impropria utilizzazione degli strumenti informatici da parte del Caio e del Tizio.

La prima, di euro 2.280,00 legata ai costi sostenuti dall'amministrazione per restituire funzionalità al sistema informatico"alterato" e reso inutilizzabile a causa della contrazione del virus della categoria "*blaster*" del tipo *Mslaugh.exe* (cd. "operazione di bonifica");

la seconda, di euro 9.159,60, legata alla conseguente necessità di predisporre, ad opera e cura dell'amministrazione penalizzata e danneggiata dall'arresto del sistema informatico a sua

volta causato dall'immissione del suddetto "virus", un sistema di protezione della rete locale idoneo ad evitare la ripetizione di analoghi episodi (cd. "sistema antivirus");

la terza, determinata in euro 11.439,60, alla stregua di un criterio equitativo che prende a riferimento la somma delle prime due voci di danno – diretto ed indiretto – di immediata e comprovata quantificazione, discendente dal disservizio cagionato sull'ordinato e lineare svolgimento dell'attività istituzionale dell'amministrazione danneggiata dalle illecite condotte dei convenuti che avevano integrato, nell'utilizzare parte del proprio orario di lavoro, ed in modo improprio gli strumenti operativi di cui erano stati dotati, una patente violazione dei doveri del proprio ufficio, totalmente affrancandosi dal rispetto delle regole deontologiche poste a presidio dell'integrità strutturale e funzionale del rispettivo rapporto di lavoro.

La prima voce di danno, ascendente ad euro 2.280,00, rappresenta, come anticipato sopra, il costo sostenuto dalla Direzione provinciale del lavoro di Potenza, per "bonificare" il sistema informatico dei propri uffici, e reso inutilizzabile dall'immissione di un virus della categoria "*blaster*" per effetto dell'avvenuta esecuzione di operazioni assolutamente non correlate ai compiti d'Istituto.

La predetta somma costituisce il corrispettivo liquidato e pagato alla ditta […] che aveva eseguito i necessari lavori di riparazione del sistema, così consentendo la ripresa della piena funzionalità di tutti gli strumenti informatici che avevano subito, per circa un mese – e precisamente dal 22 ottobre 2003 al 26 novembre 2003 – una forzata inattività a causa della propagazione del virus.

La descritta spesa costituisce certamente una fattispecie di danno ingiusto, non essendo correlata ad alcuna esigenza di ordinaria funzionalità dell'apparato organizzativo dell'amministrazione, e manifestandosi anzi come il frutto di un evento – la contrazione di un virus con modalità accertate come non pertinenti all'attività istituzionale – che poteva e doveva essere previsto, e dunque evitato.

Dai dati emergenti dall'elevato contenuto tecnico delle rassegnate relazioni peritali più sopra richiamate, è possibile affermare che il virus che ha determinato, in successiva propagazione, l'arresto e la temporanea inutizzabilità del Sistema in dotazione alla Direzione provinciale del lavoro di Potenza, è stato contratto dal computer assegnato al dipendente Tizio, attraverso la copia di "*files*" non funzionali assolutamente all'attività lavorativa.

Costituisce prova, e non mero indizio, di quanto affermato la rilevata coincidenza delle date di contrazione del "virus" della categoria "*blaster*" *Mslaugh.exe* con quelle in cui venivano effettuate le operazioni di copia di "*files*" relativi a fatture ricomprese in un programma di contabilità privata non pertinente con l'attività lavorativa svolta dal Tizio.

La predetta circostanza, corroborata da inconfutabili riscontri tecnici eseguiti in sede di ricognizione dalla ditta incaricata della operazione di "bonifica" del sistema informatico, consente, ad avviso di questo Giudice, di ricondurre alla personale responsabilità del Tizio il danno derivante dall'ingiustificata spesa sostenuta dalla Direzione provinciale del lavoro di Potenza per la riattivazione del sistema.

E la condotta serbata dal Tizio nella fattispecie in esame si manifesta come connotata da colpa grave in quanto, pur non essendo evidentemente preordinata alla contrazione del "virus", è tuttavia segnata dalla piena e consapevole volontà di utilizzare uno strumento informatico in dotazione dell'Ufficio presso il quale egli prestava servizio, e quindi annoverabile tra i beni strumentali all'ottimale esecuzione ed adempimento di compiti strettamente istituzionali, per realizzare invece scopi e finalità di carattere eminentemente personale: l'evento dannoso in questo modo verificatosi – contrazione e propagazione successiva del virus con i conseguenti ingiustificati costi – rappresenta così la conseguenza prossima, prevedibile ed evitabile, dell'iniziale condotta volitiva.

Il Tizio poteva e doveva astenersi dall'eseguire operazioni non pertinenti con l'attività lavorativa propria tanto in ragione del generalizzato dovere di osservanza delle regole organizzative dell'Ufficio che non consentono lo svolgimento di operazioni diverse da quelle riconducibili alle mansioni assegnate, quanto, e soprattutto, in virtù della conoscibilità dei pericoli derivanti dalla non corretta utilizzazione del sistema informatico, conoscibilità resa possibile dall'intervento di specifiche comunicazioni diramate dalla Direzione provinciale del lavoro di Potenza in data 8 novembre 2000 e 22 marzo 2002, ed indirizzate al personale tutto della sede locale.

In esse, infatti, richiamandosi l'intervenuta verificazione di alcuni episodi di alterazione di *computers*, si sollecitava una più rigorosa osservanza delle regole disciplinanti il corretto uso degli

strumenti informatici, con esplicito invito ad astenersi dall'installazione di versioni di sistemi operativi diversi da quelli già esistenti ed autorizzati dal Ministero, e tanto al fine di non arrecare danni al sistema.

Il significato di tali "avvertimenti", che evidentemente non escludevano la possibilità che un "virus" potesse essere contratto anche attraverso l'ordinaria e consentita utilizzazione del sistema informatico, (circostanza, questa, conosciuta ed ammessa in tesi anche da questo Giudicante), ma che tuttavia evidenziavano l'indice di maggiore probabilità verificatoria di guasti connessi con l'uso di programmi cd. "non consentiti", doveva essere vieppiù percepito come rilevante da parte di un soggetto che, come il Tizio, era ed è titolare di approfondite e specifiche competenze settoriali.

L'inosservanza di tali elementari e specifiche regole precauzionali – peraltro, perfettamente e pienamente conosciute o riconoscibili – da parte del Tizio rende la condotta dal medesimo tenuta nel caso di specie come connotata da colpa grave, e dunque meritevole della sanzione risarcitoria prevista dal sistema di tutela della responsabilità amministrativa di cui questo Giudice è espressione.

Nell'individuare ed affermare la responsabilità del Tizio per la provocata – in modo gravemente colpevole – contrazione del "virus", il Collegio si determina nell'attribuire solo ad esso l'intero danno di euro 2.280,00 derivante dal costo sopportato dall'amministrazione per la necessaria riattivazione del sistema informatico: pertanto, viene ad essere disattesa, su tale specifico aspetto, la richiesta dell'attore pubblico di paritaria ed eguale attribuzione ad entrambi gli odierni convenuti Tizio e Caio della suddetta partita di danno.

Una volta esclusa la diretta responsabilità personale del Caio per l'avvenuta contrazione, ed il successivo contagio o propagazione del "virus", il Collegio deve soffermarsi ad analizzare ed esaminare la condotta a questi contestata dalla Procura regionale locale per la ricerca e conseguente affermazione della responsabilità discendente dal "disservizio" recato alla struttura operativa dell'amministrazione di appartenenza.

Anche in questo caso il Collegio utilizza, ai fini di informata ed effettiva giustizia, gli elementi cognitivi e tecnici risultanti dalle più volte richiamate relazioni peritali, e dalle quali si ricava la certezza dell'assenza di ogni attinenza della quasi totalità (90%) dei siti visitati dal Caio con il lavoro svolto dal medesimo, trattandosi di siti "a carattere pornografico". Analoga ricerca, pure svolta sul computer del Tizio, non ha invece prodotto alcun utile risultato, essendo emersa l'intervenuta cancellazione di ogni traccia riferita ai siti "Internet" visitati dal medesimo.

La ricerca effettuata con successo ha consentito,così, di "mappare" tutti i collegamenti effettuati dal Caio nel periodo 10 dicembre 2002 – 11 novembre 2003 con indicazione delle date e dell'ora di collegamento.

Dagli stessi dati emerge che i siti "illeciti" visitati sono circa 400, e che il tempo ad essi dedicato dal Caio – complessivamente – è di circa 30 ore, ovviamente distribuite nei vari giorni del periodo considerato.

Il costo complessivo del collegamento telefonico utilizzato per attivare le suddette "improprie" connessioni risulta essere stato di euro 32,73.

Le relazioni pongono, infine, in evidenza come le analoghe indagini svolte sul PC del Tizio non abbiano consentito di individuare alcun collegamento a siti "Internet": tale circostanza viene definita dal perito nominato dalla Procura della Repubblica presso il Tribunale di Potenza nell'ambito dell'indagine penale da questa svolta per il perseguimento dei reati di cui agli artt.81 e 314 c.p. come assolutamente anomala, e tecnicamente inverosimile, se non ipotizzando ed ammettendo l'intervento di una successiva ed abile attività di manomissione della memoria, anche remota, del PC del Tizio, che manifesta l'intenzione, da parte dell'utente, di non voler mostrare, o comunque rendere visibili, i siti visitati.

L'operazione di "ripulitura" non è invece stata effettuata nel PC del Caio, e tale circostanza consente così a questo Giudice di poter procedere alla valutazione dell'entità e del rilievo attribuibile, ai fini dell'affermazione della responsabilità amministrativa, alla dimostrata impropria utilizzazione del suddetto computer da parte del suddetto convenuto.

A tale riguardo, il Collegio richiama, in premessa, i tratti essenziali e qualificatori della figura, di elaborazione giurisprudenziale, del cd. "danno da disservizio".

Esso si sostanzia, come già affermato in precedenti pronunce di questa stessa sezione giurisdizionale, nel danno patrimoniale che deriva dalla minore e non corretta resa della spesa sostenuta dalla pubblica amministrazione in termini di efficienza–risultato dell'azione amministrativa.

E, nel caso in esame, la spesa priva di utile e proficua correlazione comprende tanto l'onere retributivo posto a carico della pubblica amministrazione in adempimento dell'obbligazione contrattuale nascente dal rapporto di lavoro con il dipendente, quanto il costo "strutturale" della corretta Installazione, manutenzione e gestione del Sistema informatico, che è bene strumentale volto all'ottimizzazione dell'attività amministrativa verso il conseguimento della migliore qualità del servizio pubblico.

Nel caso di accertato "disservizio", le risorse, finanziarie e strumentali, impiegate dalla pubblica amministrazione per l'attualizzazione delle finalità che le sono proprie, e che sono intimamente connesse con i principi di legalità, efficienza, efficacia, economicità e produttività, risultano sprecate e dunque dannosamente impiegate, perché alla fine sprovviste di ogni utilità ordinariamente ritraibile dal corretto impiego delle stesse.

La descritta alterazione del rapporto esistente tra risorse e/o spese, da un lato, e efficienza e/o risultato, dall'altro lato, richiama all'attenzione dell'interprete altre considerazioni, significativamente rilevanti per la corretta affermazione della responsabilità amministrativa rinvenibile nella descritta dinamica operativa degenerata o involuta.

La prima attiene all'individuazione dell'interesse pubblico danneggiato ed oggetto di "sanzione risarcitoria": il Collegio ritiene di poter affermare che il conseguimento della finalità dell'azione amministrativa secondo i ricordati canoni di efficienza, economicità, produttività ed efficacia costituisce un vero e proprio bene del patrimonio della pubblica amministrazione che, anche se non suscettibile di immediata percezione materiale, al pari di un bene mobile o immobile, è pacificamente riconducibile a quel complesso di interessi e di ricchezze costituenti il precipitato procedimentale e provvedimentale dell'azione della pubblica amministrazione, ed in quanto tali riconducibili ad una dimensione ampia di patrimonio pubblico.

Tale dimensione appare, peraltro, perfettamente e compiutamente aderente con il principio costituzionale contenuto nell'art.97 Cost. che valorizza in chiave costituzionale tanto il buon andamento dell'organizzazione amministrativa nel momento procedimentale, quanto in quello del risultato finale.

La seconda attiene, invece, alla valutazione dell'elemento soggettivo richiesto nella particolare ipotesi della verificazione del danno da disservizio, e dunque della connotazione psicologica caratterizzante la condotta tradottasi nel "desostanziamento" del servizio prestato verso la pubblica amministrazione. Il Collegio osserva come in tale ipotesi al soggetto agente sia richiesto un comportamento aderente agli obblighi e ai doveri nascenti dal rapporto di servizio, tra i quali vi è quello di curare "…. in conformità delle leggi, con diligenza e nel miglior modo, l'interesse dell'amministrazione per il pubblico bene" (art.13, d.p.r. 10 gennaio 1957, n.3).

L'efficienza diviene così modalità di svolgimento dell'attività amministrativa da parte del soggetto agente e si rivela idonea a costituire parametro di valutazione dell'antigiuridicità della condotta in relazione all'elemento soggettivo.

In altre parole, la distorta o non corretta utilizzazione delle risorse strumentali della pubblica amministrazione da parte dell'impiegato, compromette la definizione ottimale del risultato amministrativo finale cui le stesse sono preposte, provoca la lesione di un bene del patrimonio pubblico – il risultato finale dell'azione amministrativa – e viola la regola dell'efficienza che è normativamente preordinata alla ottimale cura dell'interesse della pubblica amministrazione "per il pubblico bene".

La condotta tenuta dal Caio, che è consistita nell'utilizzazione del proprio PC, in diversi e ben individuati momenti dell'attività lavorativa, per scopi diversi da quelli istituzionali, integra pienamente la fattispecie di danno da disservizio ora delineata nei suoi tratti generali.

Né vale ad escludere, ad avviso di questo Giudicante, o a ridurre la responsabilità dell'odierno convenuto, la circostanza, pure eccepita dalla difesa con specifico richiamo alle riflessioni dubitative formulate dal perito nominato dai convenuti, secondo la quale altri soggetti avrebbero potuto accedere ai siti "illeciti" dalla postazione di lavoro del Caio, sfruttando l'assenza di questi che, in alcune delle date in cui risultano essere stati visitati i suddetti siti, sarebbe ampiamente comprovata.

Questo Giudice, al riguardo, afferma come sia intimamente connesso alla corretta utilizzazione di un bene strumentale in dotazione dell'Ufficio, rimesso alla personale e responsabile gestione dell'utente che ne sfrutta potenzialità e capacità per l'ottimizzazione della propria attività lavorativa, ad esso destinando, e da esso ricevendo, materiale e documentazione caratterizzata da

elevata "sensibilità" professionale e lavorativa, l'obbligo di predisporre adeguate cautele che impediscano ad altri di farne un uso improprio.

La stessa previsione di una "chiave di accesso" al PC richiama l'esigenza di assicurare riservatezza ed inviolabilità nella gestione dello strumento informatico.

La mancata predisposizione di tali minime cautele oltre a manifestare scarsa diligenza nella cura di un bene pubblico, si traduce nella colpevole accettazione del rischio di manomissioni dello stesso da parte di terzi non autorizzati, in aperta violazione delle regole poste a presidio della responsabile gestione di tutti i beni, servizi e risorse strumentali e professionali poste a disposizione dell'impiegato per l'ottimale espletamento delle proprie mansioni.

Poste queste premesse, e passando all'esame della condotta serbata dal Caio, così come conclamatasi dalle tracce conservate nella rete informatica, questo Giudice può affermare che la stessa si è tradotta certamente in una profonda e significativa alterazione dei contenuti propri del servizio, o della prestazione che questi doveva assicurare all'amministrazione controparte del rapporto di lavoro, in ragione del vincolo sinallagmatico che fissava, in termini di reciprocità, diritti e doveri strutturalmente e funzionalmente ricompresi nel lineare ed ordinato svolgimento dell'attività lavorativa.

E tale fenomeno degenerativo del rapporto di servizio, lungi dal ridursi nell'area del minor conseguimento di obiettivi dell'azione amministrativa, ovvero del mancato conseguimento dei risultati idealmente ed istituzionalmente legati alla spesa sostenuta dall'amministrazione per assicurare la controprestazione retributiva, finisce con il manifestarsi in forme articolate e complesse che pongono in evidenza una vera e propria "disaffezione" dai propri compiti di servizio, frutto di volontaria e premeditata predisposizione di espedienti tecnici ed operativi protesi a consentire un'utilizzazione di strumenti e di beni della pubblica amministrazione del tutto avulsa dalle finalità istituzionali che ne caratterizzano invece il corretto uso.

La conosciuta atipicità del danno derivante dal "disservizio" recato alla struttura ordinamentale e funzionale dell'attività della pubblica amministrazione, consente a questo Giudicante di attribuire ad essa tratti, lineamenti e significati che, se pure diversi ed originali in ragione della specificità dell'alterazione procedimentale e sinallagmatica di volta in volta registrata, risultano tutti cementati ed uniformati dal comune denominatore del danno ingiusto recato ad un bene pubblico, "*recte*": ad un bene ricompresso nel patrimonio della pubblica amministrazione, costituito dal buon andamento amministrativo, che è valore tutelato dalla Costituzione in quanto ritenuto modello operativo ineliminabile per l'ottimale e compiuto conseguimento di obiettivi pubblici.

Nel contesto di tale premessa argomentativa, l'emergenza del danno, e la conseguente reazione dell'ordinamento, non potrà esser circoscritta negli angusti limiti della pur intervenuta alterazione del rapporto sinallagmatico e nelle conseguenze ad esso ascrivibili in termini di "esito finale" dell'attività procedimentale deviata, ma dovrà soffermarsi, nell'attenta e particolareggiata disamina delle attività precedenti, concomitanti e successive alla condotta "*ictu oculi*" dannosa, sull'effettiva portata di una vera e propria attività di affrancamento dal modello ordinamentale ed istituzionale voluto dal legislatore.

Così, nel caso in esame, il disservizio non è solo il danno che emerge dal tempo impiegato nella "navigazione" e nella visita dei siti che eufemisticamente si definiscono "non istituzionali", con conseguente sottrazione dell'impegno lavorativo invece destinato al corretto assolvimento degli obblighi istituzionali, ma si rivela e si manifesta nelle fattezze di un vero e proprio "*modus cogitandi*" e "*modus operandi*" per la cui integrazione occorre destinare non una parte della propria attività lavorativa, ma modellare invece la stessa per precostituirsi condizioni, modelli di conoscenza, espedienti e tecniche di salvaguardia che finiscono per assurgere al ruolo di obbiettivo primario della prestazione lavorativa.

In diverse parole, il danno da disservizio derivante da impropria utilizzazione, continua, costante e pervicace, di un bene della pubblica amministrazione, nella specie di uno strumento informatico, costituisce, solo nel suo risultato immediatamente percepibile, la visibile manifestazione finale dell'intrapresa e definita deviazione dall'ordinato svolgimento della prestazione lavorativa, ma, nella realtà della personale e complessiva organizzazione dell'attività amministrativa, esso si arricchisce e si alimenta di ben più gravi e consistenti "deviazioni" costituite dalla necessità di organizzare, per il conseguimento del voluto scopo illecito, un modello di articolazione lavorativa ed organizzatoria del tutto avulso e, per così dire, "alternativo", rispetto a quello istituzionalmente preordinato al conseguimento del valore pubblico.

Per quanto, poi, attiene alla determinazione del danno, questo Giudice, in assenza di criteri probatori, sì come derivanti dalla vastità e complessità del bene leso dalla condotta dell'agente, decide di procedere, ai sensi dell'art.1226 c.c. alla quantificazione dello stesso "*ex bono et aequo*", cioè secondo equità.

[…]

Aderendo a tali criteri, rilevato che il numero delle ore dedicate all'effettiva visita dei circa 400 siti illeciti da parte del Caio risulta accertato in poco meno di 30, dispiegate nell'arco di 11 mesi, e considerato, altresì, che a tali ore vanno aggiunti i tempi di preparazione – antecedenti – e di adeguata e piena ripresa dell'attività lavorativa ordinaria – successivi – questo Giudice ritiene di poter quantificare il danno provocato al "servizio" dell'amministrazione pari a euro 100,00 per ogni ora, somma che ricomprende anche i costi dei collegamenti telefonici attivati, nonché "l'usura" dello strumento informatico scorrettamente utilizzato ed il pregiudizio della mancata utilizzazione dello stesso per i fini istituzionalmente propri, rivelandosi la deviazione dall'uso ordinario come un vero e proprio inadempimento contrattuale dal quale emerge una prestazione del tutto diversa ("*aliud pro alio*") da quella invece ritraibile dalla messa a disposizione dell'utente dello Strumento informatico.

Il danno addebitabile al Caio può così essere quantificato in euro 3.000,00 già rivalutati (euro 100,00 X n.30 ore).

La predetta somma di euro 3.000,00 va addebitata anche al Tizio, nella composizione costituita dall'accertato danno di euro 2.280,00 derivante dal costo sostenuto dall'amministrazione per la "bonifica" del sistema, secondo quanto motivato "*supra*", e di euro 720,00 per il disservizio arrecato all'amministrazione dalla solo parzialmente comprovata utilizzazione del proprio PC per fini diversi da quelli istituzionali: per l'intervenuta integrazione di tale danno si ritengono validi i principi sul punto già espressi per l'esistenza del danno da disservizio a carico del Caio; relativizzati, ovviamente, al diverso contenuto dei siti visitati ed alle diverse modalità di "utilizzazione alternativa" utilizzate dal Tizio, in relazione al quale gli accertamenti svolti hanno rilevato l'avvenuta predisposizione di un programma creato per la gestione di una contabilità aziendale, contenente fatture e documentazione commerciale del tutto estranea all'attività di istituto.

Il Collegio, infine, reputa di non poter considerare, come invece richiesto dall'attore pubblico, voce di danno, addebitabile agli odierni convenuti, la spesa sostenuta dalla Direzione provinciale del lavoro di Potenza per la doverosa, e semmai tardiva, predisposizione di un sistema di adeguata salvaguardia del circuito informatico dall'aggressione di "virus" in grado di minarne la funzionalità.

È infatti di tutta evidenza come l'approntamento di siffatti sistemi di sicurezza si riveli oggi indispensabile, in ogni struttura in cui sia operante una rete informatica, per garantire la corretta funzionalità del sistema stesso, preservandolo da intrusioni di "infezioni informatiche" ipoteticamente veicolabili anche da informazioni o da siti istituzionali, e dunque "leciti", nonché dalla vasta congerie di posta elettronica che quotidianamente viene recapitata verso la totalità degli indirizzi conosciuti. La predetta spesa, pertanto, non risulta, ad avviso di questo Giudice, assolutamente annoverabile tra le ipotesi di danno al patrimonio della pubblica amministrazione, rivelandosi, al contrario, e nell'attuale contesto di elevata elaborazione informatica, doverosa e necessaria.

[…]

10.3. Uso di posta elettronica ed Internet nella p.a. e peculato

Corte di Cassazione, sez.VI penale, 21 maggio 2008, n.20326

[…]

All'indagato - dipendente del Comune di Trani - era stato contestato il reato di peculato perché si serviva del computer dell'ufficio, cui era collegato un masterizzatore DVD, per uso personale usufruendo della rete elettrica e informatica del Comune: navigava in Internet su siti non istituzionali, scaricando su archivi personali dati e immagini non inerenti alla pubblica funzione - prevalentemente materiale di carattere pornografico - con danno economico dell'ente.

Sul computer in questione e sul sopporto esterno, venivano rinvenuti circa 10.000 documenti di cui solo una minima parte di natura lavorativa.

Il Tribunale, nel revocare la misura cautelare, osservava che il reato di peculato tutela il patrimonio della P.A. e che lo stesso non poteva essere depauperato a seguito dei collegamenti in questione di un computer "comunque e sempre collegato alla rete elettrica e telefonica indipendentemente dall'uso e dalla navigazione". Con particolare riferimento al collegamento alla rete elettrica, non si era "indicato il danno patrimoniale", atteso che "i *computers* sono sempre collegati alla rete elettrica, né può ritenersi ulteriore consumo di energia elettrica per il fatto che a un computer siano collegate una o più periferiche".

Il Tribunale disconosceva anche la sussistenza di esigenze cautelari perché "pur ritenendo un danno patrimoniale per l'ente per la navigazione in Internet sino al 2003" (il consulente tecnico aveva accertato che la navigazione in Internet si arrestava al giugno 2003) non era ipotizzabile un pericolo di reiterazione "in considerazione della sua illibata personalità e dell'atteggiamento pacatamente esplicativo tenuto in occasione del suo interrogatorio.

Avverso la predetta ordinanza propone ricorso per Cassazione il Procuratore della Repubblica presso il Tribunale di Bari il quale richiama tutta la giurisprudenza di questa Corte di Cassazione che ritiene che con il reato di peculato non sia offeso solo il patrimonio dell'ente pubblico, ma anche il buon andamento degli uffici della pubblica amministrazione il quale può non essere turbato solo da un uso occasionale della cosa pubblica, ma non in caso di condotta reiterata e consolidata nel tempo. Peraltro, non risultava affatto accertato agli atti del processo se il contratto del Comune con l'ente gestore di Internet prevedesse un uso illimitato del servizio con tariffa fissa, circostanza per nulla verificata da parte dei giudici di merito, ma solo supposta. Del tutto inadeguata appariva infine la motivazione sulle esigenze cautelari sopra riportata.

Premesso che l'ordinanza impugnata sembra quasi trascurare la circostanza che la disposizione dell'art.314 c.p., oltre a tutelare il patrimonio della pubblica amministrazione mira ad assicurare anche il corretto andamento degli uffici della stessa basato su un rapporto di fiducia e di lealtà col personale dipendente, secondo la costante giurisprudenza di questa Corte, il Tribunale del riesame dà per scontato un dato che non emerge affatto dagli atti, cioè che il computer fosse perennemente collegato alla rete elettrica e telefonica in modo da comportare costi fissi per la pubblica amministrazione indipendente dalla navigazione in Internet. Ora, a parte il fatto che tale assunto è errato per ciò che attiene all'energia elettrica, che viene consumata in quanto l'apparecchio sia acceso, ciò che più conta è che da nessun dato si ricava che il tipo di convenzione con il *provider* prevedesse un accesso costante al *web* a un costo fisso anziché un accesso di volta in volta consentito solo previo contatto telefonico, non occorrendo spendere parole per dimostrare come in questo secondo caso l'indagato si sarebbe appropriato anche delle energie appartenenti all'ente sotto forma di telefonate di volta in volta eseguite per la navigazione in Internet per finalità totalmente estranee alla pubblica funzione (masterizzazione di DVD audio e scaricamento di immagini e di film).

L'ordinanza impugnata dà la prima ipotesi come appartenente al notorio ma ciò è del tutto arbitrario, specie in considerazione che tale tipo di convenzione si è diffusa recentemente, mentre i fatti di cui è causa risalgono all'anno 2003, onde la questione avrebbe dovuto formare oggetto di dimostrazione precisa. L'ordinanza va quindi annullata in punto di gravi indizi di colpevolezza con rinvio al Tribunale di Bari perché spieghi non solo per quali motivi ha ritenuto l'insussistenza dei gravi indizi del reato solo in relazione al danno cagionato (asseritamene mancante), ma anche da

quali dati probatori concreti relativi al caso di specie abbia desunto l'esistenza di un certo tipo di convenzione con l'ente gestore del servizio telefonico.

Ma l'ordinanza impugnata va annullata anche in punto di esigenze cautelari perché l'incensuratezza, considerato il tipo e la reiterazione del reato di specie, non ha un significato decisivo; significato men che meno attribuibile all'"atteggiamento esplicativo" avuto dall'indagato in sede di interrogatorio. Il Tribunale dovrà motivare se sussista un pericolo di reiterazione, tenuto conto del fatto che sono stati trovati sull'apparecchio in questione e sul disco esterno ben 10.000 *files*, di cui solo una modestissima parte di natura attinente alle funzioni esercitate.

[…]

10.4. 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 datoriale 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, definendone 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 indebiti utilizzi 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'onere 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 *files*, 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'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *files* 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 *online* 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 *files* 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 *email*, 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.

APPENDICE NORMATIVA

NORME SOVRANAZIONALI

Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
(Roma, 4 novembre 1950)

Articolo 8 - Diritto al rispetto della vita privata e familiare

1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.

Articolo 9 - Libertà di pensiero, di coscienza e di religione

1. Ogni persona ha diritto alla libertà di pensiero, di coscienza e di religione; tale diritto include la libertà di cambiare religione o credo, così come la libertà di manifestare la propria religione o il proprio credo individualmente o collettivamente, in pubblico o in privato, mediante il culto, l'insegnamento, le pratiche e l'osservanza dei riti.

2. La libertà di manifestare la propria religione o il proprio credo non può essere oggetto di restrizioni diverse da quelle che sono stabilite dalla legge e costituiscono misure necessarie, in una società democratica, per la pubblica sicurezza, la protezione dell'ordine, della salute o della morale pubblica, o per la protezione dei diritti e della libertà altrui.

Articolo 10 - Libertà di espressione

1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione.

2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, per la sicurezza nazionale, per l'integrità territoriale o per la pubblica sicurezza, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario.

Carta dei diritti fondamentali dell'Unione europea
(Nizza, 7 dicembre 2000)

Articolo 7 - Rispetto della vita privata e della vita familiare

1. Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8 - Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 11 - Libertà di espressione e d'informazione

1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

2. La libertà dei media e il loro pluralismo sono rispettati.

NORME COSTITUZIONALI

Costituzione degli Stati Uniti – Bill of Rights

First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Costituzione italiana

Art.13

1. La libertà personale è inviolabile.

2. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge.

Art.14

1. Il domicilio è inviolabile.

2. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale.

Art.15

1. La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

2. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Art.21

1. Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.

2. La stampa non può essere soggetta ad autorizzazioni o censure.

3. 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.

[…]

6. 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.

NORME NAZIONALI

Codice penale

Art.6 - Reati commessi nel territorio dello Stato

1. Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana.

2. Il reato si considera commesso nel territorio dello Stato quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione.

Art.57 - Reati commessi col mezzo della stampa periodica

1. Salva la responsabilità dell'autore della pubblicazione e fuori dei casi di concorso, il direttore o il vice-direttore responsabile, il quale omette di esercitare sul contenuto del periodico da lui diretto il controllo necessario ad impedire che col mezzo della pubblicazione siano commessi reati, è punito, a titolo di colpa, se un reato è commesso, con la pena stabilita per tale reato, diminuita in misura non eccedente un terzo.

Art.57-*bis* - Reati commessi col mezzo della stampa non periodica

1. Nel caso di stampa non periodica, le disposizioni di cui al precedente articolo si applicano all'editore, se l'autore della pubblicazione è ignoto o non imputabile, ovvero allo stampatore, se l'editore non è indicato o non è imputabile.

Art.58 - Stampa clandestina

1. Le disposizioni dell'articolo precedente si applicano anche se non sono state osservate le prescrizioni di legge sulla pubblicazione e diffusione della stampa periodica e non periodica.

Art.494 - Sostituzione di persona

1. Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno.

Art.594 - Ingiuria

1. Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a euro 516.

2. Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa.

3. La pena è della reclusione fino a un anno o della multa fino a euro 1.032 se l'offesa consiste nell'attribuzione di un fatto determinato.

4. Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone.

Art.595 - Diffamazione

1. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032.

2. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a euro 2.065.

3. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516.

4. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza o ad una autorità costituita in collegio, le pene sono aumentate.

Art.596-*bis* - Diffamazione col mezzo della stampa.

1. Se il delitto di diffamazione è commesso col mezzo della stampa le disposizioni dell'articolo precedente si applicano anche al direttore o vice-direttore responsabile, all'editore e allo stampatore, per i reati preveduti negli articoli 57, 57-bis e 58.

Art.600-*ter* - Pornografia minorile

1. Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche è punito con la reclusione da sei a dodici anni e con la multa da euro 25.822 a euro 258.228.

2. Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.

3. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.

4. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.

5. Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.

Art.600-*quater* - Detenzione di materiale pornografico

1. Chiunque, al di fuori delle ipotesi previste dall'art.600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.

2. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

Art.600-*quater*.1 - Pornografia virtuale

1. Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

2. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Art.616 - Violazione, sottrazione e soppressione di corrispondenza

1. Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

2. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.

3. Il delitto è punibile a querela della persona offesa.

4. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

Art.617-*quater* - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

2. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

3. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

4. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

Art.617-*quinquies* - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

1. Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art.617-quater.

Art.617-*sexies* - Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

1. Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art.617-quater.

Art.618 - Rivelazione del contenuto di corrispondenza.

1. Chiunque, fuori dei casi preveduti dall'art.616, essendo venuto abusivamente a cognizione del contenuto di una corrispondenza a lui non diretta, che doveva rimanere segreta, senza giusta causa lo rivela, in tutto o in parte, è punito, se dal fatto deriva nocumento, con la reclusione fino a sei mesi o con la multa da euro 103 a euro 516.

2. Il delitto è punibile a querela della persona offesa.

Legge 22 aprile 1941, n.633

Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

Art.93

1. Le corrispondenze epistolari, gli epistolari, le memorie familiari e personali e gli altri scritti della medesima natura, allorché abbiano carattere confidenziale o si riferiscano alla intimità della vita privata, non possono essere pubblicati, riprodotti od in qualunque modo portati alla conoscenza del pubblico senza il consenso dell'autore, e, trattandosi di corrispondenze epistolari e di epistolari, anche del destinatario.

2. Dopo la morte dell'autore o del destinatario occorre il consenso del coniuge o dei figli, o, in loro mancanza, dei genitori; mancando il coniuge, i figli e i genitori, dei fratelli e delle sorelle, e, in loro mancanza, degli ascendenti e dei discendenti fino al quarto grado.

3. Quando le persone indicate nel comma precedente siano più e vi sia tra loro dissenso, decide l'autorità giudiziaria, sentito il Pubblico Ministero.

4. È rispettata, in ogni caso, la volontà del defunto quando risulti da scritto.

Legge 8 febbraio 1948, n.47

Disposizioni sulla stampa

Art.1 - Definizione di stampa o stampato

1. Sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione.

Art.2 - Indicazioni obbligatorie sugli stampati

1. Ogni stampato deve indicare il luogo e l'anno della pubblicazione, nonché il nome e il domicilio dello stampatore e, se esiste, dell'editore.

2. I giornali, le pubblicazioni delle agenzie d'informazioni e i periodici di qualsiasi altro genere devono recare la indicazione:

- del luogo e della data della pubblicazione;

- del nome e del domicilio dello stampatore;

- del nome del proprietario e del direttore o vice direttore responsabile.

3. All'identità delle indicazioni, obbligatorie e non obbligatorie, che contrassegnano gli stampati, deve corrispondere identità di contenuto in tutti gli esemplari.

Art.3 - Direttore responsabile

1. Ogni giornale o altro periodico deve avere un direttore responsabile.

2. Il direttore responsabile deve essere cittadino italiano e possedere gli altri requisiti per l'iscrizione nelle liste elettorali politiche.

Art.5 - Registrazione

1. Nessun giornale o periodico può essere pubblicato se non sia stato registrato presso la cancelleria del tribunale, nella cui circoscrizione la pubblicazione deve effettuarsi.

2. Per la registrazione occorre che siano depositati nella cancelleria:

1) una dichiarazione, con le firme autenticate del proprietario e del direttore o vice direttore responsabile, dalla quale risultino il nome e il domicilio di essi e della persona che esercita l'impresa giornalistica, se questa è diversa dal proprietario, nonché il titolo e la natura della pubblicazione;

2) i documenti comprovanti il possesso dei requisiti indicati negli artt.3 e 4;

3) un documento da cui risulti l'iscrizione nell'albo dei giornalisti, nei casi in cui questa sia richiesta dalle leggi sull'ordinamento professionale;

4) copia dell'atto di costituzione o dello statuto, se proprietario è una persona giuridica.

3. Il presidente del tribunale o un giudice da lui delegato, verificata la regolarità dei documenti presentati, ordina, entro quindici giorni, l'iscrizione del giornale o periodico in apposito registro tenuto dalla cancelleria.

4. Il registro è pubblico.

Legge 20 maggio 1970, n.300

Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento

Art.4 – Impianti audiovisivi

1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

Legge 7 marzo 2001, n.62

Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n.416

Art.1 - Definizioni e disciplina del prodotto editoriale

1. Per «prodotto editoriale», ai fini della presente legge, si intende il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva, con esclusione dei prodotti discografici o cinematografici.

2. Non costituiscono prodotto editoriale i supporti che riproducono esclusivamente suoni e voci, le opere filmiche ed i prodotti destinati esclusivamente all'informazione aziendale sia ad uso interno sia presso il pubblico. Per «opera filmica» si intende lo spettacolo, con contenuto narrativo o documentaristico, realizzato su supporto di qualsiasi natura, purché costituente opera dell'ingegno ai sensi della disciplina sul diritto d'autore, destinato originariamente, dal titolare dei diritti di utilizzazione economica, alla programmazione nelle sale cinematografiche ovvero alla diffusione al pubblico attraverso i mezzi audiovisivi.

3. 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.

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

Art.1 - Finalità

1. Il presente decreto è diretto a promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico.

2. Non rientrano nel campo di applicazione del presente decreto:

a) i rapporti fra contribuente e amministrazione finanziaria connessi con l'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi nonché la regolamentazione degli aspetti tributari dei servizi della società dell'informazione ed in particolare del commercio elettronico;

b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n.675, e al d.lgs. 13 maggio 1998, n.171, e successive modificazioni;

c) le intese restrittive della concorrenza;

d) le prestazioni di servizi della società dell'informazione effettuate da soggetti stabiliti in Paesi non appartenenti allo spazio economico europeo;

e) le attività, dei notai o di altre professioni, nella misura in cui implicano un nesso diretto e specifico con l'esercizio dei pubblici poteri;

f) la rappresentanza e la difesa processuali;

g) i giochi d'azzardo, ove ammessi, che implicano una posta pecuniaria, i giochi di fortuna, compresi il lotto, le lotterie, le scommesse i concorsi pronostici e gli altri giochi come definiti dalla normativa vigente, nonché quelli nei quali l'elemento aleatorio è prevalente.

3. Sono fatte salve le disposizioni comunitarie e nazionali sulla tutela della salute pubblica e dei consumatori, sul regime autorizzatorio in ordine alle prestazioni di servizi investigativi o di vigilanza privata, nonché in materia di ordine pubblico e di sicurezza, di prevenzione del riciclaggio del denaro, del traffico illecito di stupefacenti, di commercio, importazione ed esportazione di armi, munizioni ed esplosivi e dei materiali d'armamento di cui alla legge 9 luglio 1990, n.185.

Art.2 - Definizioni

1. Ai fini del presente decreto si intende per:

a) «servizi della società dell'informazione»: le attività economiche svolte in linea - online -, nonché i servizi definiti dall'art.1, comma 1, lett.b), della legge 21 giugno 1986, n.317, e successive modificazioni;

b) «prestatore»: la persona fisica o giuridica che presta un servizio della società dell'informazione;

c) «prestatore stabilito»: il prestatore che esercita effettivamente un'attività economica mediante una stabile organizzazione per un tempo indeterminato. La presenza e l'uso dei mezzi tecnici e delle tecnologie necessarie per prestare un servizio non costituiscono di per sé uno stabilimento del prestatore;

d) «destinatario del servizio»: il soggetto che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili informazioni;

e) «consumatore»: qualsiasi persona fisica che agisca con finalità non riferibili all'attività commerciale, imprenditoriale o professionale eventualmente svolta;

f) «comunicazioni commerciali»: tutte le forme di comunicazione destinate, in modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di un soggetto che esercita un'attività agricola, commerciale, industriale, artigianale o una libera professione. Non sono di per sé comunicazioni commerciali:

1) le informazioni che consentono un accesso diretto all'attività dell'impresa, del soggetto o dell'organizzazione, come un nome di dominio, o un indirizzo di posta elettronica;

2) le comunicazioni relative a beni, servizi o all'immagine di tale impresa, soggetto o organizzazione, elaborate in modo indipendente, in particolare senza alcun corrispettivo;

g) «professione regolamentata»: professione riconosciuta ai sensi dell'art.2 del d.lgs. 27 gennaio 1992, n.115, ovvero ai sensi dell'art.2 del d.lgs. 2 maggio 1994, n.319;

Art.7 - Informazioni generali obbligatorie

1. Il prestatore, in aggiunta agli obblighi informativi previsti per specifici beni e servizi, deve rendere facilmente accessibili, in modo diretto e permanente, ai destinatari del servizio e alle Autorità competenti le seguenti informazioni:

a) il nome, la denominazione o la ragione sociale;

b) il domicilio o la sede legale;

c) gli estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;

d) il numero di iscrizione al repertorio delle attività economiche, REA, o al registro delle imprese;

e) gli elementi di individuazione, nonché gli estremi della competente autorità di vigilanza qualora un'attività sia soggetta a concessione, licenza od autorizzazione;

f) per quanto riguarda le professioni regolamentate:

1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione;

2) il titolo professionale e lo Stato membro in cui è stato rilasciato;

3) il riferimento alle norme professionali e agli eventuali codici di condotta vigenti nello Stato membro di stabilimento e le modalità di consultazione dei medesimi;

g) il numero della partita IVA o altro numero di identificazione considerato equivalente nello Stato membro, qualora il prestatore eserciti un'attività soggetta ad imposta;

h) l'indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei diversi servizi della società dell'informazione forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;

i) l'indicazione delle attività consentite al consumatore e al destinatario del servizio e gli estremi del contratto qualora un'attività sia soggetta ad autorizzazione o l'oggetto della prestazione sia fornito sulla base di un contratto di licenza d'uso.

2. Il prestatore deve aggiornare le informazioni di cui al comma 1.

3. La registrazione della testata editoriale telematica è obbligatoria esclusivamente per le attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze previste dalla legge 7 marzo 2001, n.62.

Art.9 - Comunicazione commerciale non sollecitata

1. Fatti salvi gli obblighi previsti dal d.lgs. 22 maggio 1999, n.185, e dal d.lgs. 13 maggio 1998, n.171, le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.

2. La prova del carattere sollecitato delle comunicazioni commerciali è onere del prestatore.

Art.14 - Responsabilità nell'attività di semplice trasporto - *Mere conduit* -

1. Nella prestazione di un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione, il prestatore non è responsabile delle informazioni trasmesse a condizione che:

a) non dia origine alla trasmissione;

b) non selezioni il destinatario della trasmissione;

c) non selezioni né modifichi le informazioni trasmesse.

2. Le attività di trasmissione e di fornitura di accesso di cui al comma 1 includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo.

3. L'autorità giudiziaria o quella amministrativa, avente funzioni di vigilanza, può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse.

Art.15 - Responsabilità nell'attività di memorizzazione temporanea – *Caching* -

1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che:

a) non modifichi le informazioni;

b) si conformi alle condizioni di accesso alle informazioni;

c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore;

d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni;

e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza 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.

Art.16 - Responsabilità nell'attività di memorizzazione di informazioni - *Hosting* -

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 risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità 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.

Art.17 - Assenza dell'obbligo generale di sorveglianza

1. Nella prestazione dei servizi di cui agli articoli 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 articoli 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.

D.lgs. 30 giugno 2003 n.196
Codice in materia di protezione dei dati personali

Art.4 - Definizioni

1. Ai fini del presente codice si intende per:

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 modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) «dato personale», qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) «dati identificativi», i dati personali che permettono l'identificazione diretta dell'interessato;

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;

e) «dati giudiziari», i dati personali idonei a rivelare provvedimenti di cui all'art.3, comma 1, lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

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;

h) «incaricati», le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) «interessato», la persona fisica, la persona giuridica, l'ente o l'associazione 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;

n) «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) «blocco», la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) «banca di dati», qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) «Garante», l'autorità di cui all'art.153, istituita dalla legge 31 dicembre 1996, n.675.

2. Ai fini del presente codice si intende, inoltre, per:

a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) «chiamata», la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) «reti di comunicazione elettronica», i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la

diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art.2, lett.c), della direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio;

f) «abbonato», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) «posta elettronica», messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

a) «misure minime», il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art.31;

b) «strumenti elettronici», gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) «autenticazione informatica», l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) «credenziali di autenticazione», i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) «parola chiave», componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) «profilo di autorizzazione», l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) «sistema di autorizzazione», l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

a) «scopi storici», le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) «scopi statistici», le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) «scopi scientifici», le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art.130 - Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24 nonché ai sensi di quanto previsto dal comma 3-bis del presente articolo.

3-bis. In deroga a quanto previsto dall'art.129, il trattamento dei dati di cui all'art.129, comma 1, mediante l'impiego del telefono per le finalità di cui all'art.7, comma 4, lett.b), è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario in un registro pubblico delle opposizioni.

3-ter. Il registro di cui al comma 3-bis è istituito con decreto del Presidente della Repubblica da adottare ai sensi dell'art.17, comma 2, della legge 23 agosto 1988, n.400, previa deliberazione del Consiglio dei ministri, acquisito il parere del Consiglio di Stato e delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, nonché, per i relativi profili di competenza, il parere dell'Autorità per le garanzie nelle comunicazioni, che si esprime entro il medesimo termine, secondo i seguenti criteri e princìpi generali:

a) attribuzione dell'istituzione e della gestione del registro ad un ente o organismo pubblico titolare di competenze inerenti alla materia;

b) previsione che l'ente o organismo deputato all'istituzione e alla gestione del registro vi provveda con le risorse umane e strumentali di cui dispone o affidandone la realizzazione e la gestione a terzi, che se ne assumono interamente gli oneri finanziari e organizzativi, mediante contratto di servizio, nel rispetto del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al d.lgs. 12 aprile 2006, n.163. I soggetti che si avvalgono del registro per effettuare le comunicazioni corrispondono tariffe di accesso basate sugli effettivi costi di funzionamento e di manutenzione. Il Ministro dello sviluppo economico, con proprio provvedimento, determina tali tariffe;

c) previsione che le modalità tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale è intestatario secondo modalità semplificate ed anche in via telematica o telefonica;

d) previsione di modalità tecniche di funzionamento e di accesso al registro mediante interrogazioni selettive che non consentano il trasferimento dei dati presenti nel registro stesso, prevedendo il tracciamento delle operazioni compiute e la conservazione dei dati relativi agli accessi;

e) disciplina delle tempistiche e delle modalità dell'iscrizione al registro, senza distinzione di settore di attività o di categoria merceologica, e del relativo aggiornamento, nonché del correlativo periodo massimo di utilizzabilità dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente;

f) obbligo per i soggetti che effettuano trattamenti di dati per le finalità di cui all'art.7, comma 4, lett.b), di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilità e sulle modalità di iscrizione nel registro per opporsi a futuri contatti;

g) previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli 23 e 24.

3-quater. La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3-bis e sul trattamento dei dati sono attribuiti al Garante.

4. Fatto salvo quanto previsto nel comma 1, 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, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'art.7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'art.143, comma 1, lett.b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

Art.131 - Informazioni ad abbonati e utenti

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'abbonato e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'abbonato informa l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.

3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

Art.132 - Conservazione di dati di traffico per altre finalità.

1. Fermo restando quanto previsto dall'art.123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data di comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

[…]

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art.391-quater del codice di procedura penale, ferme restando le condizioni di cui all'art.8, comma 2, lett.f), per il traffico entrante.

[…]

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'art.226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al d.lgs. 28 luglio 1989, n.271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato art.226 delle norme di cui al d.lgs. n.271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'art.326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

Art.133 - Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'art.12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'art.11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

D.lgs. 7 marzo 2005, n.82
Codice dell'amministrazione digitale

Art.2 - Finalità e ambito di applicazione

1. Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'art.1, comma 2, del d.lgs. 30 marzo 2001, n.165, nel rispetto del riparto di competenza di cui all'art. 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'art.1, comma 5, della l. 30 dicembre 2004, n.311.

3. Le disposizioni di cui al capo II, agli articoli 40, 43 e 44 del capo III, nonché al capo IV, si applicano ai privati ai sensi dell'art.3 del d.p.r. 28 dicembre 2000, n.445, e successive modificazioni

4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.

5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con d.lgs. 30 giugno 2003, n.196. I cittadini e le imprese hanno, comunque, 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.

6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali. Con decreti del Presidente del Consiglio dei Ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria.

Art.3 - Diritto all'uso delle tecnologie

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all'articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice

1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.

Art.4 - Partecipazione al procedimento amministrativo informatico

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del d.p.r. 28 dicembre 2000, n.445.

2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

Art.5 - Effettuazione dei pagamenti con modalità informatiche

1. Le pubbliche amministrazioni consentono, sul territorio nazionale, l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, fatte salve le attività di riscossione dei tributi regolate da specifiche normative, con l'uso delle tecnologie dell'informazione e della comunicazione.

2. Le pubbliche amministrazioni centrali possono avvalersi, senza nuovi o maggiori oneri per la finanza pubblica, di prestatori di servizi di pagamento per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito o prepagate e di ogni altro strumento di pagamento elettronico disponibile. Il prestatore dei servizi di pagamento che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito e la relativa causale, la corrispondenza di ciascun pagamento, i capitoli e gli articoli d'entrata oppure le contabilità speciali interessate.

3. Con decreto del Ministro per la pubblica amministrazione e l'innovazione ed i Ministri competenti per materia, di concerto con il Ministro dell'economia e delle finanze, sentito DigitPA sono individuate le operazioni di pagamento interessate dai commi 1 e 2, i tempi da cui decorre la disposizione di cui al comma 1, le relative modalità per il riversamento, la rendicontazione da parte del prestatore dei servizi di pagamento e l'interazione tra i sistemi e i soggetti coinvolti nel pagamento, nonché il modello di convenzione che il prestatore di servizi di pagamento deve sottoscrivere per effettuare il servizio.

4. Le regioni, anche per quanto concerne i propri enti e le amministrazioni del Servizio sanitario nazionale, e gli enti locali adeguano i propri ordinamenti al principio di cui al comma 1.

Art.5-*bis* - Comunicazioni tra imprese e amministrazioni pubbliche

1. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

2. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dello sviluppo economico e con il Ministro per la semplificazione normativa, sono adottate le modalità di attuazione del comma 1 da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.

3. DigitPA, anche avvalendosi degli uffici di cui all'art.17, provvede alla verifica dell'attuazione del comma 1 secondo le modalità e i termini indicati nel decreto di cui al comma 2.

4. Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1.

Art.6 - Utilizzo della posta elettronica certificata

1. Per le comunicazioni di cui all'art.48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.

1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli artt.16, comma 10, e 16-bis, comma 5, del d.l. 29 novembre 2008, n.185, convertito, con modificazioni, dalla l.28 gennaio 2009,

n.2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali.

Art.7 - Qualità dei servizi resi e soddisfazione dell'utenza

1. Le pubbliche amministrazioni provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.

2. Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.

Art.8 - Alfabetizzazione informatica dei cittadini

1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.

Art.9 - Partecipazione democratica elettronica

1. Le pubbliche amministrazioni favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.

Art.12 - Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa

1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nonché per la garanzia dei diritti dei cittadini e delle imprese di cui al capo I, sezione II, del presente decreto.

1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'art.14 del d.lgs. 30 marzo 2001, n.165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'art.10 del d.lgs. 27 ottobre 2009, n.150, dettano disposizioni per l'attuazione delle disposizioni del presente decreto.

1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli artt.21 e 55 del d.lgs. 30 marzo 2001, n.165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.

2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'art.71.

3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.

4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.

5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'art.71.

5-bis. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione attraverso le tecnologie dell'informazione e della comunicazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

Art.13 - Formazione informatica dei dipendenti pubblici

1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'art.7-bis, del d.lgs. 30 marzo 2001, n.165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione.

Art.47 - Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di segnatura di protocollo di cui all'art.55 del d.p.r. 28 dicembre 2000, n.445;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'art.71;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al d.p.r. 11 febbraio 2005, n.68.

3. Le pubbliche amministrazioni e gli altri soggetti di cui all'art.2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. Le pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Art.48 - Posta elettronica certificata

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del d.p.r. 11 febbraio 2005, n.68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al d.p.r. 11 febbraio 2005, n.68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

Art.49 - Segretezza della corrispondenza trasmessa per via telematica

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

D.l. 27 luglio 2005, n.144, conv. in legge31 luglio 2005, n.155
Misure urgenti per il contrasto del terrorismo internazionale

Art.6 - Nuove norme sui dati del traffico telefonico e telematico

1. A decorrere dalla data di entrata in vigore del presente decreto e fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni e limitatamente alle informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi, debbono essere conservati fino alla data di entrata in vigore del provvedimento legislativo di attuazione della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, e comunque non oltre il 31 dicembre 2008, dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art.132 del d.lgs. 30 giugno 2003, n.196, possono essere utilizzati esclusivamente per le finalità del presente decreto, salvo l'esercizio dell'azione penale per i reati comunque perseguibili.

2. All'art.55, comma 7, del d.lgs. 1 agosto 2003, n.259, le parole: «al momento dell'attivazione del servizio» sono sostituite dalle seguenti: «prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.). Le predette imprese adottano tutte le necessarie misure affinché venga garantita l'acquisizione dei dati anagrafici riportati su un documento di identità, nonché del tipo, del numero e della riproduzione del documento presentato dall'acquirente ed assicurano il corretto trattamento dei dati acquisiti».

3. All'art.132 del d.lgs. 30 giugno 2003, n.196, sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «al traffico telefonico», sono inserite le seguenti: «, inclusi quelli concernenti le chiamate senza risposta,»;

b) al comma 1, sono aggiunte, in fine, le seguenti parole: «, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi»;

c) al comma 2, dopo le parole: «al traffico telefonico», sono inserite le seguenti: «, inclusi quelli concernenti le chiamate senza risposta,»;

d) al comma 2, dopo le parole: «per ulteriori ventiquattro mesi», sono inserite le seguenti: «e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi»;

e) al comma 3, le parole: «giudice su istanza del pubblico ministero o» sono sostituite dalle seguenti: «pubblico ministero anche su istanza»;

f) dopo il comma 4 è inserito il seguente:

«4-bis. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone l'acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati».

Art.7 - Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e Internet

1. A decorrere dal quindicesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2011, chiunque, quale attività principale, intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni anche telematiche, deve chiederne la licenza al questore. La licenza non è richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale. (*)

2. Per coloro che già esercitano le attività di cui al comma 1, la licenza deve essere richiesta entro sessanta giorni dalla data di entrata in vigore del presente decreto.

3. La licenza si intende rilasciata trascorsi sessanta giorni dall'inoltro della domanda. Si applicano in quanto compatibili le disposizioni dei capi III e IV del titolo I e del capo II del titolo III del testo unico delle leggi di pubblica sicurezza, di cui al r.d. 18 giugno 1931, n.773, nonché le disposizioni vigenti in materia di sorvegliabilità dei locali adibiti a pubblici esercizi. Restano ferme le disposizioni di cui al d.lgs. 1 agosto 2003, n.259, nonché le attribuzioni degli enti locali in materia.

[4. Con decreto del Ministro dell'interno, di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, sentito il Garante per la protezione dei dati personali, da adottarsi entro quindici giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono stabilite le misure che il titolare o il gestore di un esercizio in cui si svolgono le attività di cui al comma 1 è tenuto ad osservare per il monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati, anche in deroga a quanto previsto dal comma 1 dell'art.122 e dal comma 3 dell'art.123 del d.lgs. 30 giugno 2003, n.196, nonché le misure di preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili.

5. Fatte salve le modalità di accesso ai dati previste dal codice di procedura penale e dal d.lgs. 30 giugno 2003, n.196, il controllo sull'osservanza del decreto di cui al comma 4 e l'accesso ai relativi dati sono effettuati dall'organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni.] (**)

(*) Il comma 1 è stato modificato dall'art.2, comma 19, lett. a), del d.l. 29 dicembre 2010, n.225.

(**) I commi 4 e 5 sono stati abrogati dall'art.2, comma 19, lett. b), del d.l. 29 dicembre 2010, n.225.

D.m. 16 agosto 2005

Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, ai sensi dell'art.7, comma 4, del d.l. 27 luglio 2005, n.144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155

Art.1 - Obblighi dei titolari e dei gestori

1. I titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie nel quale sono poste a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, sono tenuti a:

a) adottare le misure fisiche o tecnologiche occorrenti per impedire l'accesso agli apparecchi terminali a persone che non siano preventivamente identificate con le modalità di cui alla lett.b);

b) identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente;

c) adottare le misure di cui all'art.2, occorrenti per il monitoraggio delle attività;

d) informare, anche in lingue straniere, il pubblico delle condizioni d'uso dei terminali messi a disposizione, comprese quelle di cui alle lettere a) e b);

e) rendere disponibili, a richiesta, anche per via telematica, i dati acquisiti a norma delle lettere b) e c), esclusi comunque i contenuti delle comunicazioni, al Servizio polizia postale e delle comunicazioni, quale organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni, nonché, in conformità al codice di procedura penale, all'autorità giudiziaria e alla polizia giudiziaria;

f) assicurare il corretto trattamento dei dati acquisiti e la loro conservazione fino al 31 dicembre 2007.

2. L'accesso del servizio polizia postale e delle comunicazioni di cui al comma 1, lett.e), può comprendere i dati del traffico telematico solo se effettuato previa autorizzazione dell'autorità giudiziaria in conformità alla legge in vigore.

3. Nel caso di accesso ai terminali ed ai relativi servizi telematici in abbonamento o altra forma di offerta che consenta una pluralità di accessi, mediante l'utilizzazione di credenziali di accesso ad uso plurimo, le operazioni di identificazione di cui al comma 1, lett.b), sono effettuate una sola volta, prima della consegna delle predette credenziali ad uso plurimo. Il gestore o titolare dell'esercizio o del circolo è in ogni modo tenuto a vigilare affinché non siano usate credenziali di accesso consegnate ad altri utenti.

4. I dati acquisiti a norma del comma 1, lettere b) e c), sono raccolti e conservati con modalità informatiche. Per gli esercizi o i circoli aventi non più di tre apparecchi terminali a disposizione del pubblico, i predetti dati possono essere registrati su di un apposito registro cartaceo con le pagine preventivamente numerate e vidimate dalla autorità locale di pubblica sicurezza ove viene registrato anche l'identificativo della apparecchiatura assegnata all'utente e l'orario di inizio e fine della fruizione dell'apparato.

Art.2 - Monitoraggio delle attività

1. I soggetti di cui all'art.1 adottano le misure necessarie a memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni.

2. Gli stessi soggetti adottano le misure necessarie affinché i dati registrati siano mantenuti, con modalità che ne garantiscano l'inalterabilità e la non accessibilità da parte di persone non autorizzate, per il tempo indicato nel comma 1 dell'art.7, del d.l. 27 luglio 2005, n.144, convertito con modifiche nella legge 31 luglio 2005, n.155, fermo restando che i dati del traffico conservati oltre i limiti previsti dall'art.132, commi 1 e 2, del d.lgs. 30 giugno 2003, n.196, possono essere utilizzati esclusivamente per le finalità del predetto decreto-legge.

Art.3 - Accesso alle reti telematiche attraverso postazioni non vigilate

1. Le disposizioni dell'art.1, con esclusione di quella di cui al comma 1, lett.c), si applicano anche nei confronti dei fornitori di apparecchi terminali utilizzabili per le comunicazioni telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, collocati in aree non vigilate. In tal caso gli abbonamenti, forniti anche mediante credenziali di accesso prepagate o gratuite, non potranno avere validità superiore ai dodici mesi dall'ultima operazione di identificazione.

2. In deroga a quanto previsto al comma 1, possono consentirsi tempi di utilizzazione maggiori e comunque non superiori a cinque anni, nel caso di credenziali di accesso ad uso plurimo utilizzabili esclusivamente dai frequentatori di centri di ricerca, università ed altri istituti di istruzione per i terminali installati all'interno delle medesime strutture.

Art.4 - Accesso alle reti telematiche attraverso tecnologia senza fili

1. I soggetti che offrono accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico sono tenuti ad adottare le misure fisiche o tecnologiche occorrenti per impedire l'uso di apparecchi terminali che non consentono l'identificazione dell'utente, ovvero ad utenti che non siano identificati secondo le modalità di cui all'art.1.

Art.5 - Esclusioni

1. Le disposizioni del presente decreto non si applicano:

a) ai rivenditori di apparecchi terminali o altri prodotti elettronici per le attività di prova svolte sotto la diretta vigilanza degli addetti alle dimostrazioni;

b) all'offerta di servizio fax salvo che si utilizzino tecnologie a commutazione di pacchetto (voip);

c) all'accesso alle reti telematiche attraverso apparati che utilizzano SIM/USIM attive sulla rete di telefonia mobile rilasciate ai sensi dell'art.55 del d.lgs. 1 agosto 2003, n.259.