Centro Nexa su Internet & Società
Politecnico di Torino

To be or not to be (anonymous)?
Riflessioni in tema di libertà e controllo

Silvia Bisi

INTRODUZIONE

Internet e anonimato

SOMMARIO: 1. Internet, filtri, censura e anonimato. – 2. Principali ostacoli all'anonimato online. – 3. La Rete anonima. – 4. Dove siamo, dove andiamo e dove potremmo andare. Anonimamente?.

> «Suppose you wanted to witness the birth and development of a legal system. You would need a large, complex social system that lies outside of all other legal authorities. Moreover, you would need that system somehow to accelerate the seemingly millennial progress of legal development, so you could witness more than a mere moment of the process.
>
> This hypothetical system might seem like a social scientist's fantasy, but it actually exists. It's called the Internet»[1].

1. *Internet, filtri, censura e anonimato.*

Un recente studio della Commissione Europea sulla percezione da parte dei cittadini europei dell'impatto delle tecnologie dell'informazione sulle loro vite[2] ha messo in luce come una larghissima percentuale del campione intervistato pensi che l'utilizzo di Internet abbia inciso positivamente sulla propria capacità di essere informati, sulle opportunità di apprendimento, oltre che su quelle di entrare in contatto e scambiare opinioni con nuove persone di differenti culture[3].
Nella **Raccomandazione** del Parlamento Europeo del **26 marzo 2009** destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet[4] è messo chiaramente in evidenza, per la prima volta, come Internet stia «diventando uno strumento indispensabile per promuovere iniziative democratiche, un nuovo foro per il dibattito politico […], uno strumento fondamentale a livello mondiale per esercitare la libertà di espressione (ad esempio il blog) e per sviluppare attività commerciali, nonché uno strumento per promuovere l'acquisizione di competenze informatiche e la diffusione della conoscenza (e-learning); […] ha anche apportato un numero crescente di vantaggi per

[1] B. WITTES, *Law in Cyberspace. Witnessing the Birth of a Legal System on the Net*, in *Legal Times*, January 23, 1995, reperibile all'URL http://kumo.swcp.com/synth/text/legal_times_article (27/02/2011).
[2] Flash Eurobarometer no. 241: Information society as seen by EU citizens, Analytical Report, 2008, http://ec.europa.eu/public_opinion/flash/fl_241_en.pdf (22/09/2010). Lo studio è stato condotto su un campione di 27.000 cittadini europei.
[3] *Ibidem*, p. 27 ss.
[4] In Internet all'URL http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//IT (18/9/2009).

persone di ogni età, per esempio quello di poter comunicare con altri individui in ogni parte del mondo, estendendo in tal modo la possibilità di acquisire familiarità con altre culture e aumentare la comprensione di popoli e culture diversi; […] ampliato la gamma delle fonti di notizie a disposizione dei singoli, che possono ora attingere a un flusso di informazioni proveniente da diverse parti del mondo» (Considerando A): insomma «Internet dà pieno significato alla definizione di libertà di espressione sancita all'articolo 11 della Carta dei diritti fondamentali dell'Unione europea, in particolare nella sua dimensione "senza limiti di frontiera"» (Considerando C)[5].

Proprio la mancanza di frontiere è ciò che fa di Internet il luogo (o *non luogo*) più adatto per «cogliere il gioco tra pieno e vuoto di diritto»[6]: il timore («*new moral panic*»[7]) per il proliferare di gravi reati quali la pedopornografia costringe a considerare la prospettiva di un «"pieno" di diritto che consenta di perseguire efficacemente gli autori di comunicazioni lesive dei minori»[8], ma, d'altro canto, le nuove immense opportunità di comunicazione consiglierebbero un «vuoto» di diritto per scongiurare i rischi censori giustificati di volta in volta con ragioni politiche o morali.

La protezione dei minori è una delle motivazioni addotte per giustificare l'introduzione di leggi fortemente limitative per l'esercizio delle libertà personali su Internet: diversi Stati impongono filtri alla Rete per controllare il flusso di informazioni in entrata ed in uscita e reprimere forme di «resistenza democratica»[9] che solo qualche anno fa erano inimmaginabili. Si pensi ai provvedimenti sul controllo della Rete introdotti in **Kazakistan** con il pretesto di combattere la pedopornografia *online* e «fermare la diffusione di informazioni illegali su Internet»[10], ma anche all'**australiano Plan for Cyber Safety**[11], che nella sua attuale formulazione prevede un sistema di filtri a livello di ISP, funzionanti secondo una blacklist decisa da un'autorità governativa (ACMA: *Australian Communications and Media Authority*) ed in grado di bloccare non solo contenuti a carattere pedopornografico, ma potenzialmente qualsiasi tipo di contenuto[12].

Sui filtri, in qualsiasi modo attuati, il Consiglio d'Europa si espresse già il **26 marzo 2008**[13] con una **Raccomandazione**, escludendo la legittimità del loro impiego ogniqualvolta confligga con la libertà di

---

[5] Ancora prima, in realtà, una Raccomandazione del Consiglio d'Europa (*Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet*, 7 novembre 2007, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282007%2916) aveva sottolineato come «access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the information society», riconoscendo espressamente il «public service value of the Internet» e la sua importanza come strumento essenziale nella vita quotidiana delle persone, rispetto ai campi della comunicazione, informazione, conoscenza e delle transazioni commerciali.

[6] S. RODOTÀ, *Anche il diritto insegue la società che corre, e cambia*, in *Telèma*, n. 11, 1998, reperibile anche all'URL http://www.lomb.cgil.it/ext/mai/telema.htm (08/06/2010).

[7] A. HAMILTON, *The Net Out of Control: A New Moral Panic: Censorship and Sexuality*, in Liberty (ed.), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet*, Pluto Press, London, 1999, pp. 169-186, nonché L. EDWARDS, *Pornography, Censorship and the Internet*, in L. EDWARDS, C. WAELDE (eds.), *Law and the Internet*, Hart Publishing, Oxford, 2009, anche all'URL http://ssrn.com/abstract=1435093 (01/03/2011).

[8] S. RODOTÀ, op. ult. cit.

[9] «Dai blog ai social network fino al recentissimo, e già quasi invecchiato, sistema twitter sempre di più oggi l'informazione è il prodotto di una comunicazione continua e collettiva a livello mondiale. […] su questi strumenti, e specialmente sui più innovativi, poggia una forma di resistenza democratica mai immaginata prima»: cfr. F. PIZZETTI, *Relazione annuale 2008 del Garante per la protezione dei dati personali*, *Discorso del Presidente*, Roma, 2 luglio 2009, pp. 20-21, http://www.garanteprivacy.it/garante/document?ID=1628456 (18/9/2009).

[10] Cfr. *Kazakhstan to tighten internet law*, in *Al Jazeera*, 26 giugno 2009, http://english.aljazeera.net/news/europe/2009/06/200962511571432764 5.html, nonché il rapporto OSCE *Governing the Internet*, 2007, http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf, p. 119 ss. (5/9/2009).

[11] Cfr. http://pandora.nla.gov.au/pan/22093/20071124-102/www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf (versione originale presentata durante la campagna elettorale). Il piano aggiornato: http://www.minister.dbcde.gov.au/media/media_releases/2009/115; le differenze principali fra le due versioni: http://libertus.net/censor/isp-blocking/au-govplan-overview.html (tutti 08/06/2010).

[12] Cfr. http://openinternet.com.au/wp-content/uploads/2010/02/EFA-Filtering-Fact-Sheets1.pdf, ma anche http://www.ifex.org/international/2010/03/12/internet_enemies.pdf (23/12/2010).

[13] *Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters*, adottata dal Consiglio dei Ministri il 26 marzo 2008, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6 (30/9/2009).

espressione e di informazione degli adulti che accedono alla Rete[14], in linea con quanto stabilito dall'art. 10 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo, e con i soli limiti che sono ivi imposti (secondo comma). In questo senso, ogni tipo di filtro che incida sulla libertà di espressione o di informazione in Rete dovrebbe essere *trasparente*, ossia dovrebbe mettere gli utenti nella posizione di essere consapevoli della sua eventuale presenza, e di poterlo all'occorrenza rimuovere.
La Raccomandazione si rivolgeva in particolar modo agli ISP, definiti «those who design, use (install, activate, deactivate and implement) and monitor Internet filters», ed agli stessi Stati membri, ponendosi come scopo «to prevent state and private censorship»[15], ed è stata ripresa molto recentemente da una Dichiarazione[16] dello stesso Consiglio d'Europa che pone in stretta relazione il principio della *net-neutrality* e l'art. 10 poc'anzi citato, ricordando come «[e]lectronic communication networks have become basic tools for the free exchange of ideas and information. They help to ensure freedom of expression and access to information, pluralism and diversity and contribute to the enjoyment of a range of fundamental rights».
Attualmente, Parlamento Europeo e Consiglio stanno vagliando una proposta di Direttiva[17] nella quale i filtri potrebbero essere introdotti, ancora una volta, come strumenti per combattere la pedopornografia e gli abusi sui minori[18].
Al **World Summit on the Information Society** delle Nazioni Unite, nel 2003, il ruolo di Internet veniva a più riprese esaltato in una dichiarazione di principi che, tra l'altro, poneva in evidenza come «[c]onnectivity is a central enabling agent in building the Information Society. Universal, ubiquitous, equitable and affordable access to ICT infrastructure and services, constitutes one of the challenges of the Information Society and should be an objective of all stakeholders involved in building it», e, più in particolare, «[…] the establishment of ICT public access points in places such as post offices, schools, libraries and archives, can provide effective means for ensuring universal access to the infrastructure and services of the Information Society»[19].
Nel corso degli anni il ruolo dell'accesso ad Internet come diritto fondamentale è andato sempre più rafforzandosi[20]: in questi termini ne hanno parlato il consiglio costituzionale francese[21], il Segretario di Stato americano Hillary Clinton durante il suo discorso[22] contro la censura in Internet, e dal 1 luglio 2010 l'accesso ad Internet ad almeno 1 Mbps è inoltre un diritto espressamente riconosciuto dalla legge

---

[14] Si veda, per alcuni interessanti spunti offerti dalla giurisprudenza statunitense sul punto, G. ZICCARDI, *La libertà di espressione in Internet al vaglio della Corte Suprema degli Stati Uniti*, in *Quaderni Costituzionali*, n. 1, 1998, pp. 123-134.
[15] Di particolare interesse appare il passaggio nel quale il Consiglio sottolineava come gli Stati membri dovessero garantire che «nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights».
[16] *Declaration of the Committee of Ministers on network neutrality*, adottata dal Consiglio dei Ministri il 29 settembre 2010, https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2829.09.2010_2%29 (10/10/2010).
[17] Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la decisione quadro 2004/68/GAI, COM(2010)94 definitivo, 29 marzo 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0094:FIN:IT:PDF (22/09/2010).
[18] Ma in realtà i filtri non sono strumenti utili nemmeno a questi fini: cfr. i documenti http://www.edri.org/files/blocking_booklet.pdf nonché http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (23/12/2010).
[19] UN World Summit on Information Society (WSIS), *Declaration of Principles - Building the Information Society: a global challenge in the new Millennium*, doc. WSIS-03/GENEVA/DOC/4-E, 12 December 2003, http://www.itu.int/wsis/docs/geneva/official/dop.html (14/07/2010), rispettivamente parr. 21 e 23.
[20] Un sondaggio recentemente pubblicato dalla BBC mostra come la maggioranza del campione intervistato (quattro persone su cinque, su un totale di oltre 27.000 provenienti da 26 diversi paesi) abbia dichiarato che l'accesso ad Internet dovrebbe essere considerato un diritto fondamentale: cfr. *Four in Five Regard Internet Access as a Fundamental Right: Global Poll*, http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/ 08_03_10_BBC_internet_poll.pdf (30/09/2010). La ricerca è stata condotta tra il 30 novembre 2009 e il 7 febbraio 2010.
[21] Cfr. *infra*, Capitolo Terzo, par. 2.
[22] *Secretary of State Clinton on Internet Freedom*, 21 gennaio 2010, http://www.america.gov/st/texttrans-english/2010/January/20100121142618eaifas0.6585352.html (15/12/2010).

per tutti i **cittadini finlandesi**[23], mentre in **Estonia** il riconoscimento di un diritto all'accesso ad Internet risale addirittura al 2000[24].
In **Grecia**, dal 2001, la Costituzione prevede, all'art. 5A, secondo comma, che «[a]ll persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the production, exchange and diffusion thereof constitutes an obligation of the State […]»[25].
In **Ecuador**, uno dei Paesi con la più bassa diffusione della banda larga fra la popolazione[26], la nuova Costituzione, approvata nel 2008[27], cita espressamente le reti wi-fi, stabilendo, rispettivamente agli articoli 16 e 17 del Titolo secondo, Capitolo secondo, Sezione terza, che «all persons, as individuals or as part of collectives, have the right to: universal access to information and communications technologies [...] and to free spectrum bands for the operation of wireless networks», e che «the state should promote diversity and plurality in communication by guaranteeing the allocation of spectrum frequencies through transparent and egalitarian methods», garantendo altresì «access to free spectrum bands for the operation of wireless networks and ensuring that their use is predominantly guided by the public interest»[28]. Si tratta probabilmente dell'unico esempio di «**costituzionalizzazione del wi-fi**» ad oggi esistente, ed appare perciò interessante menzionare le motivazioni che hanno condotto ad una tale scelta, pur senza approfondirne il merito: «[...] Wireless networks were included in the Assembly's discussions because of such advantages as their operation in free bands of the radio frequency spectrum, their low cost and the possibilities of self-sustainability that they offer to beneficiary communities or organisations. Wireless technologies had not formerly been widely considered as solutions for communities and stakeholders in the population segments underserved by the state in terms of telecommunications services. Now that they have been incorporated into the constitution because of their value as resources for development, the state will be obliged to incorporate these technologies in public policies and take them into account when defining new regulatory frameworks so that there are clear guidelines to facilitate their promotion and use»[29].
Tuttavia, più che diritto fondamentale in sé, Internet è, sempre più, lo strumento privilegiato di *esercizio* di molti diritti fondamentali, tra i quali sicuramente possono annoverarsi il diritto di informazione (attiva e passiva: di informare e di informarsi), di manifestazione del pensiero, di comunicazione.
Filtri e anonimato appaiono sotto questo profilo strettamente correlati: laddove i filtri apposti alla Rete si traducano in una forma, più o meno stringente e pervasiva, di censura, la possibilità di potersi affacciare alla Rete in modo anonimo diviene, innanzitutto e principalmente, una questione di esercizio di diritti fondamentali.
Non ultimo il diritto a mantenere il controllo sui propri dati personali, a decidere quali e quante informazioni si è disposti a condividere con gli altri, a conoscere chi, in quali occasioni e per quali fini li raccoglierà: e il diritto, fino a dove ciò non confligga con altri diritti che siano almeno di pari rango, a non condividere affatto informazioni personali, come estrema conseguenza e baluardo del controllo sui propri dati[30].
Già nel 1997 la posizione sull'anonimato del Gruppo di lavoro per la tutela delle persone fisiche con

---

[23] Cfr. Finnish Ministry of Transport and Communications Press Release «1 Mbit Internet access a universal service in Finland from the beginning of July», http://www.lvm.fi/web/en/pressreleases/view/1169259 (13/07/2010). Per una traduzione in lingua inglese del decreto (Decree of the Ministry of Transport and Communications on the minimum rate of a functional Internet access as a universal service, n. 732/2009): http://www.finlex.fi/en/laki/kaannokset/2009/en20090732.pdf (13/07/2010).
[24] Public Information Act, § 33: «Every person shall be afforded the opportunity to have free access to public information through the Internet in public libraries [...]», http://www.legaltext.ee/text/en/X40095K2.htm (14/07/2007). Va notato incidentalmente che l'Estonia è stata vittima nel 2007 di uno dei più eclatanti attacchi di c.d. *cyberterrorismo* degli ultimi anni, che ne ha colpito siti di governo e istituzionali, media e banche, e tuttavia il diritto all'accesso non ne è risultato indebolito.
[25] Cfr. http://www.ministryofjustice.gr/eu2003/constitution.pdf (14/07/2010).
[26] Cfr. M.E. HIDALGO, *Ecuador: Wireless Networks as an Opportunity for Access to Broadband and Development* , Association for Progressive Communications, June 2009, http://www.apc.org/en/system/files/CILACInvestigacionEcuador_EN_20090630.pdf (07/09/2010).
[27] Cfr. http://pdba.georgetown.edu/Constitutions/Ecuador/ecuador08.html (07/09/2010).
[28] Per la traduzione in lingua inglese degli articoli citati: M.E. HIDALGO, *op. cit.*, p. 27.
[29] *Ibidem*, p. 28.
[30] Si tornerà su questo punto sia nel corso della presente Introduzione, sia al Capitolo Primo.

riguardo al trattamento dei dati personali era estremamente favorevole e chiara: «[g]arantendo l'anonimato, i singoli potrebbero partecipare alla rivoluzione di Internet senza il timore che ogni loro mossa possa essere registrata consentendo di raccogliere informazioni su di loro, che potrebbero essere utilizzate successivamente contro la loro volontà»[31]. Erano già ben presenti in quella Raccomandazione i problemi che attualmente si pongono come i principali ostacoli all'anonimato online («Chi è responsabile per l'inserimento di un particolare documento di pornografia infantile su Internet? Chi ha trasmesso un particolare documento protetto da copyright?»), e, tuttavia, era chiaramente individuato anche il ruolo assunto dall'anonimato in rete, con riferimento alle comunicazioni anonime («ad esempio quando una vittima di un'aggressione sessuale o di una persona che soffre di dipendenza dall'alcol o dalle droghe, desidera condividere le sue esperienze con altri, quando una persona che pensa al suicidio desidera consultare uno specialista sulla rete o quando qualcuno desidera denunciare un crimine senza timore di subire ritorsioni»), alla libertà di espressione (ad esempio «nei casi dei dissidenti politici soggetti a un regime politico totalitario che desiderano esprimere la loro opposizione al sistema politico in cui vivono e richiamare l'attenzione sulle violazioni dei diritti umani»), e, più in generale, ai «dati transazionali, identificabili per il solo fatto di esistere, [che] possono costituire uno strumento attraverso il quale il comportamento di una persona può essere seguito e controllato in una misura che non è mai stata possibile prima»[32].

I principi cardine di necessità, finalità e proporzionalità nel trattamento dei dati personali (che in Italia saranno esplicitati chiaramente con il Codice del 2003) assumevano in quel documento un significato particolare in relazione all'anonimato, laddove veniva sottolineato come «il principio che la raccolta di dati personali identificabili deve essere limitata al minimo necessario, dev'essere riconosciuto nelle legislazioni nazionali e internazionali che si occupano di Internet. Inoltre esso deve essere incluso nei codici di condotta, nelle linee guida degli altri strumenti di "soft law" che vengono sviluppati. Dove ciò sia appropriato, il principio deve specificare che ci deve sempre essere la possibilità di conservare l'anonimato»[33].

Nello stesso documento si sottolineava poi l'esigenza di intensificare «le discussioni nel quadro del consorzio della rete Internet […] al fine di sviluppare l'infrastruttura e i protocolli Internet che conducono all'attività dell'utilizzatore anonimo», incentivando finanziariamente i progetti di ricerca rivolti allo sviluppo di «strumenti anonimi di pagamento attraverso Internet e strumenti di accesso anonimi (ad esempio, terminali pubblici Internet)»[34].

Nel 2000 quelle prime raccomandazioni vengono riprese dallo stesso Gruppo «Art. 29», che in un documento di lavoro[35] espressamente cita software anonimizzante, proxy server e posta elettronica anonima (tra le varie tecniche) quali «misure intese al miglioramento della vita privata» online[36].

Molto più recentemente è, infine, la stessa Commissione a puntualizzare come sia un obiettivo da perseguire all'interno dell'attuale cornice normativa quello di minimizzare il trattamento di dati personali utilizzando dati anonimi o pseudonimi quando possibile, anche avvalendosi dell'utilizzo di «[…] measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult»[37].

Gli sviluppi tecnologici degli ultimi anni, in particolare, hanno riportato alta l'attenzione per la possibilità, giuridica e tecnologica, di mantenere l'anonimato nelle attività svolte online, soprattutto a

---

31 Gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali, Raccomandazione 3/97, *Anonimato su Internet*, 3 dicembre 1997, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_it.pdf (27/09/2010).

32 *Ibidem*, p. 5.

33 *Ibidem*, p. 12.

34 *Ibidem*.

35 Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, Documento di lavoro 5063/00/IT/DEF., 21 novembre 2000, http://www.garanteprivacy.it/garante/document?ID=434621 (20/09/2010).

36 Cfr. *ibidem*, p. 87 ss.

37 Commission of the European Communities, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, 2.5.2007, http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf (15/06/2010), p. 3.

fronte della moltiplicazione di risorse (tecnologiche) in grado di ricostruire le identità ed i movimenti degli utenti della Rete (tanto che si è parlato di *deanonymization* e *reidentification*[38]) e di posizioni altalenanti da parte dei legislatori nazionali sulla legittimità dell'anonimato online. Anche a livello europeo, nel 2008 (e, quindi, in un momento di poco successivo rispetto alle posizioni di cui si è finora reso conto), venne evidenziata la necessità di trovare una soluzione «to the problems caused by electronic networks roaming and by the anonymous character of prepaid telecommunication products»[39], e, forse anche come conseguenza di tale posizione, nei primi mesi del 2009 fu presentata un'interrogazione alla Commissione da parte di un europarlamentare svedese[40] che, citando l'esperienza del proprio Paese d'origine ed il ruolo ricoperto dall'anonimato in particolari contesti (come le testimonianze rese a giornalisti e forze dell'ordine in relazione a gravi delitti o a crimini di carattere finanziario), chiese espressamente se da parte della Commissione vi fosse l'intenzione di formulare una proposta volta a proibire l'uso degli *anonymizers* (anche solo in alcuni settori), se fosse considerata facoltà degli Stati membri quella di proibirne l'uso e se, al contrario, si ritenesse che l'«anonimato elettronico» fosse o dovesse essere garantito a livello europeo.
La risposta fece, prevedibilmente, riferimento a questioni di sicurezza e di *law enforcement* rimesse alle valutazioni dei singoli Stati, i quali, in ogni caso, sono tenuti a rispettare i principi e le garanzie relativi alle libertà fondamentali riconosciuti dalla Convenzione Europea sui Diritti dell'Uomo e dai Trattati, e che sono tenuti a giustificare eventuali scelte operate in termini di proporzionalità, rispettando i limiti dettati da quanto ritenuto effettivamente necessario in una società democratica. Quanto all'esistenza di un «diritto all'anonimato» in Europa, venne precisato in particolare che «The fundamental right to protection of personal data is enshrined in Article 8 of the EU Charter. Whilst there is no explicit right to electronic anonymity as such under Community law, the Data Protection Directive 95/46/EC, is to require that personal data must be processed fairly and lawfully, including the data minimisation principle. This principle may be furthered by the use of anonymous data wherever possible»[41].

2. *Principali ostacoli all'anonimato online.*

Uno degli argomenti utilizzati contro la possibilità di mantenere l'anonimato online è rappresentato dalla necessità di perseguire gli autori dei reati commessi attraverso Internet. Quando si parla di reati universalmente considerati gravi, come il terrorismo o la già citata pedopornografia, che scuotono le coscienze, individuare l'autore del reato diventa una priorità a cui risulta arduo contrapporre altri interessi ed altri valori.
Davanti all'esigenza di porre fine all'utilizzo della Rete per sfruttare i minori, l'importanza dell'anonimato e dei valori che vi sono sottesi sembra cedere inevitabilmente il passo a forme di identificazione, monitoraggio e registrazione sempre più invasive. Sorvegliare un'intera popolazione non appare così grave, o sproporzionato, se può rivelarsi utile a sventare un attacco terroristico, e, secondo questa impostazione, dopo gli eventi dell'11 settembre 2001 la National Security Agency (NSA) statunitense iniziò ad intercettare segretamente e senza alcuna forma di garanzia tutte le telefonate dei cittadini americani. Nel 2002 si diffuse la notizia secondo cui il Dipartimento della Difesa stava implementando un progetto di *data mining* chiamato «Total Information Awareness» (TIA) destinato a raccogliere una grande varietà di dati relativi alle persone (di carattere finanziario, sanitario, sull'istruzione, ecc.) che sarebbero stati analizzati alla ricerca di «suspicious behavior patterns». Nel 2006 il database telefonico costituito dalla NSA al fine di identificare potenziali terroristi venne indicato

[38] P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, University of Colorado Law Legal Studies Research Paper No. 09-12, anche all'URL http://ssrn.com/abstract=1450006 (15/09/2010).
[39] Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/104344.pdf (15/06/2010).
[40] Cfr. *Written question by Jens Holm (GUE/NGL) to the Commission*, E-0897/09, 13 febbraio 2009, http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2009-0897&language=EN (15/09/2010).
[41] Answer given by Mr Barrot on behalf of the Commission, 3 April 2009, http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-0897&language=EN (15/06/2010).

come il più grande database mai realizzato al mondo. Quattro anni dopo la nuova frontiera è costituita dalle intercettazioni di comunicazioni cifrate in Rete, e negli Stati Uniti (come in molti altri Paesi, compreso il nostro[42]) sembra che il giudizio di bilanciamento fra privacy e sicurezza si concluda immancabilmente a favore di quest'ultima: «[f]ederal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone»[43].

Spesso le reazioni di fronte a quelle che si configurano come vere e proprie invasioni della sfera personale degli individui[44] si risolvono nella convinzione secondo la quale se non si ha nulla da nascondere non si ha nulla da temere. Tale tipo di approccio, che in dottrina è stato indicato anche come «the "nothing to hide" argument»[45], sembra tuttavia muovere da (almeno) due assunti discutibili.

In primo luogo: la protezione della privacy ed il principio di autodeterminazione con riguardo alla circolazione (ed alla *non-circolazione*) dei dati personali sono strettamente connessi alla dimensione sociale dell'individuo ed hanno essi stessi un valore sociale, che non si contrappone al bene comune ma contribuisce alla sua costruzione.

«Privacy» non è «about hiding a wrong», ma ha a che fare con i diritti umani, la dignità e il rispetto[46]. Già agli albori della discussione sull'infoetica, e con particolare riferimento alla conservazione dei dati sul traffico telefonico, pur non ponendo in dubbio che la sicurezza collettiva «può ben valere qualche limitazione della riservatezza» si sottolineava che «questo tema non può essere più posto in termini astratti, senza tener conto degli straordinari mutamenti quantitativi e qualitativi determinati dall'evoluzione dei servizi telefonici e dalla crescita continua delle possibilità di raccogliere, conservare, usare i dati personali. […] Una rete a maglie fittissime viene stesa su tutta la società, che consente di seguire implacabilmente ogni traccia lasciata da ciascuno di noi, ricostruendo l'insieme dei rapporti sociali attraverso l'individuazione di tutte le persone chiamate, il luogo e la durata delle telefonate. Il rischio di abusi è evidente […]»[47]. In altre epoche, il Cardinale Richelieu sintetizzò mirabilmente in due celebri frasi questo rischio: «con due righe scritte da un uomo si può fare un processo al più innocente» e «datemi sei righe scritte dal più onesto degli uomini, e vi troverò qualcosa sufficiente a farlo impiccare».

E ciò conduce a considerare il secondo assunto del «"nothing to hide" argument» che si vorrebbe qui porre in discussione, ossia il riferimento ad un «ecosistema» (giuridico, sociale, culturale) nel quale sono dati come assoluti i valori di «giusto» e «sbagliato», che sono invece relativi e dipendono da chi decide *cosa* sia giusto e sbagliato, quando e dove. Avere oggi «qualcosa da nascondere» in una cosiddetta «democrazia occidentale» può avere un significato molto diverso da quello che assumerebbe in un regime totalitario in cui «sbagliato» può essere qualsiasi espressione libera del pensiero che si ponga contro la propaganda di regime. Un esempio recentissimo di cronaca mostra che anche le «democrazie occidentali» sono tutt'altro che immuni da derive censorie: *WikiLeaks* ha mostrato al mondo un altro lato del «"nothing to hide" argument», quello che riguarda i Governi e i documenti dei servizi segreti, il ricorso alla tortura durante la guerra in Iraq e gli accordi commerciali scaturiti da una supposta

---

[42] Cfr. *infra*, Capitolo Secondo.

[43] C. SAVAGE, *U.S. Tries to Make It Easier to Wiretap the Internet*, in *The New York Times*, 27 settembre 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html (27/09/2010).

[44] Nell'ultimo caso citato, poi, appare fra le proposte quella di aprire delle *backdoors* nei sistemi di comunicazione, che dovrebbero essere usate dagli investigatori in caso di necessità ma che, inevitabilmente, prestano il fianco a numerosi altri usi illeciti. Nell'articolo di Savage viene riportato come «Several privacy and technology advocates argued that requiring interception capabilities would create holes that would inevitably be exploited by hackers», e può immaginarsi, ad esempio, che una *backdoor* consenta ad un terzo di prendere il controllo della macchina di un ignaro utente e di utilizzarla come «testa di ponte», agevolando, in ipotesi, la commissione di crimini anziché combatterla.

[45] D.J. SOLOVE, *«I've Got Nothing to Hide» and Other Misunderstandings of Privacy*, in *San Diego Law Review*, Vol. 44, 2007; GWU Law School Public Law Research Paper No. 289, http://ssrn.com/abstract=998565 (17/09/2010).

[46] B. SCHNEIER, *The Eternal Value of Privacy*, in *Wired*, 18 maggio 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886 (10/10/2010). Cfr. anche *infra*, Capitolo primo.

[47] S. RODOTÀ, *Se nasce l'uomo col codice a barre*, in *La Repubblica*, 20 ottobre 1999, anche all'URL http://www.privacy.it/rodo19991020.html (22/11/2010).

corruzione di alte cariche di Stato. WikiLeaks protegge l'anonimato delle sue fonti[48] perché solo in questo modo i «collaboratori» (spesso impiegati o comunque membri delle stesse organizzazioni di cui vengono divulgate le notizie) possono convincersi a fornire informazioni senza temere ripercussioni sul piano personale.
Non è dato sapere quando la fisiologia di un sistema democratico può divenire patologia, anche se magari solo limitatamente ad alcuni aspetti. La stessa amministrazione americana che meno di un anno prima[49] aveva elogiato la Rete in relazione al diritto di accedere liberamente alle informazioni, sostenendo che «the more freely information flows, the stronger societies become» e che «access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship», ha riservato parole molto dure a WikiLeaks, accusato di aver perpetrato un attacco contro gli Stati Uniti e l'intera comunità internazionale[50].
Il modo migliore di difendere un sistema (giuridico, informatico, sociale) è, in genere e ragionando in termini astratti, quello di evitare di introdurre vulnerabilità. Nel contesto di cui ci stiamo occupando possono essere annoverate tra le «vulnerabilità» sia le limitazioni di diritti dettate da (e tollerate in virtù di) una qualche forma di «emergenza», sia l'incertezza del diritto, causata da norme che (consapevolmente o meno) siano formulate dal legislatore in maniera così poco chiara da rendere plausibili molte diverse (e magari fra loro inconciliabili) interpretazioni.
La scelta non è fra sicurezza e riservatezza, ma fra controllo e libertà: «Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide»[51].

3. La Rete anonima.

Ci sarà sempre spazio per l'anonimato: è nella struttura stessa di Internet, nel suo DNA[52]. La Rete, che nasce per essere aperta e decentrata, con l'obiettivo di ostacolare ogni forma di controllo e di sopravvivere agli attacchi che siano volti a distruggerla o anche solo ad isolarla, appare tendenzialmente come l'antitesi tecnologica dell'identificazione totale. E, in questo contesto, l'identificazione o è totale, o perde gran parte della sua ragione di esistere: per raggiungere un paradiso fiscale in Rete non bisogna possedere un aereo, e per navigare basta un *click* (e, all'occorrenza, un *proxy* ben configurato o una VPN).
L'identificazione globale è qualcosa a cui, parlando in termini tecnici e al di là di ogni giudizio di valore,

---

[48] «[...] we operate a number of servers across multiple international jurisdictions and we do not keep logs. Hence these logs can not be seized. Anonymization occurs early in the WikiLeaks network, long before information passes to our web servers. Without specialized global internet traffic analysis, multiple parts of our organisation must conspire with each other to strip submitters of their anonymity. However, we also provide instructions on how to submit material to us, via net cafes, wireless hot spots and even the post so that even if WikiLeaks is infiltrated by an external agency, sources can still not be traced. Because sources who are of substantial political or intelligence interest may have their computers bugged or their homes fitted with hidden video cameras, we suggest that if sources are going to send WikiLeaks something very sensitive, they do so away from the home and work. […]»: cfr. *About WikiLeaks*, sezione 1.6, *Anonymity for sources*, http://213.251.145.96/about.html (14/12/2010). Da notare come l'uso di *net cafes* e *wireless hot spots* sia espressamente incoraggiato proprio al fine di mantenere la sicurezza delle fonti anche in caso di un attacco a WikiLeaks perpetrato dall'interno.

[49] Cfr. *supra*, nota n. 22.

[50] Cfr. *La rabbia di Hillary Clinton contro WikiLeaks. Il sito sotto inchiesta promette nuove rivelazioni*, in *Il Sole 24 Ore*, 29 novembre 2010, http://www.ilsole24ore.com/art/notizie/2010-11-29/clinton-contro-wikileaks-attacco-194053.shtml?uuid=AYcIronC (15/12/2010). Si veda anche M. CASTELLS, *La ciberguerra di WikiLeaks*, in *Internazionale*, n. 877, 17 dicembre 2010, http://www.internazionale.it/?p=24266 (20/12/2010).

[51] B. SCHNEIER, op. cit.

[52] J.D. WALLACE, *Nameless in Cyberspace. Anonymity on the Internet*, Cato Institute Briefing Papers, no. 54, December 8, 1999, http://www.cato.org/pubs/briefs/bp54.pdf (15/12/2010).

non si può pensare in tempi brevi[53], poiché implica non solo che ogni paese del mondo (compresi tutti quelli che al momento non hanno nemmeno l'obbligo del documento d'identità) identifichi le persone che vogliono accedere alla Rete, ma che lo faccia con gli stessi standard, e che questi standard siano così «sicuri» da non permettere a nessun «malintenzionato» di violare il sistema.
L'esperienza insegna tuttavia che nessun sistema informatico-telematico è mai stato concepito in maniera tale da scongiurare qualunque rischio, e un tale sistema (verosimilmente centralizzato e gestito da un'unica autorità a livello planetario che ad oggi non solo non esiste, ma è anche difficilmente ipotizzabile) recherebbe in sé un rischio nuovo: si immagini un database nel quale sono memorizzate le credenziali d'accesso di tutti gli utenti di Internet e a quanto la sua sola esistenza possa rendere esponenzialmente più remunerativo il furto d'identità e, perciò, esponenzialmente più appetibile ogni attacco al sistema.
Ammesso, infine, che effettivamente un metodo di identificazione tecnicamente «sicuro» e globale venga concepito, e che, dunque, il fattore infrastrutturale metta al bando l'anonimato, ciò nulla dice a proposito del fattore umano. Si parla della Rete, e probabilmente a ragione, come di un «luogo» nel quale con intensità sempre maggiore si svolge la vita delle persone, ed è un «luogo-non luogo» che ha le sue regole dettate *in primis* dalla tecnologia, l'infrastruttura, e solo poi, dal diritto e dalle convenzioni sociali che ne costituiscono la sovrastruttura. Si tratta tuttavia di una sovrastruttura debole, perché frammentaria: non esiste, e potrebbe non essere nemmeno auspicabile, il diritto (oggettivo) che governa Internet, ma solo quello dei singoli Stati cui appartengono le persone, così come per lo più frammentarie e disomogenee, perché dipendenti da culture ed esperienze diverse, sono le convenzioni sociali. «Internet non è una rete di computer, ma un intreccio infinito di persone», recitava il manifesto che candidava Internet al Nobel per la pace. Ma Internet è entrambe le cose: concentrarsi solo sulle persone rischia di far perdere di vista ciò che di positivo e di negativo è reso possibile dall'infrastruttura tecnologica (per quanto qui ci riguarda maggiormente: l'espressione più piena e libera della persona che sia mai stata consentita, ed il controllo più capillare sulla stessa che sia mai stato realizzato), mentre concentrarsi solo sulla tecnologia rischia di tradursi in una corsa affannosa alla realizzazione di una *lex informatica* che se non considera il fattore umano rimarrà sempre miope, debole con i forti e forte con i deboli. Quanto potrà un ipotetico sistema sicuro di identificazione globale di fronte alle questioni poste dalla sicurezza informatica nei confronti di una popolazione mondiale in cui l'analfabetismo (e, a maggior ragione, l'analfabetismo informatico) è ancora una piaga anche per i Paesi «civilizzati»[54]? Quanto potrà nei confronti di fenomeni come il *phishing* o il *social engineering* più in generale, e contro le tecniche di *hacking* che non si rivolgono alla macchina ma all'uomo, e che nell'uomo, da sempre, trovano le migliori *backdoors* per l'accesso ai più protetti sistemi informatici?[55]

---

[53] Cfr., anche su quanto si dirà a breve, P.C. REICH, S. WEINSTEIN, C. WILD, A.S. CABANLONG, *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity*, in *European Journal of Law and Technology*, Vol. 1, n. 2, 2010, p. 35 ss., http://ejlt.org//article/download/40/59 (15/12/2010).

[54] «Cinque italiani su cento tra i 14 e i 65 anni non sanno distinguere una lettera da un'altra, una cifra dall'altra. Trentotto lo sanno fare, ma riescono solo a leggere con difficoltà una scritta e a decifrare qualche cifra. Trentatré superano questa condizione ma qui si fermano: un testo scritto che riguardi fatti collettivi, di rilievo anche nella vita quotidiana, è oltre la portata delle loro capacità di lettura e scrittura, un grafico con qualche percentuale è un'icona incomprensibile. Secondo specialisti internazionali, soltanto il 20 per cento della popolazione adulta italiana possiede gli strumenti minimi indispensabili di lettura, scrittura e calcolo necessari per orientarsi in una società contemporanea»: cfr. T. DE MAURO, *Analfabeti d'Italia*, in *Internazionale*, 7/13 marzo 2008, anche all'URL http://eddyburg.it/article/articleview/10848/0/65/ (30/11/2010). Quanto ai dati sull'accesso ad Internet, L'Italia si colloca ben al di sotto della media europea per numero di famiglie connesse (il 53%, ma è significativo anche che solo il 20,6% della popolazione sia raggiunto dalla banda larga) oltre che per la diffusione degli acquisti on-line: cfr. audizione del Presidente Calabrò alla IX Commissione (Trasporti, poste e comunicazione), *La numerazione automatica dei canali della televisione digitale terrestre, l'accesso alla rete e l'adozione da parte di Telecom del modello Open Access, lo sviluppo della banda larga e delle reti di nuova generazione*, 21 luglio 2010, part. p. 14, http://www.agcom.it/Default.aspx?message=visualizzadocument&DocID=4724 (15/12/2010). Molto interessante anche la recentissima indagine ISTAT *Cittadini e nuove tecnologie*, 23 dicembre 2010, all'URL http://www.istat.it/salastampa/comunicati/in_calendario/nuovetec/20101223_00/testointegrale20101223.pdf (23/12/2010).

[55] «A company may have puchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. That company is still totally vulnerable. Individuals may follow every best-security practice recommended by the experts,

Ipotizziamo un ulteriore scenario che preveda un'infrastruttura perfetta e degli agenti perfetti, e, sempre ipoteticamente, andiamo anche oltre il principio della personalità della responsabilità penale, stabilendo che, come il proprietario della firma digitale è responsabile per gli atti commessi con il proprio dispositivo di firma, anche sul proprietario di questo immaginifico «token d'accesso» alla Rete ricada una responsabilità penale oggettiva per ogni reato che dovesse essere commesso online a suo nome, il DNA della Rete permetterebbe con un solo server anonimo il crollo di questa imponente struttura: è il principio dell'«onion routing»[56] che è alla base di Tor.
La domanda dovrebbe perciò forse essere se sia ragionevole, e se valga la pena (in termini di investimenti in ricerca e di tempo speso sulla questione, da un lato, ed in termini di bilanciamento dei diritti, dall'altro) mirare ad un futuro più o meno prossimo nel quale l'anonimato sia bandito dalla Rete, o se, piuttosto, accettarne i «costi» (ed eventualmente concentrare gli sforzi nel tentativo di comprimerli) a fronte di un certo numero di benefici, o, in alternativa, bandirlo solo per determinati scopi e per determinati usi della Rete (ad esempio in tema di *e-governance*).

4. *Dove siamo, dove andiamo e dove potremmo andare. Anonimamente?*

In una sentenza[57] della *High Court* irlandese in tema di *copyright* si legge che «The internet is only a means of communication. It has not rewritten the legal rules of each nation through which it passes. It is not an amorphous extraterrestrial body with an entitlement to norms that run counter to the fundamental principles of human rights». Tale passaggio, che nella sentenza citata mira a sottolineare come le violazioni del diritto d'autore non assumano una diversa valenza e liceità per il solo fatto di essere commesse online, appare interessante anche (e soprattutto) a prescindere dallo specifico contesto, e in un'ottica per certi versi contraria. È infatti certamente vero, come si legge poco oltre, che «[t]here is nothing in the criminal or civil law which legalises that which is otherwise illegal simply because the transaction takes place over the internet», ma è anche vero che troppo spesso ad Internet si guarda come «luogo» pericoloso, in cui, proprio per questo, debbano valere diverse e più stringenti norme volte a prevenire la commissione di illeciti.
In Italia gli esempi di questa distorsione sono molteplici e si sono susseguite nel tempo proposte di legge volte a trattare diversamente condotte già previste come reato perché tenute in Rete: si pensi al c.d. «emendamento D'Alia» recante «Repressione di attività di apologia o istigazione a delinquere compiuta a mezzo internet»[58] o alla «Proposta di legge per Internet territorio della libertà, dei diritti e dei doveri» (più nota come «D.d.L. Carlucci»[59]), che fu presentata come una misura per combattere la

---

slavishly install every reccommended security product, and be thoroughly vigilant about proper system configuration and applying security patches. Those individuals are still completely vulnerable. […] Why? Because the *human* factor is truly security's weakest link.»: così Kevin Mitnick in K.D. MITNICK, W.L. SIMON, *The Art of Deception: Controlling the Human Element of Security*, Wiley Publishing. Indianapolis, 2002, p. 3.

[56] «Onion Routing prevents the transport medium from knowing who is communicating with whom -- the network knows only that communication is taking place. In addition, the content of the communication is hidden from eavesdroppers up to the point where the traffic leaves the OR network»: per approfondimenti cfr. http://www.onion-router.net/ (15/12/2010).

[57] Cfr. High Court of Ireland, EMI Records & Ors -v- Eircom Ltd, [2010] IEHC 108, 16 aprile 2010, http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument (11/12/2010).

[58] Proposta di modifica n. 50.0.100 al D.d.L. n. 733/2009, reperibile all'URL http://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emend&leg=16&id=392701&idoggetto=413875 (10/12/2010), di cui si riportano di seguito alcuni stralci: «Art. 50-bis - Repressione di attività di apologia o incitamento di associazioni criminose o di attività illecite compiuta a mezzo internet. 1. Quando si procede per delitti di istigazione a delinquere o a disobbedire alle leggi, ovvero per delitti di apologia di reato, previsti dal codice penale o da altre disposizioni penali, e sussistono concreti elementi che consentano di ritenere che alcuno compia detta attività di apologia o di istigazione in via telematica sulla rete internet, il Ministro dell'interno, in seguito a comunicazione dell'autorità giudiziaria, può disporre con proprio decreto l'interruzione della attività indicata, ordinando ai fornitori di connettività alla rete internet di utilizzare gli appositi strumenti di filtraggio necessari a tal fine. [...] 4. I fornitori dei servizi di connettività alla rete internet, per l'effetto del decreto di cui al comma 1, devono provvedere ad eseguire l'attività di filtraggio imposta entro il termine di 24 ore. [...] 5. Al quarto comma dell'articolo 266 del codice penale, il numero 1) è così sostituito: "col mezzo della stampa, in via telematica sulla rete internet, o con altro mezzo di propaganda"».

[59] Testo reperibile all'URL http://www.gabriellacarlucci.it/wp-content/uploads/2009/03/proposta-di-legge.doc

pedopornografia online (anche se, in realtà, nel testo sono menzionati solo il diritto d'autore e la diffamazione) e che mirava ad introdurre il «divieto di effettuare o agevolare l'immissione nella rete di contenuti in qualsiasi forma (testuale, sonora, audiovisiva e informatica, ivi comprese le banche dati) in maniera anonima».
È tuttavia, evidentemente, una distorsione, alimentata dai media «tradizionali»[60], che trova un certo consenso anche fra i «sostenitori» della Rete, dai quali sempre più spesso provengono preoccupate istanze rivolte alla risoluzione del problema dell'identificazione degli utenti online.
Muovendo, come fanno i giudici irlandesi, dall'assunto secondo cui «Internet è un mezzo di comunicazione», appare più che ragionevole, quasi banale, concludere che ciò che è illecito offline lo sia anche online, ma non si vede perché non debba considerarsi altrettanto ragionevole che ciò che è perfettamente lecito offline, nella vita quotidiana di uomini «disconnessi», non debba esserlo anche quando si stabilisce la connessione ad Internet.
L'anonimato in Rete non appare molto diverso dall'anonimato di cui ognuno può godere ogni giorno fuori dalla Rete, dove invece il problema dell'identificazione non è (ancora) sentito o percepito come tale, e dove, comunque, appare più un dato fattuale che un diritto riconosciuto dall'ordinamento, eccezion fatta per alcuni casi in cui è espressamente tutelato: si pensi al diritto dell'autore di rimanere anonimo, o della madre di figlio naturale a non essere menzionata, o al diritto all'anonimato del paziente tossicodipendente. Al di là di pochi esempi, come i precedenti, nei quali l'ordinamento attribuisce un valore proprio all'anonimato, come strumento per la piena espressione del pensiero o per la protezione dell'identità personale del soggetto, della sua salute e della sua dignità, esistono comunque spazi di anonimato che sono normalmente preservati perché non esiste un reale interesse all'identificazione continua e globale di tutta la popolazione e, in ogni caso, ad un tale interesse si opporrebbero ragioni di salvaguardia della dignità, dei diritti e delle libertà fondamentali dei singoli individui destinati comunque a prevalere. Libertà personale significa poter uscire di casa senza essere identificati sull'uscio da un funzionario di polizia o da chiunque altro ne svolga il ruolo, non dover essere «etichettati» ad ogni passo con i nostri dati anagrafici o le nostre convinzioni personali (e, per inciso, non furono tempi felici quelli in cui parte della popolazione fu obbligata a portare cucito sugli abiti il simbolo del proprio credo religioso), poter utilizzare un telefono pubblico, entrare in locali pubblici senza dichiarare la nostra identità. E parlare, e ascoltare, senza essere costretti sempre ed aprioristicamente a declinare le nostre generalità. Tutto questo fa parte di ciò che siamo abituati a chiamare «libertà»: perché non dovrebbe valere anche nei «luoghi di Internet»? Esistono, e da ultimo è stato riconosciuto anche in una recente proposta di legge[61], tecnologie di cui avvalersi per l'identificazione degli autori dei reati sia online che offline, e, da sempre, le indagini si svolgono a posteriori, dopo la commissione del fatto di reato, e non prima, in un'ottica di generalprevenzione che finisce per sfociare in un pregiudizio: siamo tutti potenziali terroristi, ed in quanto tali sottoposti a continuo controllo.
In questo lavoro si parlerà di privacy, e di anonimato, e dei valori e dei rischi che vi sono sottesi, e sarà particolarmente analizzata la situazione italiana per la sua peculiarità, in sé e rispetto al quadro internazionale, ponendo l'accento sia sugli aspetti giuridici che su quelli tecnologici che incidono sulla libertà di accesso alla Rete. Come già qui è stato anticipato, si tratta di un argomento sul quale molto è stato detto e sul quale molto, probabilmente, si dirà ancora nel prossimo futuro, anche in virtù del fragile equilibrio fra gli interessi coinvolti, che a seconda del momento storico portano a privilegiare soluzioni spesso agli antipodi e talvolta costituiscono non il frutto di una vera riflessione, quanto

---

(10/12/2010).

[60] «The media tend to spot and magnify the activities of miscreants, clowns, and fools in cyberspace because they make good reading and viewing. […] They are only a small portion of what is actually happening. […] Computer-mediated communication offers an environment unlike any heretofore made available, with the potential for genuinely interactive and cooperative innovation. To saddle such promise with an overload of baggage from a bygone era would be tragic»: così A.W. BRANSCOMB, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, in *Yale Law Journal*, n. 104, 1995, pp. 1677-1678.

[61] Cfr. Relazione al D.d.L. n. 2494/2010, *Nuove disposizioni in materia di sicurezza pubblica*, p. 4, http://www.senato.it/service/PDF/PDFServer/BGT/00514970.pdf (23/12/2010). Il contenuto di tale D.d.L. sarà approfondito nel corso del Capitolo Secondo.

piuttosto la reazione frettolosa e scomposta a fatti di cronaca o di politica, o ad «emergenze» che richiederebbero soluzioni tutt'altro che «emergenziali».
Si tratta, perciò, di un lavoro necessariamente «in divenire», che al momento della prima stesura si limita a fotografare la situazione esistente, ma che è redatto con l'auspicio di poter fornire, nel complesso, qualche spunto per un approfondimento sul tema, anche se alcune delle norme analizzate hanno subito notevoli mutamenti nel corso della ricerca e sembra ragionevole prevederne ulteriori.

CAPITOLO PRIMO

L'anonimato

SOMMARIO: 1. Libertà e dignità al tempo delle reti. – 2. Il diritto fondamentale alla protezione dei dati personali, la libertà di espressione, la libertà di impressione. – 3. E-sorveglianti ed e-sorvegliati. – 4. L'anonimato in Italia. Uno strano caso.

Libertà e dignità al tempo delle reti.

Molti dei nostri gesti quotidiani lasciano tracce di noi e del nostro modo di vivere. Siamo sempre più *networked persons*[62]: la memorizzazione di massicce quantità di dati personali in banche dati, sempre più numerose, che possono essere non solo facilmente consultate ma anche messe in relazione fra loro, ha fatto sì che ogni individuo veda oggi affiancarsi al corpo fisico un nuovo «corpo elettronico», formato dall'insieme di tutti i dati personali che lo riguardano.
Fino a poco più di un decennio fa, quando gli archivi erano per lo più cartacei, chi voleva reperire informazioni relative a terzi doveva cimentarsi con gli ostacoli posti dalla dislocazione fisica degli archivi, dall'accesso agli stessi e dal reperimento ed estrazione delle informazioni. L'informatica ha quasi annullato queste difficoltà: spesso è sufficiente interrogare un motore di ricerca ed Internet ci restituisce molteplici informazioni idonee a rivelare passato e presente delle persone, le loro abitudini, professione, status, hobbies e interessi. «*To Google*», dal nome del celeberrimo motore, è ormai il verbo[63] utilizzato per indicare le ricerche condotte in Rete, in uno spazio in cui, e il problema è stato più volte portato all'attenzione del Garante per la protezione dei dati personali[64], *il passato non passa mai.*
Siamo «entità» nello spazio virtuale, costruite da altri mediante la correlazione di dati che sfuggono sempre più al controllo dell'interessato: chiunque può teoricamente «espropriarci» del nostro corpo elettronico, toglierci il potere di controllare l'immagine e la storia personale che la Rete offre di noi[65]. Non solo, infatti, determinate informazioni personali, magari socialmente pregiudizievoli, possono rimanere a disposizione di chiunque ben oltre i limiti temporali dettati dal principio di finalità del trattamento dei dati, ma, anche qualora tali dati venissero cancellati, essi potrebbero comunque rimanere accessibili attraverso meccanismi di memorizzazione quali la «copia cache», in violazione di

---

[62] S. RODOTÀ, *Privacy, libertà, dignità*, *Discorso conclusivo della 26ª Conferenza internazionale sulla privacy e sulla protezione dei dati personali*, Wroclaw, 14-16 settembre 2004, http://www.privacy.it/rodo20040916.html (20/10/2010).
[63] Il 15 giugno 2006 il verbo *Google* diventa ufficialmente una voce dell'Oxford English Dictionary («The definitive record of the English language»): cfr. http://www.oed.com/public/update0606/june-2006-update (20/10/2010).
[64] Si veda, a titolo di esempio, la decisione del Garante del 10 novembre 2004, http://www.garanteprivacy.it/garante/doc.jsp?ID=1116068 (20/10/2010). Nel caso *de quo* il ricorrente (un operatore pubblicitario) lamentava il fatto che chiunque utilizzasse uno dei comuni motori di ricerca presenti in Internet, inserendo il suo nome o quello della sua società, ricevesse sempre in primo luogo non le notizie riguardanti la sua attuale o più recente attività professionale, ma due provvedimenti con i quali gli erano state a suo tempo applicate due sanzioni amministrative, una delle quali risalente al 1996 e l'altra al 2002. Il ricorrente e la sua società non contestavano né le sanzioni, né il fatto che l'ente in questione dovesse pubblicarle ufficialmente anche sul sito istituzionale. Si opponevano, invece, a che i provvedimenti stessi fossero reperibili indiscriminatamente in Internet sempre e da chiunque, anche da persone semplicemente intente a contattare la società: ciò, sosteneva l'interessato, pregiudicava l'immagine che la clientela poteva farsi dell'attività da lui svolta e chiedeva, pertanto, l'adozione di opportune cautele, quale, in alternativa all'oscuramento del nominativo, un accesso meno «diretto» alle pagine web in questione.
[65] S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. CONTI, Laterza, Bari, 2005, p. 120 e ss.

quel diritto all'oblio[66] garantito dal D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) al fine di assicurare il rispetto dell'identità della persona anche in un aspetto dinamico, in quello cioè che potrebbe essere definito quale «diritto di cambiare», ovvero il diritto di essere correttamente rappresentati nel contesto sociale non solo per quello che si è stati ma anche, e soprattutto, per quello che si è diventati, in un arco temporale di sviluppo e maturazione della persona che investe tutta la vita[67].
Se è vero che dalla *Magna Charta Libertatum* del 1215 l'inviolabilità del corpo fisico è uno dei principi fondamentali delle democrazie, altrettanto non può dirsi per il corpo elettronico, della cui esistenza tuttora non c'è una vera consapevolezza e che non viene percepito come altrettanto inviolabile ed importante, nonostante le conseguenze di una violazione del corpo elettronico possano tradursi in discriminazioni e stigmatizzazioni anche molto pesanti, con ripercussioni notevoli sulla psiche dell'individuo, e quindi sul suo corpo «fisico» e sulla sua salute intesa, nell'ormai ampiamente condivisa definizione dell'Organizzazione Mondiale della Sanità, quale stato di completo benessere fisico, sociale e mentale.
I diritti della «persona virtuale» rappresentano «(pre)condizioni per il riconoscimento e la tutela della dignità della persona al tempo delle reti»[68]. La valenza del diritto alla protezione dei dati personali è perciò, nel contesto che ci si appresta ad esaminare (ma in realtà, come si dirà a breve, anche *ab origine*) duplice: di diritto fondamentale *ex se*, e di *strumento* di libertà, ossia di presupposto per l'esercizio di altre libertà, fra cui primariamente quella di espressione.

Il diritto fondamentale alla protezione dei dati personali, la libertà di espressione, la libertà di impressione.

La Carta dei diritti fondamentali dell'Unione Europea riconosce, all'art. 8 (inserito nel Titolo II: «Libertà»), il diritto di ognuno alla protezione dei dati di carattere personale che lo riguardano[69]. Lungi dall'essere un diritto per pochi privilegiati personaggi «pubblici», quale, forse, poteva configurarsi in un primo tempo (come *right to be let alone*)[70], il diritto alla privacy è oggi, principalmente, il diritto dell'individuo ad avere ed a mantenere il controllo sulle informazioni che lo riguardano.
Sono cambiati, da quel primo momento di attenzione per la sfera privata dell'individuo, sia lo scenario tecnologico, sia il contesto giuridico-istituzionale: già nel 1995 si cominciava a parlare di evoluzione ed adeguamento del concetto di privacy che, da diritto di stampo prettamente privatistico, incentrato sulla tutela della riservatezza e della vita intima e familiare della persona, passava «alla più comprensiva nozione di "protezione dei dati", che va ben al di là dei problemi legati alla tutela della riservatezza

---

66 Sul «diritto all'oblio» si veda, in particolare, V. MAYER-SCHÖNBERGER, *Delete. Il diritto all'oblio nell'era digitale*, Egea, Milano, 2010, nonché S. NIGER, *Il diritto all'oblio*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, diretto da F. GALGANO, CEDAM, Padova, 2008, pp. 59-73.

67 Cfr. G. SANTANIELLO, *Il sistema delle garanzie della privacy*, in AA.VV., *Trattato di diritto amministrativo*, CEDAM, 2000, Vol. XXVI, p. 9, per il quale l'identità personale, quale «riflesso ideale esternato dalla interiorità della persona», non è solo quella attuale, ma può altresì essere vista quale riflesso di una serie di successive identità.

68 M. PAISSAN, *Relazione al convegno ISIMM «Dei delitti e delle reti. Diritti d'autore, innovazione tecnologica e sviluppo del mercato»*, Roma, 29 novembre 2005, p. 3 (fino al 15/03/2009 – data di ultima verifica – reperibile all'URL http://www.isimm.it/document/Documenti/CO291105/paissan.pdf).

69 Carta dei diritti fondamentali dell'Unione Europea, art. 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».

70 L'espressione *right to be let alone*, usata dal giudice americano Cooley nel 1888 e già a metà dell'Ottocento dallo scrittore Robert Kerr, che ne parlava descrivendo la società dell'Inghilterra vittoriana, viene riportata per la prima volta in un paper a carattere giuridico in *The Right to Privacy*, considerato, com'è noto, decisivo per la nascita del moderno diritto alla privacy. In tale articolo, tuttavia, il riferimento degli Autori è principalmente alle violazioni della vita privata perpetrate a mezzo stampa: «[…]Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life […]» (cfr. S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, vol. IV, n. 5, pp. 193-220, anche all'URL http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, 23/11/2010).

individuale, individuando ormai un criterio di base per la legalità dell'azione pubblica»[71]. Dalla Convenzione di Strasburgo del 28 gennaio 1981, ratificata in Italia dalla l. 21 febbraio 1989, n. 98, che riconosceva il diritto al rispetto della vita privata a fronte del trattamento automatizzato dei dati personali, passando per la Direttiva n. 46/1995, attuata dalla l. 31 dicembre 1996, n. 675, fino al Codice del 2003, la privacy, o meglio, il diritto alla protezione dei dati personali (che è qualcosa di ulteriore rispetto a quell'iniziale *right to be let alone*, anche se le due espressioni sono normalmente usate come sinonimi) ha subito un'evoluzione nel tempo fino a divenire diritto all'*autodeterminazione informativa*, a «costruire liberamente e difendere la propria sfera privata»[72], rilevante per l'ordinamento sia quale valore in sé[73] sia quale strumento di tutela di altri diritti di libertà costituzionalmente garantiti.
Il diritto alla tutela dei dati personali rappresenta «una distinta figura di diritto della personalità, in quanto l'interesse a non subire un abusivo trattamento dei dati personali è esso stesso un distinto interesse della persona, pur se riconducibile al più ampio interesse al rispetto della vita privata»[74], e viene ricondotto, direttamente o attraverso il riferimento a diverse disposizioni di legge ordinaria, alla protezione offerta dall'art. 2 Cost., coerentemente con il fatto che «il valore centrale della persona nell'ambito dell'ordinamento impone di riconoscere come fondamentali tutti gli interessi che ad essa si riferiscono»[75], ma anche, e per quanto qui forse maggiormente ci interessa, «nell'art. 21 Cost., leggendo la garanzia della libertà di pensiero anche in chiave negativa, nel senso di assicurare tutela anche all'interesse a non diffondere notizie o informazioni da cui il pensiero possa essere dedotto»[76].
Libertà di manifestazione del pensiero e privacy colgono entrambi la dimensione sociale dell'individuo[77]: «dal punto di vista delle relazioni personali e sociali, la privacy si presenta come una "rivendicazione dei limiti necessari per difendere il diritto di ciascuno a non essere semplificato, oggettivato o valutato fuori contesto"»[78].
In dottrina[79] è stato anche sottolineato come, per vero, sia proprio il carattere di garanzia per altri diritti di libertà a fondare la dimensione costituzionale della privacy, tanto che nella Relazione della Commissione Bozzi per le riforme istituzionali[80] era stato proposto di inserire nel testo costituzionale un art. 21-*bis* che, al secondo comma, vietava «la raccolta e l'uso di informazioni che implicassero discriminazioni o lesioni di diritti fondamentali della persona, in tal modo riecheggiando l'opinione espressa nella relazione di minoranza redatta allora da Stefano Rodotà che invocava l'individuazione di "limiti alla libertà di raccolta e di circolazione delle informazioni in relazione ad altri valori costituzionali ritenuti prevalenti"»[81].

---

71 S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 44.
72 ID., *Repertorio di fine secolo*, Laterza, Bari, 1999, p. 202.
73 Cfr., *inter alia*, P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, Milano, 2002, pp. 44-48. Sulla *Selbstbestimmung* e sull'affermazione di un rango costituzionale del diritto all'autodeterminazione informativa già nei primi Anni Ottanta cfr. S. SIMITIS, *Die informationelle Selbstbestimmung-Grundbedingung einer verfassungkonformen Informationsordnung*, in *Neue Juristische Wochenschrift*, 1984, p. 398 ss.; E. DENNINGER, *Das Recht auf informationelle Selbstbestimmung und innere Sicherheit*, in *Kritische Justiz*, 1985, vol. 18, n. 3, p. 215 ss.
74 C.M. BIANCA, in C.M. BIANCA, F.D. BUSNELLI, *La protezione dei dati personali*, Cedam, Padova, 2007, p. XXII.
75 P.M. VECCHI, in C.M. BIANCA, F.D. BUSNELLI, *op. cit.*, p. 6, nonché A. SCALISI, *Il valore della persona nel sistema e i nuovi diritti della personalità*, Giuffrè, Milano, 1990, p. 46 ss. Sulla tutela della privacy in riferimento all'identità: L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Giappichelli, Torino, 2004, part. p. 207 ss.
76 *Ibidem*.
77 Cfr. E. PELINO, *Il diritto di manifestare il pensiero*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, Cedam, Padova, 2004, p. 432 ss.
78 S. RODOTÀ, *Prefazione*, in D. LYON, *La società sorvegliata: tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, p. IX. La citazione è tratta da J. ROSEN, *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, New York, 2000, p. 20, in cui il diritto alla privacy emerge soprattutto nella sua dimensione sociale, come valorizzazione del contesto: «In a world of short attention spans, privacy is necessary to protect citizens from the misjudgements that can result from the exposure of too much information as well as too little information. Filtered or unfiltered, information taken out of context is no substitute for the genuine knowledge that can only emerge slowly over time» (p. 10).
79 P. COSTANZO, *La dimensione costituzionale della* privacy, in G.F. FERRARI (a cura di), *La legge sulla privacy dieci anni dopo*, Egea, Milano, 2008, pp. 49-62.
80 Cfr. Camera dei Deputati, Senato della Repubblica, *Commissione parlamentare per le riforme istituzionali*, IX legislatura, doc. XVI-bis, n. 3-bis, all'URL http://www.camera.it/EventiCostituzione2007/files/09%20Legislatura/Documenti/XVI-bis%20n%203/XVI%20bis%20n%203.pdf (22/11/2010).
81 P. COSTANZO, *op. cit.*, p. 58.

La privacy è oggi, in primo luogo, tutela dell'eguaglianza sostanziale: significa, per l'individuo, non dover subire discriminazioni per le proprie opinioni, di qualunque natura esse siano, per il proprio credo religioso, per le proprie condizioni di salute[82]. Ma si traduce anche, a parziale corollario, nel diritto di esprimere liberamente sé stessi e le proprie opinioni, nella libertà di pensiero e di parola che la Costituzione garantisce, come diritto inviolabile, a ciascun individuo sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità (compreso, dunque, nell'ampia nozione fornita dall'art. 2 Cost., il *cyberspazio*[83]), nella libertà di associazione, di voto, di religione.

«Privacy», dunque, non solo come diritto a non rivelare a terzi determinate informazioni sulla propria persona, ma anche, al contrario, come diritto di non nascondere le proprie scelte[84], di esprimere sé stessi nel modo più ampio e completo possibile, in tutti i contesti sociali, senza dovere per questo subire discriminazioni, e come diritto ineliminabile per la salvaguardia della libertà e della dignità dell'individuo. E, ancora, «privacy» in una nuova accezione dinamica, che diviene «componente essenziale della cittadinanza digitale e della libera costruzione dell'identità (considerando, per esempio, il diritto di anonimato, particolarmente rilevante nel caso del dissidente politico, e il diritto all'oblio), passando così dal riconoscimento dell'autodeterminazione informativa a una effettiva redistribuzione del potere in rete»[85].

Una teoria della cultura democratica valorizza la libertà di espressione come *possibilità* di ognuno di esprimersi[86], al di là della concreta realizzazione dell'espressione individuale, ma anche la c.d. «libertà di impressione»[87], ossia il suo «lato passivo», l'«interesse generale, anch'esso indirettamente protetto dall'articolo 21 [Cost.], alla informazione; il quale in un regime di libera democrazia, implica pluralità di

---

[82] La prima applicazione italiana del diritto alla privacy così inteso anticipa di molti anni la legge sulla protezione dei dati personali del 1996. Risale infatti al 1970, ed è contenuta nello Statuto dei lavoratori (l. 20 maggio 1970, n. 300), in cui non solo era espresso un divieto generale di controllo a distanza dei lavoratori al fine di preservarne la libertà e la dignità, ma, all'art. 8, veniva fatto espresso divieto al datore di lavoro di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché, con una clausola di chiusura che costituisce una notevole anticipazione del principio di finalità nel trattamento di dati personali, su fatti non rilevanti ai fini della valutazione dell'attitudine professionale dello stesso. Recita infatti l'art. 8: «Divieto di indagini sulle opinioni. – È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore». Secondo l'art. 11 del Codice in materia di protezione dei dati personali, invece, i dati devono essere «raccolti e registrati per scopi determinati, espliciti e legittimi» e «pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati».

[83] Come è noto, in Italia la tutela dei dati personali non trova un riscontro testuale nella Carta costituzionale, ma si ritiene ormai diffusamente, in dottrina come in giurisprudenza, che esso formi parte integrante del «nucleo essenziale dei valori di personalità - che inducono a qualificarlo come parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana»: così Corte cost. 23 luglio 1991, n. 366, in cui la Corte ribadisce, in particolare, il diritto inviolabile alla libertà ed alla segretezza delle comunicazioni, sottolineando che «la Costituzione riconosce un particolare pregio all'intangibilità della sfera privata negli aspetti più significativi e più legati alla vita intima della persona umana». Sulla riconducibilità di taluni diritti riguardanti la sfera personale dell'individuo alla più ampia protezione offerta dall'art. 2 Cost. cfr. anche Cass. Civ., sez. III, 14 ottobre 2008, n. 25157, nella quale la Corte rileva come l'art. 2 Cost., «inteso quale precetto nella sua più ampia dimensione di clausola generale, "aperta" all'evoluzione dell'ordinamento», sia suscettibile «di apprestare copertura costituzionale ai nuovi valori emergenti della personalità, in correlazione anche all'obiettivo primario di tutela "del pieno sviluppo della persona umana", di cui al successivo art. 3 cpv. (implicitamente su questo punto Corte Cost. 3.2.1994, n.13). […] [L]'individuo non è considerato come un punto di aggregazione di valori (tra cui in primis, ma non esaustivamente, i diritti inviolabili), inteso come somma degli stessi, sempre autonomamente scindibili, ma come un unicum, per cui la lesione di uno qualunque di tali valori, è sotto il profilo qualitativo sempre lesione della persona umana. […] Nell'ambito di questa concezione "monistica" dei diritti della persona umana, con fondamento costituzionale, il diritto all'immagine, al nome, all'onore, alla reputazione , alla riservatezza (così come gli altri valori costituzionalmente garantiti) non sono che singoli aspetti della rilevanza costituzionale che la persona, nella sua unitarietà, ha acquistato nel sistema della Costituzione».

[84] Cfr. G. ALPA, *La disciplina dei dati personali*, in *Atti del convegno ITA*, 21 novembre 1998, Roma.

[85] S. RODOTÀ, *Prefazione* a A. DI CORINTO, A. GILIOLI, *I nemici della rete*, BUR, Milano, 2010, p. 9.

[86] J.M. BALKIN, *How Rights Change: Freedom of Speech in the Digital Era*, in *Sydney Law Review*, 2004, vol. 26, p. 11, http://www.yale.edu/lawweb/jbalkin/articles/howrightschange1.pdf (verificato il 20/10/2010), e, tradotto *Come cambiano i diritti: la libertà di espressione nell'era digitale*, in V. COMBA (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, Diabasis, Reggio Emilia, 2004, pp. 1-15.

[87] Cfr. M. CONLEY, C. PATTERSON, *Communication, Human Rights and Cyberspace*, in S. HICK, E.F. HALPIN, E. HOSKINS, *Human Rights and the Internet*, Palgrave Macmillan, New York, 2000, p. 211 ss.

fonti di informazioni, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei, alla circolazione delle notizie e delle idee ed implica altresì esclusione di interventi dei pubblici poteri suscettibili di tradursi, anche indirettamente, e contro le intenzioni, in forme di pressione per indirizzare la stampa verso obiettivi predeterminati a preferenza di altri»[88].
Possibilità, dunque, che sempre maggiormente appaiono legate alla tecnologia e, più nello specifico, alle tecnologie dell'informazione e ad Internet: non solo l'*essere* ma il *poter essere* della nostra società dipendono da tali strumenti, e, «circoscrivendo le possibilità della Società dell'Informazione (e determinando i mezzi per la realizzazione di tali possibilità) le tecnologie dell'informazione concorrono a determinare la normatività della Società dell'Informazione, il suo dover essere»[89].
Si chiedeva Stefano Rodotà nel 1999: «Tutto ciò che è tecnicamente possibile è anche eticamente ammissibile, socialmente accettabile, giuridicamente lecito?»[90]. Il continuo lasciare tracce del nostro passaggio online (ma sempre più anche offline: basti pensare ai pagamenti in moneta elettronica, alla telefonia mobile, alla videosorveglianza effettuata in maniera capillare, ai controlli di sicurezza negli aeroporti), e, dunque, la *possibilità*, per soggetti pubblici e privati, di accedere ad una mole enorme di dati riguardanti le nostre abitudini di consumo, di movimento, culturali, di vita, ha contribuito a segnare il passaggio della sorveglianza da misura eccezionale e mirata a quotidiana e generalizzata. Da cittadini a potenziali sospetti nei confronti dei pubblici poteri, e a consumatori oggettivizzati nelle proprie scelte di consumo nei confronti delle imprese impegnate nella profilazione.

E-sorveglianti ed e-sorvegliati.

Sul lato pubblico, spesso il passaggio da cittadini a potenziali sospetti avviene, si diceva nel capitolo introduttivo, in nome della «sicurezza».
Fecero scalpore alcuni fra i primi provvedimenti[91] su larga scala volti a prevenire il terrorismo (in particolare) attraverso l'utilizzo invasivo della videosorveglianza e del controllo sulle telecomunicazioni, a cui le popolazioni interessate fecero una decisa opposizione, mentre non così netta fu, come si è visto, la posizione nei confronti dell'NSA statunitense solo qualche anno dopo, in seguito agli attentati dell'11 settembre 2001. Crescono le possibilità di sorvegliare i cittadini, nuove misure vengono introdotte per prevenire la criminalità e, parallelamente, si abbassa la resistenza allo scrutinio continuo di fronte a presunti vantaggi che non derivano più solo dalla lotta «al terrorismo», ma anche ai furti lungo le vie o nei parcheggi, alle aggressioni, al vandalismo, alle rapine o alle violenze.

---

88 Così Corte Cost. 15 giugno 1972, n. 105. In Italia, il diritto all'informazione, come risvolto passivo della libertà di espressione è stato successivamente ribadito in Corte Cost. 10 luglio 1974, n. 225; 30 maggio 1977, n. 94 e 26 marzo 1993, n. 112. La stretta connessione fra libertà di espressione e di informazione è largamente riconosciuta a livello internazionale, dalla Dichiarazione universale dei diritti dell'uomo del 1948 alla Carta dei diritti fondamentali dell'Unione Europea del 2000. In dottrina cfr., per tutti, P. COSTANZO, *Informazione nel diritto costituzionale*, voce in *Digesto delle discipline pubblicistiche*, vol. 8, Utet, Torino, 1993, pp. 319-395 (part. p. 330 ss.), e, con specifico riferimento all'informazione digitale e digitalizzata, ID., *La circolazione dell'informazione giuridica digitalizzata: fenomenologia e profili problematici*, in *Il Diritto dell'informazione e dell'informatica*, 1999, fasc. 3, p. 579 ss. Si vedano anche, sul ruolo dell'anonimato in relazione alla libertà di espressione e di impressione, nonché sul processo di formazione dell'opinione pubblica, le teorie di Elisabeth Noelle-Neumann sulla «spirale del silenzio», che si verifica quando i cittadini esprimono opinioni o le nascondono per la paura dell'isolamento e la minaccia di sanzioni sociali, subendo la tirannia della maggioranza. Cfr. in particolare E. NOELLE−NEUMANN, *Chiave lessicale per una teoria dell'opinione pubblica*, in S. CRISTANTE (a cura di), *L'onda anonima*, Meltemi, Roma, 2004, pp. 202-228 (part. p. 215 ss), anche all'URL http://www.meltemieditore.it/PDFfiles/onda_anonima.pdf (02/02/2011).
89 G. SARTOR, *Corso di informatica giuridica. Vol. 1 L'Informatica giuridica e le tecnologie dell'informazione*, Giappichelli, Torino, 2008, p. 34.
90 S. RODOTÀ, *Se nasce l'uomo col codice a barre*, cit. Cfr. anche S. NIGER, *Privacy e diritti di libertà: tra anonimato, memoria e oblio*, in *Ciberspazio e diritto*, n. 1, 2006, p. 121.
91 Ci si riferisce agli esempi della Gran Bretagna (minacciata del terrorismo irlandese) e del Giappone (dopo l'attentato nella metropolitana di Tokyo del 1995). La *city* londinese, cuore del distretto economico, era protetta da un sofisticato sistema di telecamere che non solo era in grado di leggere scritte poste anche a cento metri di distanza, ma, collegandosi ad un sistema informatico, era capace di rilevare «indizi di attività terroristica», mentre il governo giapponese introduceva misure volte ad intercettare sistematicamente telefonate, fax, informazioni computerizzate e posta elettronica.

Sono allora gli stessi cittadini che, ossessionati da bisogni di sicurezza spesso enfatizzati dai pubblici poteri, finiscono per rinunciare (non alla privacy bensì) alla propria libertà, rinchiudendosi autonomamente in un benthamiano *Panopticon* nel quale ciascuno non sa chi sia il sorvegliante, e quando sorvegli, e se e come lo faccia, e a quali fini.
Uno dei paradossi della «pubblicizzazione degli spazi privati», del sapersi continuamente esposti a sguardi ignoti ed indesiderati può tuttavia essere quello di aumentare l'insicurezza: «[s]apersi scrutati riduce la spontaneità e la libertà, rende difficile il salutare ritirarsi dietro le quinte, essenziale perché ciascuno possa trovare il giusto equilibrio tra il vivere in pubblico e il bisogno di intimità»[92], e si è spinti a difendere sempre più ferocemente gli ultimi spazi domestici ancora al riparo da tecniche di sorveglianza sempre più sofisticate. «Ma se libertà e spontaneità saranno confinate nei nostri spazi rigorosamente privati, saremo portati a considerare lontano e ostile tutto quel che sta nel mondo esterno. Qui può essere il germe di nuovi conflitti, e dunque di una permanente e più radicale insicurezza, che contraddice il più forte argomento addotto per legittimare la sorveglianza, appunto la sua vocazione a produrre sicurezza»[93].
La privacy sembra giocare in questo contesto un ruolo che è al contempo essenziale e marginale: è uno strumento essenziale per rimediare agli eccessi della sorveglianza nei confronti di singoli individui che si mostrano più sensibili o più esposti alle possibili conseguenze negative dell'altrui controllo sui propri dati, ma si rivela marginale laddove si riesca a scorgere che il problema della sorveglianza (o della «dataveglianza»[94]) ha carattere sociale, e pubblico, più che individuale[95]. «[L]a sorveglianza è un mezzo attraverso cui le popolazioni sono classificate e catalogate; quindi essa non si limita ad invadere lo spazio personale o a violare la privacy degli individui. […] è un mezzo sempre più potente attraverso cui sono rafforzate le divisioni sociali, poiché la classificazione superpanottica incessantemente seleziona, controlla e classifica al fine di determinare titolarità dei diritti e accesso sociale, esclusione e inclusione. […] può esibire aspetti iniqui e antisociali anche quando le politiche della privacy siano adeguate»[96]. E spesso non lo sono[97], perché «la politica e la legislazione a favore della privacy sono notoriamente inefficaci ed insensibili rispetto ai rapidi mutamenti che interessano la sorveglianza» e «pochi cittadini e ancor meno consumatori sono sempre consapevoli delle regolamentazioni che governano la raccolta dei dati o degli estremi legali a cui possono appellarsi»[98].
Possiamo senz'altro affermare che, come parte integrante dei diritti della persona riconosciuti a livello costituzionale, e comunque quale baluardo ultimo (o primo) di tutela dell'individuo, il diritto alla protezione dei dati personali è suscettibile di «bilanciamento» solamente con altri interessi di pari rilevanza con cui dovesse entrare in tensione[99]. Fra questi, si è già accennato alla «sicurezza» ed ai paradossi che vi sono legati, ma non al concetto di «fiducia», legato tradizionalmente al nostro corpo fisico, ma non ai nostri «doppi» online.
Tuttavia, riprendendo quanto già anticipato nell'*Introduzione*, non sono poi così numerose le occasioni in cui ci viene richiesto, offline, di dimostrare la nostra identità. La percezione sensoriale (vedere una

---

92 S. RODOTÀ, *Prefazione*, in D. LYON, *La società sorvegliata*, cit., p. XIII.
93 *Ibidem*.
94 Il termine *dataveillance* fu coniato da Roger Clarke nel 1988, quale contrazione di «data surveillance». Rigettando l'idea aprioristica che la sorveglianza sia, in sé, negativa o indesiderabile, Clarke procede ad un'elencazione dei benefici e dei rischi connessi alla *personal* e *mass dataveillance*: cfr. R. CLARKE, *Information Technology and Dataveillance*, in *Communications of the ACM*, May, 1988, pp. 498-512, anche all'URL http://www.rogerclarke.com/DV/CACM88.html (02/02/2011).
95 Cfr. anche J.E. COHEN, *Privacy, Visibility, Transparency, and Exposure*, in *University of Chicago Law Review*, Vol. 75, n. 1, 2008, http://ssrn.com/abstract=1012068 (02/02/2011).
96 D. LYON, *La società sorvegliata*, cit., p. 211.
97 Cfr. *inter alia* R. CLARKE, *Dataveillance – 15 Years On*, paper for the *Privacy Issues Forum* run by the New Zealand Privacy Commissioner, Wellington, 28 March 2003, http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html (02/02/2011).
98 D. LYON, op. loc. ult. cit.
99 È stato sottolineato come, pur in assenza di una specifica ed espressa previsione costituzionale del diritto alla privacy e alla protezione dei dati personali la Corte costituzionale abbia «inequivocabilmente confermato il sistema inaugurato con la l. 675 del 1996, ratificando, per così dire, in più di un'occasione il bilanciamento ivi operato tra *privacy* ed altri diritti costituzionalmente tutelati, e in particolare il fatto che deroghe più o meno ampie alla stessa *privacy* possano essere giustificate solo invocando la tutela di diritti e valori di livello costituzionale»: così P. COSTANZO, *La dimensione costituzionale della* privacy, *cit.*, p. 59 s.

persona che entra in un negozio, sentirla parlare al telefono, stringerle la mano) sopperisce alla *richiesta* di fiducia in moltissimi casi, mentre ve ne sono altri in cui l'impressione non basta, e sono necessari documenti che dimostrino che siamo chi dichiariamo di essere, svolgiamo una certa professione, viviamo in un dato luogo o abbiamo un dato reddito. Ma generalmente, è bene sottolinearlo, non *tutte* queste informazioni sono fornite ogni volta: ad ogni episodio «problematico» dimostriamo una nostra caratteristica o sveliamo un elemento della nostra vita perché è utile rispetto al fine che intendiamo perseguire.

Dunque, perché non trasferire online tutto questo[100]? Ci possono sicuramente essere ambiti della vita in cui l'anonimato non è auspicabile, o semplicemente non è possibile, perché se chi compie l'azione ne vuole le conseguenze, deve potersi rendere identificabile. Qui la fiducia diviene responsabilità, per le azioni che l'agente vuole ricadano nella propria sfera giuridica, ed il settore più coinvolto potrebbe essere, nel senso più ampio possibile, quello dell'*e-governance*[101]. Se siamo invece normalmente anonimi in tutte le transazioni commerciali quotidiane portate a termine attraverso l'uso del contante – quanto meno in una prima fase, in cui l'edicolante o il barista non ci conoscono (ossia non abbiamo mai accettato *cookies* da loro) e comunque ci forniscono i beni o servizi richiesti, potremmo esserlo anche online. Se fuggissimo senza pagare il caffè o il quotidiano, essi potrebbero reagire rivolgendosi alle forze dell'ordine, che indagando e seguendo le nostre tracce probabilmente sarebbero in grado di risalire a noi; oppure, seccati, nutrirebbero certamente il desiderio di sapere chi siamo per poterci rintracciare, ma sarebbero in fondo consapevoli del fatto che la snellezza del sistema richiede qualche rischio, e che la perdita non è poi così significativa. O probabilmente farebbero entrambe le cose.

Ne derivano alcune brevi considerazioni:

a) è necessario cedere tutte le nostre informazioni personali, tutta la nostra storia, tutta la memoria che la Rete conserva di noi per comprare un quotidiano? Sicuramente no;

b) le indagini sugli illeciti sono ontologicamente successive alla commissione degli illeciti: se offline si seguono le tracce lasciate dall'agente (e lo si faceva ben prima della massiccia introduzione della videosorveglianza), è possibile farlo anche online, sicuramente con strumenti diversi, ma senza dover attribuire preventivamente un nome ed un volto a chiunque si affacci alla Rete[102];

c) strumenti di pagamento anonimi (carte ricaricabili, ecc.), come il contante, potrebbero essere ben più diffusi di quanto non avvenga ora, il che non si contrappone necessariamente all'imposizione di limiti (ad esempio, limiti massimi di importo che è possibile «caricare» su queste carte) dettati da altre esigenze, come quelle antiriciclaggio, ma significherebbe favorire i micropagamenti liberando al contempo l'acquirente dal rischio di essere profilato o giudicato per il contenuto del proprio «carrello virtuale»;

d) è, dunque, utile o altrimenti necessario abolire l'anonimato? Nella maggior parte dei casi no.

Responsabilità di carattere penale per reati gravi ci riportano invece a quanto già anticipato nell'*Introduzione*. I reati non diventano più gravi per il solo fatto di essere stati commessi o progettati online, e non sembra dunque sussistere una reale necessità di piegare tecnologia e diritti di rango costituzionale nel tentativo non tanto di prevenire la commissione dei medesimi reati, ma di evitare *ex post* agli organi inquirenti lo sforzo investigativo, che invece, proprio perché assistito da una pletora di garanzie per l'indagato, e reso comunque possibile ed efficace da un continuo sviluppo tecnologico (che, evidentemente, non produce solo effetti favorevoli alla criminalità), è maggiormente idoneo ad

---

[100] Chiaramente, si sta qui cercando di esemplificare una moltitudine di differenti situazioni che non possono in questa sede essere affrontate separatamente ed in maniera approfondita. Si rimanda a tal fine a R. CLARKE, *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice*, User Identification & Privacy Protection Conference, Stockholm, 14-15 June 1999, http://www.rogerclarke.com/DV/UIPP99.html (03/02/2011).

[101] Ipoteticamente la «dimostrazione» dell'identità dell'agente potrebbe avvenire a questi fini con l'utilizzo di documenti elettronici, *smart card* e simili, esattamente come avviene per l'avvocato nel processo civile telematico e come in alcune regioni già avviene per accedere ad alcuni servizi pubblici online.

[102] Estremamente interessanti sono, in tema di «ricostruzione» delle tracce lasciate online, gli studi di Latanya Sweeney che mostrano come sia possibile l'identificazione di un individuo a partire da un certo numero di dati apparentemente anonimi come il codice postale, la data di nascita o il sesso: il 53% dei cittadini americani pare sia univocamente individuato dall'insieme di queste tre informazioni. Cfr. in particolare L. SWEENEY, *k-anonymity: a model for protecting privacy*, in *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), 2002, pp. 557-570, http://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf (23/12/2010).

operare il bilanciamento fra libertà e sicurezza di quanto non lo sia la sorveglianza, in ogni sua declinazione.
Sussiste, invece, ed appare forte, il bisogno di avviare un processo di trasformazione degli *e-sorvegliati* in persone, reali *e* digitali, in grado di utilizzare consapevolmente le tecnologie e di formare a loro volta generazioni di nativi digitali che siano altrettanto consapevoli dei rischi e delle opportunità della Rete, oltre che del mondo offline. Da e-sorvegliati a *e-veglianti*: su se stessi, sui propri sistemi e sui propri famigliari. Ed anche, infine, sui propri sorveglianti, e proprio grazie all'anonimato.
Scriveva Rodotà dieci anni or sono che «[s]e la "società della trasparenza" è ormai un dato di realtà, l'unica mossa possibile sarebbe quella di sostituire alla sorveglianza ad una via (sorveglianti-sorvegliati) un potere generalizzato di controllo, reso possibile dalle nuove tecnologie elettroniche e che includa appunto anche quello dei sorvegliati sui sorveglianti», aggiungendo: «[n]on è qui il caso di discutere né l'ingenuità (?) politica di questa proposta, né le sue difficoltà tecniche»[103].
Il *synopticon* che veniva definito (dubitativamente) un'ipotesi ingenua è, come già accennato, ciò che WikiLeaks ha reso possibile, semplicemente cambiando il gioco delle luci che illuminano sorveglianti e sorvegliati.

L'anonimato in Italia. Uno strano caso.

Ma è vero che la «società della trasparenza» è un dato della realtà? Forse affermarlo è prematuro. Lo si è visto, se ne hanno riscontri quotidianamente: ci sono spinte molto forti in questo senso, ma ve ne sono anche in senso contrario, da parte di chi non intende arrendersi ad una società basata sulla sorveglianza in cui la Rete è vista come una minaccia e non per le sue enormi potenzialità.
L'Italia appare al momento un *case study* molto interessante. Per più di cinque anni, lo si vedrà a breve, un decreto «antiterrorismo» emanato d'urgenza nel mese di luglio 2005 e prontamente convertito in legge, corredato di norme interpretative e di attuazione, ha reso l'identificazione degli individui nell'accesso ad Internet la regola, con riflessi notevoli sia sulle libertà di cui si è finora parlato, sia sulla diffusione del wi-fi. Il provvedimento, noto come «decreto Pisanu», dal nome dell'allora Ministro proponente, si inquadra fra le «distorsioni» normative citate nel corso dell'*Introduzione* (par. 4) ma, al contempo, rappresenta a parere di chi scrive un passaggio importante della storia italiana di Internet, che forse è ora «storia» solo grazie al convinto, espresso e reiterato dissenso (nonché ad una certo numero di usi *contra legem* uniti talvolta a vera e propria disobbedienza civile) di tutte le parti in causa, perfino dello stesso Ministro Pisanu che nel 2009[104] si schierò, senza successo, contro l'ennesima reiterazione delle norme emergenziali da lui stesso introdotte.
Ha fatto scalpore la recente proposta[105] di inserire nella Costituzione, a completamento dell'art. 21 che riconosce la libertà di espressione, un art. 21-*bis* per garantire a tutti l'«eguale diritto di accedere alla Rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale». È vero, probabilmente, che si tratta di una precisazione (Internet come mezzo di espressione del pensiero) che, su un piano puramente teorico, potrebbe apparire superflua, ma i cinque anni di battaglie per l'abrogazione del decreto Pisanu (per quanto qui ci interessa, ma si potrebbero portare molti altri esempi) hanno insegnato che forse non basta continuare a sostenere che le garanzie costituzionali ed i valori che vi sono sottesi si applicano sia offline che online, poiché il rischio è quello di lasciare aperta una porta a chi sempre più frequentemente interviene a normare «Internet» con l'intento di limitarne l'uso e la diffusione, appellandosi di volta in volta a nuovi pericoli da prevenire e contrastare. Probabilmente, allora, la precisazione del ruolo di Internet e della sua importanza per l'espressione del pensiero è necessaria per porre un freno «dall'alto», attraverso

[103] S. RODOTÀ, *Prefazione*, cit., pp. XIII-XIV. La «società della trasparenza» citata è un riferimento a D. BRIN, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Addison-Wesley, Reading, Massachusetts, 1998.
[104] Cfr. A. GILIOLI, *Pisanu contro Pisanu*, in *L'Espresso*, 27 novembre 2009, http://espresso.repubblica.it/dettaglio/pisanu-contro-pisanu/2115894 (01/03/2011).
[105] S. RODOTÀ, *Un Articolo 21-bis per Internet*, in *Articolo21.info*, http://www.articolo21.org/2183/notizia/un-articolo21bis-per-internet-.html (30/11/2010).

il peso del rango costituzionale, a possibili derive future: «[s]olo se cresce la consapevolezza che siamo di fronte ad un diritto fondamentale della persona è possibile contrastare le logiche securitarie e mercantili che restringono il diritto a Internet. I decreti Pisanu e Romani, la pretesa dell'Agicom di regolare in via amministrativa e restrittiva l'essenziale questione del diritto d'autore hanno a loro fondamento una cultura che ritiene che le materie legate a Internet non siano accompagnate da garanzie adeguate, smentendo così nei fatti la tesi che le norme già esistenti offrano tutte le necessarie tutele. Un dialogo tra le norme esistenti e una loro formale estensione al mondo della rete farebbe avanzare nel suo insieme tutto il fronte dei diritti»[106].

[106] *Ibidem*.

CAPITOLO SECONDO

L'Italia e il «Decreto Pisanu»

SOMMARIO: 1. Introduzione. – 2. Obblighi di richiesta di licenza e obblighi di identificazione: norme diverse ed indipendenti. Ambito soggettivo di applicazione della normativa. – 2.1. Chi rientra nella definizione di «pubblico esercizio» e «circolo privato di qualsiasi specie»? Posizioni particolari. – 3. Ambito oggettivo: i dati da conservare. – 3.1. Misure di identificazione degli utenti. – 3.2. Misure di monitoraggio delle attività. – 4. Modalità di conservazione dei dati. – 5. La situazione dopo il 31 dicembre 2010. – 6. Sanzioni.

1. Introduzione.

Il D.L. 27 luglio 2005, n. 144 (convertito in L. 31 luglio 2005, n. 155) ha introdotto nel nostro ordinamento l'obbligo per chi offra un servizio di connettività al pubblico di registrarsi e ottenere una licenza preventiva dalla Questura, nonché di identificare attraverso un documento di identità gli utenti che per suo tramite accedono alla Rete, di registrarne gli accessi, custodire i relativi dati di traffico e metterli a disposizione delle forze dell'ordine e della magistratura dietro eventuale richiesta. Il provvedimento in questione, emanato d'urgenza e convertito in legge a distanza di pochi giorni dal legislatore italiano in reazione agli attentati terroristici di Londra del luglio 2005, era concepito e largamente inteso quale risposta all'esigenza contingente di individuare strumenti giuridici di prevenzione di ulteriori attacchi terroristici anche mediante un controllo penetrante sulle comunicazioni telematiche.
Il carattere transitorio della normativa, che emerge chiaramente dai resoconti stenografici relativi alla fase di conversione in legge (fase che, proprio in virtù della convinzione della maggioranza parlamentare e di parte dell'opposizione di trovarsi di fronte ad un testo tutto sommato provvisorio si è consumata in un brevissimo lasso di tempo), si è tuttavia tramutato nel tempo in ordinario: di anno in anno, e fino a dicembre 2010, le scadenze contenute nel testo della legge sono infatti state prorogate, obbligando all'identificazione preventiva gli utenti che volevano accedere alla Rete tramite un punto di accesso pubblico (ed obbligando altresì chiunque volesse 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» a richiedere di una apposita licenza preventiva alla Questura).
Il D.L. 29 dicembre 2010, n. 225, convertito con L. 26 febbraio 2011, n. 10, ha recentemente posto fine ad una «anomalia» che non aveva paragoni nelle democrazie occidentali (nonché in moltissimi altri Paesi considerati «non democratici»).
Scopo del presente capitolo è quello di analizzare in maniera approfondita le previsioni del D.L. 144/2005 nonché dei provvedimenti che vi erano collegati, di evidenziarne le più evidenti criticità e di rilevare quali siano le modifiche apportate dal D.L. 225/2010, al fine di tracciare un quadro preciso di quali siano stati gli obblighi imposti ai diversi soggetti coinvolti e quali siano quelli attuali, di arricchire l'analisi svolta finora e fornire, quale *case study* appartenente ad un recentissimo passato, eventuali spunti per future considerazioni, anche in un'ottica *de jure condendo*.

2. *Obblighi di richiesta di licenza e obblighi di identificazione: norme diverse ed indipendenti. Ambito soggettivo di applicazione della normativa.*

Come già anticipato, con la dicitura «decreto Pisanu», che prende il nome da uno dei Ministri proponenti, ci si riferisce al **decreto-legge 27 luglio 2005, n. 144**, recante Misure urgenti per il contrasto del terrorismo internazionale, convertito in legge, con modificazioni, dall'art. 1, L. 31 luglio 2005, n. 155 (Gazz. Uff. 1 agosto 2005, n. 177), entrata in vigore il giorno successivo a quello della sua pubblicazione. In relazione all'accesso ad Internet da postazioni pubbliche ed all'accesso mediante connessione wi-fi, che hanno costituito l'oggetto della presente indagine, l'articolo di riferimento è l'art. 7.

Il quarto comma dell'art. 7 rimanda poi ad un decreto ministeriale per la disciplina di dettaglio: si tratta del **D.M. 16 agosto 2005**.

Infine, per meglio interpretare quanto previsto dal decreto legge e dal decreto ministeriale, può essere utile far riferimento anche alla **Circolare del 29 agosto 2005 del Dipartimento della pubblica sicurezza**, espressamente rivolta agli Uffici ed agli Operatori di Polizia.

L'art. 7 del decreto Pisanu poneva due distinte questioni[107]:

a) il primo, secondo e terzo comma sono relativi all'obbligo di richiedere licenza preventiva al questore per «[…] chiunque 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**[…] La licenza non è richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale»;
b) il quarto e quinto comma riguardano invece «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, […] 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**

[107] Per comodità si riporta interamente il testo del previgente art. 7, «Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet», nella versione introdotta dalla L. 155/2005 (si noti che la data del «31 dicembre 2007» è la parte che è stata assoggettata a proroga anno dopo anno e va dunque letta come 31 dicembre dell'anno successivo al decreto di proroga, fino, con la proroga del 2009, al 31 dicembre 2010. La nuova formulazione dell'art. 7 sarà invece analizzata in seguito).

«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 2007, chiunque 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 e' 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 regio decreto 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 decreto legislativo 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 tecnologica, 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, e' 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'articolo 122, e dal comma 3 dell'articolo 123 del decreto legislativo 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 decreto legislativo 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.»

ovvero punti di accesso ad Internet utilizzando tecnologia senza fili». Tali misure sono elencate dal D.M. 16 agosto 2005.

Pur essendo contenute nello stesso articolo di legge le due questioni debbono mantenersi separate, poiché è possibile che taluni soggetti, pur non rientrando nella definizione di «pubblico esercizio» o «circolo privato di qualsiasi specie» di cui al primo comma, mettano a disposizione «postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili», rientrando di conseguenza nell'ambito di applicazione del quarto comma e, dunque, del D.M. 16 agosto 2005.

Tale interpretazione appare confermata dalla lettera del D.M. 16 agosto 2005, laddove:

a) la disciplina di cui all'art. 1 riguardante titolari e gestori di esercizi pubblici e circoli privati di qualsiasi specie viene estesa dall'**art. 3, comma 1**, anche ai «**fornitori**» dei medesimi terminali di cui all'art. 1 qualora «collocati in aree non vigilate» (pur se con esclusione dell'obbligo di monitorare le attività);
b) vengono espressamente citati (all'**art. 3, comma 2**) i terminali installati all'interno di «centri di ricerca, università ed altri istituti di istruzione», che non sembrano in alcun modo poter rientrare nella definizione di «pubblico esercizio» o «circolo privato di qualsiasi specie» e che, purtuttavia, sembrano rientrare a pieno titolo (sia perché logicamente inclusi – si tratta di «fornitori di apparecchi terminali utilizzabili per le comunicazioni telematiche» –, sia perché contemplati nell'ambito del medesimo articolo) fra i terminali di cui all'art. 3, comma 1, dalla cui disciplina si discostano solamente per il tempo di validità delle credenziali attraverso le quali è garantita l'identificazione dell'utente;
c) l'art. 4 si rivolge ad un insieme di destinatari ben più ampio di quello individuato dall'art. 1, ed è composto genericamente dai «**soggetti che offrono accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico**» i quali, indipendentemente dall'operatività degli articoli precedenti sono comunque «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».

Nel medesimo senso depone anche la Circolare del 29 agosto 2005 del Dipartimento della pubblica sicurezza, laddove (al secondo paragrafo della sezione «Decreto interministeriale 16 agosto 2005» chiarisce che «l'osservanza degli obblighi ivi prescritti prescinde dal regime autorizzatorio delle attività esercitate e va quindi assicurata anche da parte di coloro che già svolgono le attività in argomento, indipendentemente dagli adempimenti di cui al comma 2 dell'art. 7».

La prima fondamentale conseguenza del fatto che l'art. 7 contenesse in realtà diverse norme è che la scadenza di cui al primo comma (originariamente il 31 dicembre 2007, prorogato fino al 31 dicembre 2010), non ripetuta né altrimenti richiamata nel quarto, stante la non connessione fra le diverse questioni ivi regolate, si riferiva esclusivamente alla richiesta di licenza e non anche all'identificazione e alla conservazione dei dati di traffico. Per diversi anni, ed in particolare negli ultimi due, le istanze rivolte al legislatore andarono nel senso di chiedere di non prorogare ulteriormente la scadenza di cui al primo comma, ma a ben vedere una tale richiesta avrebbe potuto rivelarsi inutile, poiché **senza l'abrogazione dell'intero art. 7, o almeno** (come poi è effettivamente accaduto) **dei commi quarto e quinto, sarebbe caduto l'obbligo di richiedere la licenza al Questore, ma sarebbero rimasti quelli relativi all'identificazione e al monitoraggio del traffico**, non soggetti a scadenza.

Nessuna valenza pratica sembrava infatti potersi attribuire al fatto che sia dalla relazione illustrativa del disegno di legge di conversione del D.L. 144/2005[108], sia dai resoconti stenografici dei dibattiti che si susseguirono nelle commissioni parlamentari prima della conversione stessa[109], emergesse piuttosto chiaramente come tutto l'impianto dell'art. 7 (oltre che del decreto legge nel suo insieme) fosse concepito come provvisorio, e solo in quanto tale convertito in legge. È infatti al tenore letterale della norma che, in primo luogo, bisogna far riferimento in sede ermeneutica, e sebbene sembrasse almeno peculiare che soggetti a cui non è imposto alcun obbligo di «licenza» dovessero identificare in maniera forte i propri avventori o soci[110] (cosa che sarebbe accaduta se, appunto, fosse caduta la prima parte dell'art. 7 come conseguenza della mancata proroga e fosse invece rimasta in vigore la seconda parte), tale appariva la situazione consolidatasi con l'approvazione e la successiva conversione del D.L. 144/2005.

Nel corso del 2010 una disposizione contenuta nel disegno di legge collegato alla manovra finanziaria 2010 prometteva di complicare ulteriormente il quadro relativo alla sfera di applicazione soggettiva della normativa *de qua*. Il D.d.L., recante «Disposizioni in materia di semplificazione dei rapporti della Pubblica amministrazione con cittadini e imprese e delega al Governo per l'emanazione della carta dei doveri delle amministrazioni pubbliche», approvato dal Consiglio dei Ministri il 12 novembre 2009, prevedeva all'art. 3, comma 3[111] che fosse inserito un comma 2-bis all'art. 7 del D.L. 144/2005, secondo il quale «Le disposizioni del comma 1 non si applicano ai gestori di esercizi alberghieri e di altre strutture ricettive, comprese quelle che forniscono alloggio in tende o in *roulotte*, né ai proprietari o ai

---

[108] La relazione illustrativa è consultabile all'URL http://www.giustizia.it/giustizia/it/mg_1_2_1.wp;jsessionid=651660AC483822EBEAD07E0C01102B31.ajpAL01?previsiousPage=mg_1_2_1&contentId=SAN30791 (15/02/2010), e vi si legge chiaramente che l'art. 7 prevede «per un periodo circoscritto fino al 31 dicembre 2007, la necessità di una specifica autorizzazione di polizia e l'adozione di specifiche misure di identificazione degli utenti».

[109] Cfr. ad esempio, al Senato, il Resoconto stenografico dell'assemblea, seduta n. 857 del 28/07/2005, http://www.senato.it/ service/PDF/PDFServer/BGT/00145146.pdf, dove si dice che il provvedimento «come tutti quelli assunti in fasi emergenziali, presenta luci ed ombre» e che « certo, ci sono disposizioni che possono far sorgere qualche dubbio sulla loro totale aderenza al dettato costituzionale» (p. 71), o alla Camera il Resoconto stenografico dell'assemblea, seduta n. 666 del 30/07/2005, http://legxiv.camera.it/_dati/leg14/lavori/stenografici/sed666/s100.htm, in cui l'on. Ascierto dice di « riconoscere al ministro dell'interno - lo riteniamo fondamentale - di avere asserito in questa sede, stamani, che il provvedimento è perfettibile, che esso sarà sperimentale nei prossimi mesi e che potremo migliorarlo dopo averlo sperimentato» (p. 56). Indicazioni interessanti possono essere rinvenute anche dalla lettura dei resoconti delle sedute n. 858 del Senato (http://www.senato.it/service/PDF/PDFServer/BGT/00145206.pdf), dei resoconti sommari delle Commissioni (ad esempio: n. 18 del 27/07/2005, in cui si dice che « Il controllo sulle operazioni e i dati di comunicazioni telematiche di cui all'articolo 7 presenta profili di limitazione alle libertà dei cittadini che trovano però un fondamento nelle straordinarie esigenze di sicurezza ad essa sottesa e che è dunque ammissibile, anche in considerazione della sua vigenza limitata nel tempo», http://notes9.senato.it/W3/Lavori.nsf/All/E00DCEBB504DD6F4C125704C00673AED?OpenDocument; Commissioni riunite del 29/07/2005, http://legxiv.camera.it/_dati/leg14/lavori/bollet/frsmcdin.asp?percboll=/_dati/leg14/lavori/bollet/200507/0729/html/0102/&pagpro=6n3&all=off&commis=0102 e resoconto del Comitato per la legislazione del 29/07/2005, http://legxiv.camera.it/_dati/leg14/lavori/bollet/frsmcdin.asp?percboll=/_dati/leg14/lavori/bollet/200507/0729/html/48/&pagpro=4n2&all=off&commis=48). Interessante, infine, per l'oggetto della presente analisi, l'intervento dell'on. Folena alla succitata seduta della Camera n. 666 del 30/07/2005 (pp. 77-78), di cui si cita un estratto: «[…] Siamo di fronte ad una violazione di libertà fondamentali ed anche ad una misura che ha un peso economico. Infatti, le regole che saranno dettate nel decreto attuativo del Governo comporteranno un costo che graverà sulle imprese, sulle piccole attività, sugli esercenti titolari di queste attività, i quali dovranno adeguarsi - chissà come, chissà con quali risorse - a spese loro. A me sembra che questa sorta di ossessione rischi di far commettere errori molto pesanti, che - lo ripeto - nulla hanno a che fare con la lotta al terrorismo. Siamo riusciti a combattere la mafia, il terrorismo, la pedopornografia ed altri gravissimi reati con le leggi vigenti, senza bisogno di trasformare i punti di accesso ad Internet, in cui uno paga per navigare, in una sorta di orecchi che ti controllano in modo generico per un periodo di tempo illimitato. A nostro giudizio, ciò è inaccettabile!» (tutte le URL verificate da ultimo il 28/02/2011).

[110] Va precisato, tuttavia, che esercizi pubblici e circoli sono soggetti ad altri obblighi previsti dalle leggi di Pubblica Sicurezza: i titolari pertanto erano (e sono tuttora) comunque identificati, seppure ad altri fini.

[111] Il D.d.L. C.3209-bis è consultabile all'URL http://nuovo.camera.it/view/doc_viewer_full?url=http%3A//web.camera.it/_dati/leg16/lavori/stampati/pdf/16PDL0034280.pdf&back_to=http%3A//nuovo.camera.it/126%3FPDL%3D3209-BIS%26leg%3D16%26tab%3D2 (07/04/2010) nell'ultima versione risultante dallo stralcio degli articoli 14, 25 e 27 del disegno di legge n. 3209, disposto dal Presidente della Camera, ai sensi dell'articolo 123-bis, comma 1, del Regolamento, e comunicato all'Assemblea il 2 marzo 2010.

gestori di case e di appartamenti per vacanze né agli affittacamere, fermo restando quanto disposto dai commi 3, 4 e 5»[112].
Nelle intenzioni dei Ministri proponenti tale modifica avrebbe dovuto facilitare chi si fosse trovato in viaggio sul territorio nazionale, snellendo, a monte, gli adempimenti richiesti alle strutture ricettive. Tuttavia, risultò immediatamente non comprensibile sia il motivo per cui destinatari delle agevolazioni fossero le sole strutture ricettive e non anche, ad esempio, esercizi commerciali parimenti (o forse, più intensamente) frequentati dai viaggiatori in transito sul territorio, sia perché ci si fosse interessati dei soli viaggiatori (peraltro, non facendo venir meno in alcun modo l'obbligo di identificazione e tenuta dei *log*) e non dei cittadini residenti o di tutti coloro che, molto più semplicemente, non dimoravano presso una delle strutture ricettive individuate dalla norma.
Anche questa proposta di modifica, che poi non fu recepita, sembrava in ogni caso confermare l'interpretazione per cui obbligo di richiedere la licenza preventiva e obblighi di identificazione e tracciabilità del «comportamento online» degli utenti si muovessero su binari separati, ed i secondi non venissero meno in conseguenza di una mancata proroga della scadenza contenuta al primo comma dell'art. 7.

2.1. Chi rientra nella definizione di «pubblico esercizio» e «circolo privato di qualsiasi specie»? Posizioni particolari.

La definizione di «**pubblico esercizio**» è rinvenibile all'art. 86 del TULPS[113] e riguarda categorie estremamente eterogenee di esercizi commerciali, quali quelli per la somministrazione di alimenti e bevande, strutture ricettive, stabilimenti balneari, sale giochi, ecc. La norma (che richiama quella di cui all'art. 7, comma 1, D.L. 144/2005 anche nell'accennare, per taluni aspetti, ai «circoli privati») è tuttavia rivolta ad individuare gli esercizi per l'apertura dei quali è necessario ottenere la licenza, e si ritiene perciò possa fornire un'indicazione solo approssimativa delle attività contemplate dal D.L. 144/2005. La questione è comunque interessante, poiché, interpretata letteralmente, la norma di cui al comma 1 del citato art. 7 sembrava non prescrivere l'obbligo di licenza preventiva per la fornitura di connettività ad esercizi commerciali quali librerie o centri estetici, che non rientrano nella definizione del TULPS di pubblico esercizio. Il tenore complessivo del D.L. 144/2005 lasciava comunque ritenere che per «pubblico esercizio» dovesse intendersi qualsiasi attività commerciale, ed in questo senso depone anche la Circolare del Dipartimento di pubblica sicurezza del 29 agosto 2005 che espressamente parla di «esercizi commerciali aperti al pubblico» e di «circoli privati» (cfr. secondo paragrafo della sezione «Disciplina della licenza»).
Quanto ai **circoli privati**, la norma di riferimento è il D.P.R. 4 aprile 2001, n. 235, «Regolamento recante semplificazioni del procedimento per il rilascio dell'autorizzazione alla somministrazione di alimenti e bevande da parte di circoli privati», che tuttavia utilizza l'espressione «circoli privati» solo nel titolo e all'art. 1, comma 1 (che ribadisce «Le disposizioni del presente regolamento si applicano al procedimento relativo alla somministrazione di alimenti e bevande da parte di circoli privati»), mentre all'art. 2, comma 1, sono citate le «associazioni» e i «circoli». In assenza di una specifica definizione può ritenersi che i circoli privati si differenzino dai pubblici esercizi in quanto costituiti non in forma di impresa, ma come associazioni senza scopo di lucro, generalmente non riconosciute. La differenza principale rispetto ai pubblici esercizi è perciò, ai nostri scopi, che mentre a questi può accedere chiunque indistintamente, ai circoli può accedere solo chi sia associato al circolo stesso (in genere in possesso di una tessera o altro contrassegno idoneo a provare il vincolo associativo).
Ciò premesso, appare abbastanza agevole identificare chi fosse soggetto all'obbligo di licenza e chi invece ne fosse escluso. Fra gli esempi più significativi di esclusione potevano annoverarsi i **privati con rete «aperta»** (anche se «organizzati»: v. ad esempio il progetto FON[114]), poiché in nessun modo

[112] Ossia: ferme restando le disposizioni relative all'identificazione e al monitoraggio. Appariva leggermente «sviante» il riferimento al terzo comma, poiché esso si riferiva principalmente a questioni connesse all'obbligo di licenza che il comma 2-bis invece mirava proprio ad escludere, ma può ritenersi che tale richiamo valesse solamente a ribadire l'applicabilità – nella misura in cui si fossero rivelate compatibili – delle norme ivi citate.
[113] R.D. 18 giugno 1931, n. 773, richiamato anche dallo stesso art. 7, terzo comma, laddove specifica che si applicano le norme contenute nel capo II del titolo III del TULPS (capo che si apre proprio con l'art. 86).
[114] «Fon is the world's first global WiFi network built by people like you. We think of it as crowdsourced WiFi. As a member of the Fon community, you agree to share a little bit of your WiFi at home, and get free roaming at Fon Spots worldwide in

potevano essere equiparati alla nozione di «circolo privato» – che presuppone comunque la messa a disposizione di un luogo di ritrovo, indipendentemente dalla tipologia di accesso e alla frequentazione dello stesso – né tantomeno di «esercizio».
Erano inoltre esclusi gli enti – anche solo *lato sensu* – pubblici che non possono rientrare nella definizione di «circolo privato» o in quella di «pubblico esercizio». Tuttavia alcuni di essi, come si è visto (**università**, **centri di ricerca** e «**altri istituti di istruzione**») sono stati espressamente inquadrati dall'art. 3 co. 2 del D.M. 16 agosto 2005 in una più ampia categoria di «fornitori» che erano soggetti a tutti gli obblighi dei titolari e dei gestori tranne che per il monitoraggio delle attività.
Per le **biblioteche** (non espressamente prese in considerazione dalla normativa in esame) sembrava potersi abbracciare la medesima soluzione, e tale interpretazione è suffragata dalla risposta fornita il 16 ottobre 2005 dal Ministro Pisanu alla lettera inviata congiuntamente dai Presidenti di ANCI e UPI su sollecitazione dell'AIB, di cui si riporta uno stralcio (enfasi aggiunta):
«[...] va osservato che l'art. 7 del decreto legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, ha integrato la disciplina amministrativa degli esercizi pubblici di telefonia ed internet, eppertanto **debbono munirsi della relativa licenza solo tali esercizi ed i circoli privati di qualsiasi specie, in quanto espressamente contemplati dalla norma**, nei quali sono posti a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni anche telematiche.
La richiamata disposizione, riguardante il regime autorizzatorio, non trova quindi applicazione per le postazioni non vigilate gestite direttamente da biblioteche o altri enti pubblici, per le quali va invece applicato l'articolo 3 del decreto del 16 agosto 2005, in combinato disposto con l'articolo 1 dello stesso decreto, che impongono di adottare le misure fisiche e tecnologiche occorrenti per impedire l'accesso agli apparecchi terminali a persone che non siano state preventivamente identificate, anche mediante credenziali di accesso pre-pagate o gratuite.»[115]
Nella lettera del Ministro si faceva anche riferimento al fatto che il Dipartimento della pubblica sicurezza avrebbe dovuto comunicare all'AIB le specifiche disposizioni impartite alle Questure in merito alle credenziali di accesso e alle conseguenti modalità di identificazione delle persone ma, interpellati tramite mailing-list gli iscritti all'AIB, fu appurato che non risultava alcuna ulteriore comunicazioni del Ministro o del Dipartimento della pubblica sicurezza a loro specificamente diretta.
I **privati** che non proteggono l'accesso alla propria Rete wireless non rientrano nemmeno nella definizione di fornitori di cui al predetto art. 3, che comunque si riferisce alla fornitura di terminali e non (solo) di connettività. Più problematica risultava invece l'interpretazione dell'art. 4, laddove non si parla più né di terminali né di fornitori o di esercizi, ma di semplice «accesso alle reti telematiche» e di «soggetti» che offrono un tale accesso. Sembrava tuttavia potersi ritenere che i privati che lasciavano «aperta» la propria rete domestica si ponessero al di fuori anche dell'ambito di operatività di questa norma, dal momento che l'offerta di connettività doveva avvenire, ai sensi dell'art. 4, «in aree messe a disposizione del pubblico», e tali non possono certamente ritenersi né il privato domicilio né le sue immediate pertinenze, né (poiché ciò non costituisce oggetto di un atto di volontà specifico del singolo di «mettere a disposizione l'area») le aree pubbliche o private confinanti che fossero state coperte dal segnale wi-fi.
La portata estremamente ampia della disposizione in oggetto non consentiva invece di escludere dall'obbligo di identificazione **figure che si collocano ad un livello intermedio fra i privati ed i circoli**, come possono essere, ad esempio, le parrocchie (ma, eventualmente, anche singoli privati nell'esercizio di un'attività di volontariato «autonoma», non collegata cioè ad un'associazione) che mettono a disposizione alcuni locali per attività ricreative (come i «doposcuola»): per essi trovava infatti applicazione l'art. 4 per quanto riguarda la fornitura di connettività attraverso tecnologia senza fili poiché è possibile individuare delle aree «messe a disposizione del pubblico», mentre in assenza di uno specifico richiamo in tal senso (presente per la sola identificazione) apparivano esclusi gli altri obblighi previsti dall'art. 1 dello stesso Decreto. Se, tuttavia, oltre alla connettività, tali soggetti avessero messo a

return. Sharing WiFi with Fon is safe and secure, and you wont even notice when others are connected because Fon only uses a tiny portion of your bandwidth. […]»: http://www.fon.com/en/info/whatsFon (28/02/2011).
[115] Testo reperibile sul sito dell'AIB all'URL http://www.aib.it/aib/cen/stampa/c0509.htm (15/02/2010).

disposizione anche dei terminali dedicati alla navigazione in Internet, sarebbe divenuto interamente applicabile l'art. 3 e, dunque, l'insieme delle disposizioni dell'art. 1, con la sola eccezione dell'obbligo di monitoraggio delle attività degli utenti.
Non è mai stato chiarito, infine, cosa si intendesse con la dicitura «**postazioni pubbliche non vigilate per comunicazioni telematiche**» di cui all'art. 7, quarto comma, del D.L. 144/2005, ripresa dall'art. 3 primo comma del D.M. 16 agosto 2005 (che parla di «fornitori di apparecchi terminali utilizzabili per le comunicazioni telematiche […] collocati in aree non vigilate»). In particolare, appariva arduo comprendere in cosa avrebbe dovuto esplicitarsi una eventuale attività di «vigilanza» e chi (presumibilmente il «fornitore») avrebbe dovuto attuarla, e la questione poteva rivelarsi interessante poiché, stante il tenore letterale della norma, dalla presenza o meno di tale «vigilanza» nelle aree in cui erano messi a disposizione di altri soggetti dei terminali destinati alla navigazione dipendeva l'applicabilità dell'art. 3 del D.M. 16 agosto 2005. Di conseguenza era ipotizzabile un'ulteriore categoria di soggetti, individuata in modo residuale ed «a contrario», coincidente con i «fornitori» che non possono essere qualificati né pubblici esercizi né circoli privati e che mettevano a disposizione del pubblico dei terminali in aree vigilate, i quali non sarebbero stati soggetti a nessuno degli obblighi (licenza, identificazione, monitoraggio) imposti dalla normativa in esame. Ancora diversa, e logicamente (e teleologicamente) più giustificabile, è invece l'ipotesi in cui le postazioni vigilate non fossero «pubbliche»[116], ma destinate ad essere frequentate da un gruppo più o meno circoscritto di persone, come può avvenire all'interno di un istituto di istruzione (una scuola, o anche un ente privato che organizzi corsi di formazione) nel quale si tengano lezioni in aula utilizzando terminali abilitati ad accedere ad Internet: sugli iscritti avrebbe infatti «vigilato» l'insegnante e/o altro personale (come i tecnici di laboratorio o altri ausiliari), e, contemporaneamente, non si sarebbe nemmeno potuto parlare di «postazioni pubbliche», talché anche in questo caso dovevano considerarsi esclusi gli obblighi di licenza, identificazione e monitoraggio.
La tabella che segue costituisce un tentativo di sintetizzare quanto finora esposto (e, per comodità, anticipa parzialmente quanto si dirà *infra* al par. 3.2).

Tabella 1 – Sintesi dei possibili soggetti coinvolti e dei relativi obblighi (fino al 31 dicembre 2010).

Soggetti	**Obbligo richiesta licenza**	**Obbligo identificazione**	**Obbligo monitoraggio**
1) Esercizi commerciali, circoli privati, associazioni, ecc. che mettono a disposizione **terminali** (aree vigilate e non)	X	X	X
2) - Università, centri di ricerca, altri istituti di istruzione - biblioteche - altri fornitori che non siano 1) che mettono a disposizione **terminali** in aree non vigilate		X	
3) Chiunque offra solo accesso alle reti telematiche mediante **WiFi** (no terminali), in un'**area messa a disposizione del pubblico**		X	
4) Chiunque lasci aperta la propria rete **WiFi** (consapevolmente o meno) **senza mettere a disposizione un'area**			
5) «Fornitori» (non 1) che mettono a disposizione **terminali** in **aree vigilate**			

[116] Si noti che il carattere di accessibilità «pubblica» del terminale è richiamato solo dal quarto comma del D.L. 144/2005 e non anche dalla normativa di dettaglio posta dal D.M. 16 agosto 2005.

(postazioni **pubbliche** - ipotesi - **e non**)			

3. Ambito oggettivo: i dati da conservare.

Appare importante distinguere, all'interno del D.L. 144/2005, le disposizioni che impattano sugli obblighi di conservazione dei dati del traffico Internet che gravano sui fornitori dei servizi di rete (art. 6) e quelle che invece, per espressa indicazione della relazione illustrativa al disegno di legge, sono destinate «ad incidere non sulle attività inerenti alla fornitura delle reti o dei servizi di comunicazione elettronica, ma sull'offerta "all'utente occasionale" di specifici servizi in locali pubblici o aperti al pubblico»[117] (art. 7).
Concentrandoci, in questa sede, sulle sole prescrizioni introdotte dall'art. 7, che, al quarto comma, rimanda al contenuto del D.M. 16 agosto 2005, possiamo ulteriormente distinguere, riprendendo in parte quanto già prospettato al paragrafo precedente, fra:

- **misure di identificazione degli utenti**, prescritte a tutti i soggetti che offrivano connettività alla Rete, sia utilizzando tecnologia senza fili (in aree messe a disposizione del pubblico, secondo quanto precisato sopra), sia mettendo a disposizione terminali utilizzabili per la navigazione;
- **misure di monitoraggio delle attività**, prescritte solo nel caso in cui i terminali fossero messi a disposizione in un esercizio pubblico o in un circolo privato (secondo le definizioni di cui sopra).

3.1. Misure di identificazione degli utenti.

L'art. 1 del D.M. 16 agosto 2005 prevedeva che gli utenti dovessero essere previamente identificati «acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente».
Va in primo luogo sottolineato come per «documento d'identità» debba intendersi, ai sensi dell'art. 1, lett. d, del Testo Unico in materia di documentazione amministrativa (D.P.R. 28 dicembre 2000, n. 445), «la carta di identità ed ogni altro documento munito di fotografia rilasciato, su supporto cartaceo, magnetico o informatico, dall'amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare».
Il fatto che siano previsti anche documenti rilasciati da altri Stati introduceva, anche in relazione all'identificazione dell'utente, un elemento di complessità, derivante dal fatto che il fornitore di connettività non avrebbe dovuto essere considerato responsabile per la mancata identificazione sia qualora gli si fosse presentato un documento apparentemente rilasciato dallo Stato italiano falsificato «ad arte», sia, a maggior ragione, quando il documento fosse in apparenza emesso da uno Stato estero, dal momento che dal gestore di un Internet point non poteva certo esigersi una conoscenza approfondita di tutti i documenti validi ai fini dell'identificazione in tutti gli stati del mondo, in particolar modo se emessi utilizzando non solo una lingua, ma anche un alfabeto diverso dall'italiano (si pensi ad esempio all'arabo o al cinese).
Il momento iniziale dell'identificazione sembrava perciò rappresentare una prima importante debolezza del sistema introdotto dal D.L. 144/2005: ammesso che un potenziale terrorista non si fosse reso anonimo utilizzando mezzi alternativi (alcuni dei quali saranno esaminati in seguito), avrebbe comunque potuto utilizzare un documento falso, o in altro modo non «utile» ai fini di una futura identificazione, ed ottenere così il tempo necessario per accedere alla Rete, raggiungere i propri obiettivi e cancellare le proprie tracce prima che qualcuno potesse accorgersi della sua mancata identificazione. È vero infatti che il documento deve recare la foto della persona da identificare, ma ciò che, di fatto, poteva essere davvero appurato dal gestore era che un soggetto *somigliante* (secondo l'apprezzamento

[117] Cfr. nuovamente la Relazione illustrativa del disegno di legge di conversione del D.L. 144/2005.

dello stesso gestore) a quello ritratto nel documento «identificativo» si era presentato nel suo locale in un certo momento storico e per una certa durata.
Tale osservazione poteva peraltro riferirsi sia alle postazioni «vigilate», per le quali non era stabilita una scadenza delle credenziali di accesso ad uso plurimo, sia a quelle collocate in aree non vigilate di cui all'art. 3 primo comma, per le quali la durata massima di un anno dall'identificazione appariva comunque un periodo di tempo sufficiente a compiere le azioni di cui sopra, sia infine, e soprattutto, per l'accesso mediante wi-fi.
È da sottolineare anche l'incongruenza di fondo sussistente fra le modalità di identificazione diretta mediante documento e quelle di **identificazione indiretta** che furono indicate successivamente dallo stesso Ministero dell'Interno[118] come sufficienti per ottemperare all'obbligo di identificazione dell'utente.
Nel caso di identificazione tramite **SIM card** (utilizzabili per l'accesso alle reti wi-fi) era infatti espressamente previsto che le SIM fossero state rilasciate all'utente «rispettando le disposizioni relative all'identificazione dello stesso, previste dall'art. 55 del D. Lgs. n. 259/03 – Codice delle Comunicazioni Elettroniche, che prevede l'identificazione completa dell'utente prima dell'attivazione del servizio, con esclusione, quindi di SIM/USIM rilasciate da paesi stranieri».
Per le **carte di credito/debito**, considerate, invece, metodo sufficiente di identificazione dell'utente per connettersi alla Rete «attraverso l'utilizzo di postazioni pubbliche non vigilate», le incongruenze potevano ravvisarsi sotto almeno due profili: da un lato, infatti, va rilevato che molte *debit card*, all'estero ma anche in Italia[119], possono essere emesse in maniera anonima ed usate «al portatore», e dall'altro, non appaiono chiari i presupposti in base ai quali SIM e carte fossero ritenute idonee ad identificare gli utenti di tipologie di reti diverse (rispettivamente wi-fi e con postazioni non vigilate) e per quale motivo fossero poi individuati obblighi diversi a carico dei titolari (qualora l'identificazione fosse avvenuta mediante carta di credito/debito, essi avrebbero infatti dovuto «mantenere i dati associati tra la carta utilizzata e il traffico effettuato, esclusi i contenuti delle comunicazioni»[120]).
Ulteriori questioni concernenti l'identificazione degli utenti sono poi sollevate dall'art. 4 del decreto, laddove era prescritto ai soggetti che offrivano accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico di adottare le «misure fisiche o tecnologiche occorrenti per **impedire l'uso di apparecchi terminali che non consentono l'identificazione dell'utente**» (oltre che ad utenti che non fossero identificati secondo le modalità di cui all'art. 1).
Il riferimento al fatto che gli apparecchi terminali dovessero consentire l'identificazione dell'utente, in assenza di ulteriori indicazioni volte a chiarire il contenuto della norma, sembrava relativo all'utilizzo di sistemi di autenticazione informatica basate su tecniche quali il *captive portal*, che reindirizzano il browser verso una pagina di *login* (*landing page*) allo scopo di abilitare l'indirizzo IP e/o MAC del terminale alla navigazione[121].
Appare rilevante ricordare questa disposizione poiché l'interpretazione appena fornita sembrava comportare da un lato l'esclusione dalla possibilità di connettersi alla Rete per tutti i terminali che non consentano di usare tecniche di captive portal o similari, ossia che pur possedendo connettività wi-fi e supporto per il TCP/IP non siano dotati di *browser* web che supporti HTTPS[122] e, dall'altro, imponeva

---

[118] Parere reso dal Ministero dell'Interno (Dipartimento della Pubblica Sicurezza) su sollecitazione di Assoprovider il 27 novembre 2007 (n. 300D/89/44/F320/3668) e reso gentilmente disponibile da Assoprovider.
[119] Si tratta delle c.d. carte «usa e getta», operanti su diversi circuiti (Visa Electron e Mastercard), alcune in versione «ricaricabile» (ad esempio *Postepay New Gift*, di Poste Italiane), altre non ricaribili e vendute secondo tagli predefiniti (es.: *Kalibra*, emessa da Banca Popolare Italiana, e *Soldintasca* del Gruppo Intesa Sanpaolo, entrambe rilasciate anche nelle ricevitorie SISAL in modo completamente anonimo).
[120] Cfr. ancora il Parere cit. Si veda poi, su quest'ultimo punto, il par. 4, laddove si affronta la questione della scadenza dell'obbligo di conservazione dei dati relativi all'identificazione.
[121] L'utilizzo di un captive portal sembra suggerito anche nel già citato parere del 27 novembre 2007, come modalità per procedere all'identificazione dell'utente mediante SIM card: «L'esempio di richiesta di accesso alla rete attraverso la tecnologia WI-FI, e della necessaria identificazione, può essere il seguente: l'utente, dopo aver avviato il proprio dispositivo in un'area coperta dal segnale, ed aver aperto il proprio browser, potrà navigare in un ambito ristretto che consentirà, quindi, la sola registrazione al servizio. […] Una volta che l'utente terminerà le procedure di autenticazione, ed avrà immesso le credenziali ricevute, allora potrà procedere liberamente alla navigazione in rete […]».
[122] In realtà non è infrequente imbattersi in landing pages non criptate che, se da un lato risolvono il possibile problema del

ai fornitori di connettività di dotarsi di un *router* che incorporasse nel *firmware* un *captive portal*, o di utilizzare un software con le stesse funzionalità. L'obbligo imposto al fornitore era infatti duplice e ricadeva *sia* sull'identificazione dell'utente secondo le modalità di cui si è dato atto in precedenza, sia sui terminali, che dovevano essere ammessi alla navigazione solo in quanto consentissero l'identificazione. Il disgiuntivo «ovvero» è infatti da intendersi come inclusivo (*vel*): non dovevano poter accedere alla Rete *né* utenti identificati secondo le modalità di cui all'art. 1 che poi utilizzassero terminali che non consentivano l'identificazione (ad esempio, se in assenza di un *captive portal* ci si fosse limitati, in fase di registrazione, a fornire la chiave di rete all'utente), *né*, tantomeno, utenti che pur utilizzando terminali «identificabili» non fossero stati essi stessi previamente identificati (ad esempio in caso di utilizzo di credenziali altrui da parte di un utente non identificato). Tale ultima ipotesi è peraltro considerata anche all'art. 1, comma terzo, del medesimo decreto, in relazione ai gestori che mettono a disposizione terminali mediante l'utilizzazione di credenziali ad accesso plurimo: per loro era sancito l'obbligo di «vigilare affinché non siano usate credenziali di accesso consegnate ad altri utenti».
In entrambi i casi (sia per quanto riguarda le postazioni «fisse», sia per l'accesso mediante wi-fi) ai fornitori di connettività erano imposti obblighi a cui appariva difficile (se non impossibile) ottemperare. Se infatti era ipoteticamente possibile verificare di volta in volta l'identità di chi, già in possesso delle credenziali, avesse voluto accedere ai terminali situati in un determinato locale[123], risultava invece impossibile verificare che in un'area coperta dal segnale wi-fi potessero accedere alla Rete solo gli utenti effettivamente identificati e non anche altri che avessero ricevuto le credenziali d'accesso ottenendole (con o senza permesso: mediante semplice comunicazione o attraverso *packet sniffing*) dai primi, o che avessero bypassato l'ostacolo costituito dal *captive portal*.
A tale ultimo proposito va infatti sottolineata l'estrema vulnerabilità di un sistema che si basi unicamente su *captive portal* poiché sono diverse le tecniche che possono essere utilizzate per aggirarlo. La più semplice è senza dubbio quella che consiste nel porsi «in ascolto» del traffico sulla rete e forzare la propria scheda wireless ad utilizzare il MAC address di un utente che sia già stato abilitato alla navigazione (in questo caso ci sono due utenti che navigano contemporaneamente con uno stesso MAC address: l'utente «legittimo» non si accorge del suo «doppio» abusivo e se, per giunta, un illecito dovesse essere commesso, questo sarebbe attribuito al primo), ma tecniche più sofisticate prevedono ad esempio la possibilità di «nascondere» il contenuto reale dei pacchetti dentro pacchetti di altro tipo (ad esempio, una richiesta http potrebbe celarsi dentro un pacchetto DNS), appoggiandosi a server configurati all'uopo[124].
La robustezza di una rete che utilizza una chiave WPA (o, meglio, WPA2) appare nettamente superiore a quella di una rete con *captive portal* e, dunque, interpretato letteralmente l'obbligo di identificazione dell'utente *attraverso il terminale* cui faceva riferimento l'art. 4 avrebbe potuto anche vanificare l'obbligo di identificazione «fisica» precedente: mentre, infatti, gli utenti di una WLAN protetta con algoritmo WPA2 e con una password che offra una buona resistenza ad attacchi *brute force* possono ritenersi un cerchio più o meno ristretto di persone previamente identificate (salvo sempre il caso di comunicazione, volontaria o coartata, della chiave di rete ricevuta a soggetti terzi), in presenza del solo *captive portal* chiunque si trovi nel perimetro di copertura del segnale wi-fi può provare ad attaccare o ad aggirare il sistema con buone possibilità di riuscire ad accedere alla Rete in tempi ragionevoli e prescindendo da qualsiasi identificazione[125]. Il livello di sicurezza richiesto dalle norme in esame poteva, forse, essere raggiunto attraverso una combinazione di protezione dell'accesso alla rete wi-fi mediante

---

supporto HTTPS, che, in ipotesi, potrebbe rivelarsi fortemente discriminatorio escludendo a priori alcuni apparati, dall'altro ne pongono uno ben più preoccupante in termini di sicurezza, poiché le credenziali di autenticazione degli utenti sarebbero trasmesse in chiaro e sarebbero dunque maggiormente esposte ad attacchi (sniffing, ancora più grave se l'autenticazione avvenga mediante carta di credito).

123 Ma ciò appare in contrasto con quanto disposto dallo stesso comma terzo, secondo cui le operazioni di identificazione sono effettuate una sola volta, prima della consegna delle credenziali ad uso plurimo, perciò l'obbligo di vigilanza sembrerebbe basarsi meramente sulla memoria del gestore e sulla sua capacità di riconoscere *de visu* gli avventori.

124 Numerosi sono, in Rete, i siti dedicati all'argomento che forniscono istruzioni dettagliate sulla procedura da seguire.

125 Si consideri in questo contesto anche il fattore umano e quella particolare tecnica di *spoofing* nota come *Evil twin* che consiste nel riprodurre il captive portal di un hotspot al fine di sottrarre agli utenti le credenziali per la navigazione (e non solo). Cfr., a titolo esemplificativo, http://airsnarf.shmoo.com (15/02/2010).

WPA2 e, successivamente, di autenticazione attraverso *captive portal*, ferme restando sia tutte le precisazioni fatte finora, sia l'ovvia considerazione che a*d impossibilia nemo tenetur* e non appariva perciò ipotizzabile alcuna forma di responsabilità per il fornitore di connettività che pur adottando tutte le suddette misure avesse consentito, *de facto* e suo malgrado, l'accesso alla Rete a soggetti non identificati.

3.2. Misure di monitoraggio delle attività.

L'obbligo di monitoraggio delle attività compiute dall'utente è prescritto dall'art. 1, comma 1, lett. c del D.M. 16 agosto 2005, il quale rimanda per la descrizione delle misure da adottare al successivo art. 2. Deve anticiparsi da subito che anche questo obbligo, come i precedenti relativi all'identificazione fisica e «tecnologica» dell'utente, deve ritenersi superato a partire dal 1° gennaio 2011. Tuttavia, si ritiene utile darne conto sia per completare l'analisi in corso, sia per evidenziare le differenze, in parte già accennate *supra*[126], fra il tipo di monitoraggio richiesto dall'art. 7 del decreto Pisanu e quello relativo alla *data retention* imposto dalla Direttiva 2002/58/CE (e, successivamente, 2006/24/CE) relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e recepito nel nostro ordinamento con l'introduzione nel Codice in materia di protezione dei dati personali del Titolo X rubricato «Comunicazioni elettroniche» (in particolare, con l'art. 132, «Conservazione di dati di traffico per altre finalità»).
Diversi sono infatti sia l'ambito di applicazione soggettivo, sia la qualità e quantità dei dati di traffico raccolti e conservati, nonché la durata stessa degli obblighi di conservazione.
Come risulta da più provvedimenti e delibere del Garante per la protezione dei dati personali[127] devono ritenersi soggetti all'obbligo di conservazione dei dati ai sensi dell'art. 132 coloro «che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione (*cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (c.d. direttiva quadro) e D.Lgs. n. 259/2003 recante il Codice delle comunicazioni elettroniche*)»[128]. Sono invece espressamente esclusi dall'ambito di applicazione soggettiva:

- «i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche)»;
- «i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico»;
- «**i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale**»;
- «i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. "content provider")»;
- «i gestori di motori di ricerca».

L'interpretazione data dal Garante chiarisce inequivocabilmente che i soggetti individuati dal D.M. 16 agosto 2005 non sono sottoposti all'obbligo di conservazione dei dati *ex* art. 132 del Codice,

---

126 Cfr. *supra*, par. 3.
127 Cfr. Deliberazione *Misure e accorgimenti a garanzia degli interessati in tema di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati*, 19 settembre 2007, http://www.garanteprivacy.it/garante/doc.jsp?ID=1442463; Provvedimento *Sicurezza dei dati di traffico telefonico e telematico*, 17 gennaio 2008, http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111, modificato con Provvedimento *Recepimento normativo in tema di dati di traffico telefonico e telematico*, 24 luglio 2008, http://www.garanteprivacy.it/garante/doc.jsp?ID=1538224 (ID=1538237 per la versione consolidata riportata nell'Allegato A al provvedimento medesimo); Provvedimento *Conservazione dei dati di traffico: proroga dei termini*, 29 aprile 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1612508 (tutti gli URL verificati 09/03/2010).
128 Provvedimento *Recepimento normativo in tema di dati di traffico telefonico e telematico,* cit., par. 3.

conformemente sia alle indicazioni contenute nella relazione illustrativa della L. 155/2005 (riportate precedentemente[129]), sia, più in generale, al quadro normativo e regolamentare che sostanzialmente identifica i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione con gli ISP[130].

I **soggetti** individuati dal D.L. 144/2005 e dal D.M. 16 agosto 2005, di cui ci si è occupati più nello specifico al primo paragrafo, non erano pertanto interessati dalla normativa di dettaglio riguardante le categorie di dati da conservare contenuta nell'art. 3 D. Lgs. 109/2008, mentre dovevano applicarsi loro le sole disposizioni di cui all'art. 2 del D.M. 16 agosto 2005[131] sul monitoraggio dei dati di traffico, che, pur con i diversi problemi che saranno a breve evidenziati, apparivano meno «invasive» riguardo alla tipologia dei dati raccolti e sottoposti ad obbligo di conservazione rispetto alla *data retention* di cui al D. Lgs. 109/2008 (cfr. Tabella 2), probabilmente per la possibilità di «incrociare» in una eventuale fase di indagine i dati del monitoraggio con quelli mantenuti a cura dell'ISP.

L'art. 2 citato riguardava, per espresso richiamo dell'art. 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»: **risultavano perciò esclusi (fra i soggetti su cui comunque gravava un obbligo di identificazione degli utenti) sia i «fornitori di apparecchi terminali utilizzabili per le comunicazioni telematiche […] collocati in aree non vigilate»** di cui all'art. 3, **sia i «soggetti che offrono accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico»** di cui all'art. 4 (per i quali l'art. 1 è richiamato esclusivamente per ciò che concerne le modalità di identificazione degli utenti).

Quanto al **contenuto dell'obbligo di monitoraggio**, rivolto ai titolari e gestori delle attività di cui all'art. 1, esso consisteva nell'adozione di «misure necessarie a memorizzare e a mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili unicamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni» (art. 2, primo comma).

---

[129] Cfr. *supra*, par. 3.

[130] Cfr., oltre al Titolo X del Codice in materia di protezione dei dati personali, L. 8 aprile 2002, n. 59 , recante *Disciplina relativa alla fornitura di servizi di accesso ad Internet* (e relative norme di attuazione: Del. Aut. Gar. Com. 26 giugno 2002, n. 9/02/CIR, http://www2.agcom.it/provv/d_09_02_CIR.htm), D. Lgs. 1 agosto 2003, n. 259, *Codice delle comunicazioni elettroniche* (che, tra le varie definizioni, all' art. 1, lett. u, individua l'«operatore» come l'«impresa che è autorizzata a fornire una rete pubblica di comunicazioni, o una risorsa correlata»), nonché la definizione di «mercato dell'accesso ad Internet» effettuata mediante Del. Aut. Gar. Com. 10 luglio 2002, n. 219/02/CONS, http://www2.agcom.it/provv/d_219_02_CONS.htm, e, da ultimo, il D. Lgs. 30 maggio 2008, n. 109, recante *Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, che, nell'esplicitare le categorie di dati da conservare (art. 3), si riferisce agli «operatori di telefonia e di comunicazione elettronica», i quali difficilmente possono identificarsi con i «gestori» e gli altri soggetti individuati dal D.M. 16 agosto 2005: si veda sul punto la nota successiva (tutte le URL verificate il 09/03/2010).

[131] Ad ulteriore conferma di quanto si va sostenendo può richiamarsi anche il ragionamento a contrario per cui non avrebbe avuto alcun senso imporre ai gestori di esercizi pubblici o circoli privati di conservare dati relativi al «nome e indirizzo dell'abbonato o dell'utente registrato» e al «digital subscriber line number (DSL) o altro identificatore finale di chi è all'origine della comunicazione» (cfr. *infra*, Tabella 2). Infine, il D. Lgs. 109/2008, art. 4, secondo comma, impone ai «fornitori di servizi di cui al presente decreto» di inviare «annualmente al Ministero della giustizia, per il successivo inoltro alla Commissione europea, le informazioni relative: a) al numero complessivo dei casi in cui sono stati forniti i dati relativi al traffico telefonico o telematico alle autorità competenti conformemente alla legislazione nazionale applicabile; b) al periodo di tempo trascorso fra la data della memorizzazione dei dati di traffico e quella della richiesta da parte delle autorità competenti; c) ai casi in cui non è stato possibile soddisfare le richieste di accesso ai dati»: si tratta di un flusso informativo che evidentemente non è richiesto a tutti i fornitori di un accesso ad Internet ma solamente agli operatori di telefonia e ISP, come peraltro è confermato anche dal documento Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, 00068/10/EN, WP 172, adottato il 13 luglio 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf, e relativo *Annex*, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf (10/10/2010).

Ricordando ancora una volta che, contrariamente a quanto poi riscontrato nella pratica, queste disposizioni sembravano destinate ai soli gestori che mettevano a disposizione dei terminali per la navigazione, il problema del monitoraggio non era tanto l'associazione fra l'identità dell'utente ed il terminale utilizzato in un dato momento (fatta l'identificazione iniziale era semplice stabilire che ad una macchina a cui è stato assegnato un determinato IP si è connesso dalle ore x alle ore y l'utente Tizio), né tale associazione *in sé* appariva particolarmente invasiva in termini di protezione dei dati personali[132].
La questione giuridicamente più complessa, e che merita qui di essere ricordata, era relativa semmai al momento successivo riguardante le attività svolte dall'utente nell'arco temporale registrato.
Non fu mai fatta sufficiente chiarezza su cosa si intendesse per «tipologia del servizio utilizzato»: nelle intenzioni del legislatore poteva forse corrispondere a «protocollo di applicazione», attraverso il quale veniva fornito il servizio[133], ma a tale ipotesi non fu mai dato riscontro oggettivo né, nella prassi, fu ciò che intesero i gestori chiamati ad occuparsi della traduzione sul piano pratico della normativa.
Una seconda ipotesi poteva essere quella di far coincidere il concetto di «servizio» con quello di porta utilizzata, con la conseguenza che l'obbligo per il gestore avrebbe dovuto essere quello di tenere traccia di tutte le richieste ad IP esterni con i rispettivi numeri di porta[134]. L'importanza della definizione consisteva nell'individuare fino a che punto l'obbligo di monitoraggio riguardasse i dati «esteriori» della comunicazione e dove invece si rischiasse di oltrepassare la soglia che divide questi ultimi dal contenuto della comunicazione stessa. Molti programmi di monitoraggio del traffico comunemente utilizzati si basavano infatti sull'analisi dei pacchetti scambiati, ma anche solo l'*header* è in grado di rivelare molte più informazioni di quelle richieste dalla normativa in esame. Non solo: l'obbligo di monitoraggio del servizio, se interpretato in questi termini, si pone già di per sé in aperto contrasto con i dettami del Garante, per il quale «l'indirizzo IP di destinazione […] [è] dato potenzialmente correlato al contenuto della comunicazione»[135] di cui è vietata la conservazione.
La questione, mai risolta, si poneva sostanzialmente su cosa andasse considerato «comunicazione» vera e propria, e cosa invece *riguardasse* la comunicazione, senza costituire parte della stessa: al di là dell'espresso divieto di apprendere i contenuti delle comunicazioni fatto dall'art. 2 del D.M. 16 agosto 2005, è infatti la stessa Costituzione a garantire la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, che possono essere limitate soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge, sicché se il monitoraggio effettuato dai gestori fosse stato predisposto in modo da apprendere il contenuto del traffico telematico avrebbe potuto anche configurarsi un'ipotesi di reato (art. 617 quater c.p.[136]).

---

132 In sé: ci si riferisce alla semplice associazione nome utente-IP address effettuata dal gestore al momento della registrazione dell'utente, non alla successiva associazione IP address-attività svolta che presenta invece profili altamente problematici. Per quanto riguarda, poi, la fase successiva di «uscita» dell'IP sulla Rete si rimanda a quanto si dirà a breve sulla (tendenziale) unicità dell'IP in uscita dagli Internet Point e sulle «Misure intese al miglioramento della vita privata».

133 Ad esempio potrebbero ricordarsi, fra i più noti, HTTP, FTP, SMTP, POP, IMAP e RTP (spesso utilizzato per l'implementazione del VoIP), e, più in generale, tutti i protocolli compresi nel livello applicazione del modello ISO/OSI.

134 In questi termini, l'informazione potrebbe ritenersi composta da indirizzo IP di partenza e di destinazione, porta utilizzata (es.: 80 per HTTP, 25 per SMTP, ecc.) e protocollo (TCP o UDP).

135 Si veda ad esempio il provvedimento del Garante per la protezione dei dati personali del 19 novembre 2009, riportato in *Bollettino* n. 110, novembre 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1695368 (11/03/2010), nonché http://www.garanteprivacy.it/garante/doc.jsp?ID=1695393. Entrambi i provvedimenti hanno ad oggetto la *data retention*: nonostante la quantità e qualità delle informazioni conservate dagli ISP sia, come si è visto, ben più ampia, i contenuti delle comunicazioni sono fatti parimenti salvi e il Garante è perciò intervenuto in due occasione per vietare agli ISP di conservare nei propri file di log, rispettivamente, l'oggetto delle e-mail spedite dagli utenti e i singoli siti visitati ("dati di traffico afferenti l'indirizzo IP di destinazione"). Da ultimo, questa particolare «natura» dell'indirizzo IP è stata richiamata nel Report dei Garanti WP Art. 29 sulla *data retention*: «[…] the destination IP address can disclose the respective contents per se; as well as the social graph, they may also unveil information on the data subjects' most intimate preferences» (cfr. Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, 00068/10/EN, WP 172, 13 July 2010, p. 6, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp172_en.pdf, 20/07/2010).

136 Si tratta del reato di «Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche», che punisce «[c]hiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe».

Sul punto si richiama anche una recente pronuncia della Corte di Cassazione[137] che ribadisce come «l'obbligo della identificazione dell'utilizzatore del terminale Internet non pone alcun obbligo di conoscenza né tantomeno di controllo da parte del gestore, delle comunicazioni inviate», richiamando altresì il D.L. 144/2005 e il suddetto art. 2, che «nel prevedere l'obbligo […] di adottare le misure necessarie a memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio - abbinabili univocamente al terminale utilizzato dal cliente, esclude espressamente che possano essere memorizzati e mantenuti i contenuti della comunicazione. E ciò perché gli stessi non possono essere appresi dal gestore ex art. 617 quater c.p.». Proprio perché non può esservi controllo alcuno sul contenuto delle comunicazioni, il gestore non aveva (e non poteva avere) alcun obbligo ulteriore rispetto all'identificazione dell'utente: l'eventuale mancata identificazione non poteva perciò costituire violazione di un obbligo di sorveglianza idoneo a fondare una responsabilità penale di tipo omissivo (art. 40, comma 2, c.p.), poiché al gestore è «impedito di prendere contezza in alcun modo del contenuto della comunicazione inviata» (nel caso specifico portato dinanzi alla Cassazione, un'e-mail dal contenuto diffamatorio), «[c]osì che il reato ugualmente si sarebbe verificato anche se il gestore avesse annotato le generalità dell'utilizzatore del terminale per l'invio della posta elettronica. L'annotazione dei dati dell'utilizzatore, infatti, è richiesta ai fini della prova dell'utilizzazione e non al fine di impedire l'eventuale reato. E ciò a meno che il gestore non concorra nel reato ex art. 110 c.p., avendo piena conoscenza della delittuosità della comunicazione e avendone determinato l'inoltro. Il che nella specie non risulta dalla sentenza dei giudici di merito».
Non si ritiene di doversi soffermare ulteriormente su altri punti controversi della disciplina in esame che furono evidenziati nel periodo di vigenza quali criticità che impattavano più sulle libertà degli utenti che sull'effettiva esigenza di prevenire (o anche solo reprimere, per quanto qui maggiormente ci riguarda) la commissione di reati[138], mentre meritano comunque di essere menzionate quelle che il Gruppo dei Garanti Art. 29 definisce «Misure intese al miglioramento della vita privata»[139]: strumenti come remailer e anonymizer, sia per la navigazione che per lo scambio di messaggi di posta elettronica, che, utilizzati anche in combinazione tra loro, possono interrompere la «catena» che avrebbe dovuto permettere di identificare l'agente, sollevando, ancora una volta, non poche perplessità sull'efficacia delle misure qui analizzate.

Tabella 2 – Prospetto riassuntivo relativo agli obblighi di conservazione del traffico telematico.

	Data retention (art. 132 Codice Privacy, D. Lgs. 109/2008)	**Monitoraggio** (D.L. 144/2005, D.M. 16 agosto 2005)
Chi è soggetto all'obbligo?	Operatori di comunicazione elettronica → ISP	I titolari o gestori di esercizi pubblici o circoli privati di qualsiasi specie nei quali sono posti a disposizione del pubblico, dei clienti o dei soci, apparecchi terminali utilizzabili per le comunicazioni telematiche.
Quali dati?	*Per l'accesso internet:* - nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo internet (IP), un identificativo di utente o un numero	- Data della comunicazione, - ora della comunicazione, - tipologia del servizio utilizzato abbinabili unicamente al terminale

137 Cass., sez. V pen., 11 febbraio 2009, n. 6046.
138 Fra i vari, l'effettiva possibilità per gli inquirenti di risalire in modo certo all'identità di chi abbia, in ipotesi, compiuto atti criminosi utilizzando il terminale di un Internet Point, dal momento che il traffico in uscita si «affaccia» generalmente sulla Rete con uno stesso indirizzo IP e i dati di monitoraggio conservati dal gestore potrebbero non risultare sufficienti, o il fatto che il D.M. 16 agosto 2005, per espressa previsione dell'art. 5, lett. c), non si applichi «all'accesso alle reti telematiche attraverso apparati che utilizzano SIM/USIM attive sulla rete di telefonia mobile rilasciate ai sensi dell'art. 55 del decreto legislativo 1° agosto 2003, n. 259», quando le SIM possono ormai essere largamente utilizzate per fornire connettività anche mediante wi-fi.
139 Cfr. Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, Documento di lavoro *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line*, 21 novembre 2000, all'URL http://www.garanteprivacy.it/garante/document?ID=434621 (15/03/2010), p. 87 ss.

	telefonico; - data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato; - il servizio internet utilizzato; - numero telefonico chiamante per l'accesso commutato (dial-up access); - digital subscriber line number (DSL) o un altro identificatore finale di chi è all'origine della comunicazione. *Per la posta elettronica:* - indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente; - indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di host relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione; - indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione; - indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di host (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio; - indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato; - data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato; - il servizio internet utilizzato. *(estratto: ulteriori previsioni per la telefonia, invio di fax, sms e mms via Internet - V. art. 3 D.Lgs. 109/2008)*	utilizzato dall'utente. ESCLUSI: i contenuti delle comunicazioni. Inoltre, devono essere raccolti e conservati con «modalità informatiche» i dati relativi all'identificazione degli utenti: - dati anagrafici riportati su un documento d'identità; - tipo, - numero, - riproduzione del documento presentato.
Per **quanto** tempo?	12 mesi	Per il tempo indicato nel comma 1 dell'art. 7 D.L. 144/2005 (fino al 31/12/2010). I dati conservati da oltre 12 mesi possono però essere utilizzati esclusivamente per le finalità del medesimo D.L. (quindi solo «contrasto del terrorismo internazionale»?) 31 dicembre 2007 per i dati relativi all'identificazione: la lett. f dell'art. 1 DM 16 agosto 2005 non è stata modificata dalle varie proroghe.
Chi è **interessato** rispetto ai dati trattati?	Utente: «qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, senza esservi necessariamente abbonata»	Pubblico, clienti o soci di esercizi pubblici o circoli privati di qualsiasi specie nei quali sono posti a disposizione apparecchi terminali utilizzabili per le comunicazioni telematiche (utenti «occasionali»).

4. Modalità di conservazione dei dati.

Meritano, infine, di essere debitamente considerate anche le disposizioni che regolavano la raccolta e la conservazione dei dati degli utenti.

Il D.M. 16 agosto 2005 precisa infatti, all'art. 1, quarto comma, che «i dati acquisiti a norma del comma 1, lettere b) e c), sono raccolti e conservati **con modalità informatiche**», tranne nell'ipotesi prevista nello stesso comma di esercizi o circoli che mettono a disposizione del pubblico non più di tre apparecchi terminali, per i quali «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». La lett. e) del medesimo comma obbligava inoltre i gestori a «rendere disponibili, a richiesta, **anche per via telematica**, i dati acquisiti a norma delle lettere b) e c)».
Non appare utile, data anche la cessata vigenza delle disposizioni in esame, soffermarsi sul costo (in termini di manodopera, spazio dedicato allo storage, misure implementate a protezione dei dati personali e necessarie a mantenere l'inalterabilità, ecc.) che esse hanno comportato, mentre meritano un accenno le questioni di carattere interpretativo che vi sono sottese.
La lettera b) dell'art. 1, comma 1 citato prescriveva di «identificare chi accede ai servizi telefonici e telematici offerti […] acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente», mentre la lettera c) richiama il successivo art. 2, il quale, come già ricordato, al primo comma impone l'adozione di «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», e, al secondo comma, delle «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».
Non è chiaro, in primo luogo, quale fosse la **tipologia di riproduzione del documento** presentato dall'utente che il gestore era tenuto ad effettuare. Nella prassi la riproduzione dei documenti di identità, effettuata per i più svariati fini, avveniva mediante fotocopia, ma ciò sembrerebbe non rispondere agli obblighi imposti dall'art. 1 del decreto, poiché se pure dati anagrafici, tipo e numero del documento di identità fossero stati acquisiti mediante immissione dei dati stessi in un database, la fotocopia dei documenti non sarebbe stata compatibile con la prescritta conservazione con modalità informatiche ed eventuale messa a disposizione per via telematica. Il decreto sembrava dunque porre (nella pressoché totale inosservanza dei gestori) un ulteriore obbligo consistente nella acquisizione in formato digitale delle copie dei documenti di identità presentati dall'utente, che però veniva meno per gli esercizi e i circoli con meno di tre terminali messi a disposizione del pubblico che si fossero avvalsi del registro cartaceo di cui al quarto comma.
In secondo luogo, nessuna indicazione fu data in merito alle **modalità di conservazione** di detto materiale (in formato digitale o cartaceo), tranne per quanto previsto dalla lett. f), che intimava ai gestori di «assicurare il corretto trattamento dei dati acquisiti e la loro conservazione fino al 31 dicembre 2007», tale per cui sembrò potersi ritenere che i dati relativi all'identificazione, comunque acquisiti, dovessero semplicemente sottostare alla generale disciplina del Codice per la protezione dei dati personali, e, che dunque, al relativo trattamento avrebbero dovuto essere applicate disposizioni diverse a seconda dell'impiego o meno di strumenti elettronici.
Va poi rilevato che la lett. f) richiamata conteneva una **scadenza** (quella, appunto, del 31 dicembre 2007) che, non essendo stata ancorata al comma 1 dell'art. 7 del D.L. 144/2005 (e/o alla legge di conversione), non fu mai sottoposta alla proroga cui di anno in anno venne sottoposto il decreto Pisanu. Tale particolare merita di essere ricordato poiché costituisce una sorta di sintesi della scarsa attenzione posta dal legislatore per una disciplina introdotta frettolosamente, e poi prorogata in modo disattento e senza mai testare l'efficacia concreta di questo complesso di obblighi (per non parlare di un'analisi costi-benefici che, seppur annunciata all'epoca dell'introduzione del decreto, non fu mai realizzata). Dal momento che la scadenza di cui alla lett. f) è rimasta «cristallizzata» al 31 dicembre 2007, il gestore avrebbe potuto periodicamente provvedere alla cancellazione dei dati relativi all'identificazione degli utenti (estremizzando: anche subito dopo averli acquisiti) senza incorrere in alcuna sanzione e, al contempo, rendendo del tutto inutile la conservazione dei dati di monitoraggio di cui all'art. 2, dal momento che sarebbe stato spezzato il legame fra l'utente ed il traffico da questi prodotto.

Merita infine un accenno la questione, posta dall'art. 2 comma 2, relativa all'**inalterabilità** dei dati raccolti e conservati con modalità informatiche, che deve essere garantita dai soggetti di cui all'art. 1 «per il tempo indicato nel comma 1 dell'art. 7, del decreto legge 27 luglio 2005, n. 144» (dunque fino al 31 dicembre 2010). Non è mai stato chiarito né come titolari e gestori potessero garantire l'inalterabilità dei dati verso terzi anche relativamente alla *propria* attività, dal momento che avrebbero inevitabilmente ricoperto doppio ruolo di controllante e controllato, né *come* tale inalterabilità avrebbe dovuto essere garantita. Poteva ipotizzarsi (postulate, a monte, sia la perizia che la buona fede di tali gestori/amministratori) una masterizzazione periodica dei dati su supporti non riscrivibili (es.: dvd), magari con apposizione di firma digitale, ma tale operazione non avrebbe comunque risolto né il problema della successiva conservazione dei supporti, né quello, ben più consistente, della periodicità con cui procedere, poiché ovviamente finché i dati risiedono sulle macchine (terminali o server che siano) non possiedono caratteristiche di «inalterabilità». A tal proposito, nemmeno le indicazioni del Garante rivolte agli amministratori di sistema[140] aventi ad oggetto gli *access log* degli amministratori stessi[141], sembrano aver dato un contributo per la risoluzione del problema, e nemmeno le precisazioni successive[142] aventi ad oggetto proprio il requisito dell'inalterabilità, poiché esso, non solo per il fatto di essere relativo ad un flusso (dinamico) di dati, ma anche e soprattutto perché dipende da un soggetto che tecnicamente, e non può essere che così, è investito dei più ampi poteri di azione sugli stessi, è quanto mai evanescente e, si potrebbe dire, «circolare».
Minore, ma sempre ragionando *ex post*, appare invece la questione relativa al monitoraggio che doveva essere effettuato dai gestori che mettevano a disposizione **non più di tre terminali**, i quali potevano fruire dell'**eccezione prevista dal quarto comma** dell'art. 1 del D.M. 16 agosto 2005. In riferimento a questi ultimi soggetti il «monitoraggio del traffico» consisteva esclusivamente nell'annotazione sugli appositi registri dell'«identificativo della apparecchiatura assegnata all'utente» e dell'«orario di inizio e fine della fruizione dell'apparato». La parziale sovrapponibilità fra quarto comma dell'art. 1 e primo comma dell'art. 2 (che, si ricorda, prescriveva ai soggetti di cui all'art. 1 di «memorizzare e mantenere i dati relativi alla data ed ora della comunicazione ed alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente») induceva a ritenere che le misure di cui al quarto comma predetto rappresentassero un «sottoinsieme» di quelle previste all'art. 2 come regime generale, e tale interpretazione appariva suffragata dalla struttura del quarto comma (che richiama dapprima il primo comma, lett. c – e, quindi, l'art. 2 – , per poi escluderne l'applicazione per gli esercizi e i circoli aventi non più di tre terminali). Da ciò poteva derivarsi, nei confronti di questi gestori, la completa esenzione dall'obbligo di monitoraggio per quanto riguarda la «tipologia del servizio utilizzato», il che poteva indurre l'interprete, alternativamente o congiuntamente, ad individuare un elemento a suffragio dell'ipotesi formulata *supra* (par. 3.2) circa la portata «limitata» (almeno nelle intenzioni del legislatore) del termine «servizio», o ad interrogarsi ancora una volta sulla reale efficacia dell'obbligo di monitoraggio rispetto alle finalità che la normativa in esame avrebbe dovuto perseguire.

5. La situazione dopo il 31 dicembre 2010.

[140] Si noti che la definizione di amministratore di sistema data dal Garante non coincide con quella di amministratore che è stata utilizzata con riferimento all'attività dei titolari e gestori degli esercizi che sono qui presi in considerazione.
[141] Che devono possedere «caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste»: cfr. Provvedimento *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*, 27 novembre 2008, http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499 (23/03/2010).
[142] Secondo il Garante il requisito dell'inalterabilità «può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i log server centralizzati e "certificati"». Cfr. *Risposte alle domande più frequenti (FAQ)*, richiamate dal Provvedimento *Amministratori di sistema: avvio di una consultazione pubblica*, 21 aprile 2009, http://www.garanteprivacy.it/garante/doc.jsp?ID=1611986 (le FAQ sono attualmente consultabili in calce al Provvedimento *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici*, cit.: si vedano in particolare i nn. 12 e 13).

Il D.L. 29 dicembre 2010, n. 225, citato all'inizio di questo capitolo, ha abrogato[143] il quarto e quinto comma dell'art. 7 D.L. 144/2005, e modificato il primo. Si tratta di una modifica sostanziale intervenuta, dopo il lungo dibattito sull'accesso ad Internet e sul wi-fi (in particolare) in Italia, quasi a sorpresa: solo poco tempo prima infatti il Ministro per i rapporti con il Parlamento, rispondendo ad un'interrogazione in merito alla proroga dell'art. 7 del decreto legge n. 144 del 2005 in materia di accesso senza fili alla rete Internet, aveva dichiarato che «l'articolo 7 del decreto-legge n. 144 del 2005 fa parte di un gruppo di disposizioni volte a controllare attività sensibili, in particolare gli Internet *point* e gli altri esercizi nei quali sono offerti servizi di comunicazione anche telematica, in relazione a possibili minacce terroristiche. Questa disposizione risponde quindi a esigenze di sicurezza dello Stato. Va evidenziato che l'applicazione della normativa, di straordinaria importanza, ha consentito attività investigative di assoluto rilievo per il contrasto del terrorismo sia nazionale che internazionale, nonché per il contrasto del grave fenomeno della pedopornografia *on line*»[144].
Deve qui notarsi, incidentalmente, che «il grave fenomeno della pedopornografia» nulla ha a che fare, né in origine, né in seguito, con le esigenze urgenti di contrasto al terrorismo per cui il D.L. 144/2005 fu adottato, e che nonostante l'annuale proroga della scadenza di cui al primo comma dell'art. 7, i dati di monitoraggio conservati per oltre 12 mesi possono essere utilizzati, *ex* art. 2, comma 2, D.M. 16 agosto 2005, «esclusivamente per le finalità del predetto decreto-legge» (ossia «contrasto del terrorismo internazionale»). Quanto precisato dal Ministro appare perciò particolarmente preoccupante, poiché, alternativamente, o i dati di monitoraggio erano normalmente utilizzati dagli inquirenti ben oltre i limiti (temporali e di scopo) imposti dalla legge (che, certo, è una legge poco chiara, ma sembra che almeno su questo punto non lasci adito a dubbi), o ci troviamo di fronte all'ennesima prova del fatto che i sostenitori del decreto Pisanu non hanno mai effettuato una valutazione né preventiva, né consuntiva, dei suoi effetti e non ne conoscono completamente nemmeno i confini applicativi, o, cosa ancor più grave, li estendono artatamente in ottica propagandistica.
L'interrogazione e l'immediata risposta del Ministro coincidono approssimativamente con la presentazione alla Camera della prima proposta di legge volta ad abrogare l'art. 7[145], che riassume nella relazione illustrativa molte delle questioni affrontate nel corso di questa analisi. È chiaramente evidenziato che «a causa dell'articolo 7 del "decreto Pisanu", ad esempio, in Italia nessuna biblioteca, azienda privata o pubblica può dare libero accesso alla propria rete wi-fi se prima non ha fotocopiato o scansionato il documento di identità dell'utilizzatore, si è attrezzata per controllare gli accessi alle singole postazioni e i software, utilizzati dagli utenti; con la conseguenza di negare, di fatto, la possibilità di utilizzo libero della rete wi-fi», e viene chiaramente sottolineato «[…] come l'acquisizione di dati personali e il divieto di fornire accesso libero alla rete appaiano misure del tutto inefficienti. Queste norme, in effetti, non appaiono in alcun modo idonee a impedire l'attuazione di un illecito, poiché facilmente aggirabili anche da parte di soggetti con conoscenza informatica piuttosto limitata. A fronte di risultati quasi inesistenti in termini di sicurezza, i costi di tali norme sono invece altissimi. Esse hanno costituito un ostacolo alla crescita tecnologica e culturale di un Paese già in ritardo su tutti gli indici internazionali della connettività internet […]».
A questa prima proposta fece seguito il disegno di legge n. 2494, di iniziativa di un gruppo di Ministri, recante «Nuove disposizioni in materia di sicurezza pubblica», comunicato alla Presidenza del Consiglio il 13 dicembre 2010[146]. Anche questo D.d.L. si poneva come obiettivo, con il suo art. 3, di abrogare

---

143 Art. 2, comma 19, del D.L. 225/2010 (c.d. Decreto Milleproroghe): «All'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, sono apportate le seguenti modificazioni:
a) al comma 1, le parole: "fino al 31 dicembre 2010, chiunque" sono sostituite dalle seguenti: "fino al 31 dicembre 2011, chiunque, quale attività principale,";
b) i commi 4 e 5 sono abrogati. »

144 Cfr. Interrogazione dell'on. Rao all'on. Vito, del 13 ottobre 2010, consultabile all'URL http://www.governo.it/backoffice/allegati/60302-6311.doc (01/03/2011).

145 Cfr. Proposta di legge n. 3736, d'iniziativa dei deputati Lanzillotta, Gentiloni Silveri e Barbareschi, presentata il 29 settembre 2010 e volta alla «Abrogazione dell'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, concernente limiti all'esercizio e all'uso delle postazioni pubbliche per comunicazioni telematiche e dei punti di accesso ad internet mediante tecnologia senza fili», http://www.lindalanzillotta.it/docs/PROPOSTA%20LEGGE%20WI-FI.pdf (01/03/2011).

146 Il testo del D.d.L. è reperibile all'URL http://www.senato.it/service/PDF/PDFServer/BGT/00514970.pdf

integralmente l'art. 7 del D.L. 144/2005, e anch'esso, come la precedente proposta, non riuscì nell'intento, apportando però qualche ulteriore elemento di riflessione nelle sedi istituzionali che per lungo tempo non avevano voluto occuparsi delle restrizioni all'accesso alla Rete e che, improvvisamente, sembravano invece aver colto i segnali dell'esistenza di un problema. Si legge nella Relazione illustrativa che «[g]li appesantimenti burocratici dovuti a fotocopiature e archiviazioni dei documenti degli utenti sono stati indicati come fattori fortemente penalizzanti per lo sviluppo delle nuove tecnologie e degli strumenti del web. È stato, inoltre, evidenziato che in nessun paese occidentale è prevista una normativa tanto rigorosa sull'accesso alle reti Internet, e soprattutto al Wi.Fi. In questi anni c'è stata una straordinaria evoluzione tecnologica che può consentire soluzioni diverse dalle restrizioni del citato "decreto Pisanu" che permettono, comunque, l'attività investigativa».
Il D.L. 29 dicembre 2010, n. 225 giunge, infine, in seguito a quest'ultimo tentativo, senza abrogare completamente l'art. 7, ma rivisitandolo in modo sostanziale.
La nuova formulazione del primo comma prevede che «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».
L'elemento di novità rispetto a quanto descritto al par. 2 (cui si rimanda per tutte le rimanenti definizioni riguardanti l'ambito soggettivo e oggettivo di applicazione) consiste nell'inciso «**quale attività principale**», che ha (o dovrebbe avere) l'**effetto di restringere notevolmente il numero dei soggetti a cui è imposta la richiesta di licenza preventiva**.
Mentre, infatti, con la precedente formulazione la licenza era necessaria per chiunque rientrasse nella definizione di «pubblico esercizio» o «circolo privato» (requisito soggettivo), qualora mettesse a disposizione degli «apparecchi terminali utilizzabili per le comunicazioni anche telematiche» (requisito oggettivo), con la nuova formulazione la licenza diviene necessaria, per gli stessi soggetti, qualora esercitino l'attività in via «principale». Può essere precisato, per completezza, che nonostante non sussistano dubbi sulle intenzioni dei promotori delle modifiche apportate all'art. 7, che inequivocabilmente rivolgono gli obblighi di licenza residui ai soli Internet Point, così formulata la norma lascerebbe in realtà spazio a due diverse interpretazioni, ossia:

a) quella conforme alle suddette intenzioni, per cui l'obbligo di licenza sussisterebbe attualmente solo per chi possiede o intende aprire un pubblico esercizio o circolo privato nel quale l'attività principale sia quella di mettere a disposizione apparecchi terminali utilizzabili per le comunicazioni telematiche (Internet Point);
b) quella per cui l'obbligo di licenza sussisterebbe, sempre qualora siano messi a disposizione i suddetti terminali, per chiunque intenda aprire un pubblico esercizio o un circolo privato e ne faccia la propria attività principale. In questa seconda ipotesi, che pone l'accento sul fatto che l'attività da svolgere sia quella esercitata in via principale dal soggetto, e non che l'attività principale sia quella di mettere a disposizione del pubblico gli apparecchi terminali, poco cambierebbe rispetto alla formulazione precedente, dal momento che normalmente i titolari degli esercizi e dei circoli di cui si parla esercitano in via principale tale attività e rimarrebbero esclusi solamente alcuni casi marginali: si pensi ad esempio al gestore di un circolo che tuttavia svolga un'altra attività da ritenersi «principale», quale ad esempio il libero professionista. Si tratta comunque di una mera ipotesi che non trova alcun riscontro né nella supposta *ratio* della norma, né, per quanto è dato di sapere, nell'intenzione del legislatore, e si ritiene debba perciò privilegiarsi la più logica ipotesi *sub* a).

La prima conseguenza derivante dalla modifica in esame è perciò che, pur continuando a sussistere un obbligo di licenza preventiva prorogato fino al 31 dicembre 2011 per i soggetti *sub* a), ne sono sollevati tutti i soggetti per così dire «ibridi», che possedevano sia i requisiti soggettivi che quelli oggettivi di applicabilità della previgente normativa ma la cui attività rimane estranea alla pura e semplice fornitura del servizio di accesso alla Rete[147].

(01/03/2011).

[147] Deve aggiungersi, per maggiore chiarezza e per completezza rispetto a quanto già riportato *supra* al par. 3.2 e in nota n.

La seconda importantissima modifica apportata dal D.L. 225/2010 consiste, come anticipato, nell'abrogazione del quarto e quinto comma dell'art. 7 D.L. 144/2005. Conseguentemente, **sono abrogati tutti gli obblighi che nel corso della presente disamina sono stati indicati come «di identificazione» e «di monitoraggio»**.
Ciò significa, per tutti i soggetti (sia quelli per cui permane l'obbligo di licenza, che per tutti gli altri per cui era richiesto anche il «solo» obbligo di identificazione), la possibilità di fornire l'accesso alla Rete senza ulteriori formalità. Con l'abrogazione del quarto e quinto comma dell'art. 7 deve infatti ritenersi abrogato anche il D.M. 16 agosto 2005, pur non essendo rinvenibile una espressa disposizione in questo senso. Essendo, infatti, tale D.M. emanato sulla base delle previsioni del quarto comma (e recando, già nell'intestazione, *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'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155*) può ritenersi operata un'abrogazione implicita[148], dal momento che con l'abrogazione del quarto comma dell'art. 7 il legislatore ha inteso rivedere complessivamente la materia, e sono dunque da ritenersi abrogate tutte le norme incompatibili con la nuova disciplina.

6. Sanzioni.

L'aspetto sanzionatorio appare, in relazione alle norme qui richiamate, notevolmente confuso, e ciò è mutato solo in parte con l'introduzione del D.L. 225/2010. Quanto si dirà vale dunque a completamento sia dell'analisi relativa all'assetto normativo previgente, sia a quello attuale, per gli obblighi (di licenza) che ancora residuano.
I primi tre commi dell'art. 7 del D.L. 144/2005 disciplinano, come si è visto a più riprese, le modalità di richiesta e di rilascio della licenza per le categorie di soggetti che sono obbligate a richiederla, concludendo, al comma terzo, con richiami alquanto vaghi alle disposizioni previste dal TULPS ai capi III e IV del titolo I, e al capo II del titolo III.
Tali capi si occupano rispettivamente:

a) «delle autorizzazioni di polizia», in cui si rinvengono le condizioni (oggettive e soggettive) a cui è subordinato il rilascio della licenza e l'eventuale revoca, la durata della stessa, ecc.;
b) «dell'inosservanza degli ordini dell'autorità di Pubblica Sicurezza e delle contravvenzioni»;
c) «degli esercizi pubblici», di cui ci si è già occupati al par. 2.1. *supra*.

24, che tali soggetti sono esclusi anche (e ciò a prescindere dall'entrata in vigore e successiva abrogazione delle norme del «decreto Pisanu» finora analizzate) dall'obbligo di richiedere l'autorizzazione generale richiesta dal Codice delle comunicazioni elettroniche (D.Lgs. 259/2003) in virtù di una delibera AGCOM di poco precedente all'entrata in vigore del Codice stesso ma da questo non abrogata e che risulta in ogni caso coerente con il corpo delle disposizioni che vi sono contenute. La delibera 102/03/CONS, reperibile all'URL http://www.agcom.it/default.aspx?DocID=334 (20/07/2010), chiarisce che (art. 1, comma 2) «[n]on si considera fornitore di un servizio pubblico di telecomunicazioni […] quell'esercente l'attività commerciale, quale ad esempio gestore di bar, albergo, pizzeria, tabaccheria, che, non avendo come oggetto sociale principale l'attività di telecomunicazioni, mette a disposizione della propria clientela le apparecchiature terminali di rete». Allo stesso modo, deve considerarsi non applicabile a tali soggetti il D.M. 28 maggio 2003 (e ss. mm. ii.), recante *Regolamentazione dei servizi Wi-fi ad uso pubblico*, rilevante ai fini della presente ricerca poiché porrebbe ulteriori obblighi di identificazione dell'utente a carico del fornitore di connettività wi-fi. L'oggetto e l'ambito di applicazione di tale decreto, così come delineati dall'art. 2, sono infatti quelli di fissare «le condizioni per il conseguimento dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN nella banda 2,4 GHz o nelle bande 5 GHz, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni», e deve pertanto considerarsi rivolto solamente ai soggetti obbligati ad ottenere dette autorizzazioni generali.

148 Come è noto, in riferimento alla disciplina dell'abrogazione delle leggi di cui all'art. 15 delle disp. prel. c.c., la dottrina suole distinguere tra abrogazione *espressa* («per dichiarazione espressa del legislatore»), *tacita* («per incompatibilità tra le nuove disposizioni e le precedenti») e *implicita* («perché la nuova legge regola l'intera materia già regolata dalla legge anteriore»). L'abrogazione implicita, ancor più di quella tacita, è causa di notevoli incertezze interpretative, poiché dipende da una interpretazione delle disposizioni o dei complessi di disposizioni che si succedono nel tempo: si veda per tutti G. ZAGREBELSKY, *Manuale di diritto costituzionale*, *I. Il sistema delle fonti del diritto*, Torino, Utet, 1987, p. 41 ss.

Analizzando, *sub* b), le disposizioni contenute nel predetto capo IV del titolo I (artt. da 15 a 17-*sexies*) ci si accorge che il solo art. 16[149], relativo ai controlli, è applicabile anche alle fattispecie che sono qui esaminate (nel previgente assetto ciò risultava comunque superfluo in quanto superato dal disposto del quinto comma dell'art. 7 del D.L. 144/2005), mentre tutte le rimanenti disposizioni a carattere sanzionatorio colpiscono violazioni delle disposizioni del TULPS, fra le quali non è previsto l'obbligo di ottenere la specifica licenza di cui all'art. 7, comma 1, del D.L. 144/2005.
Né, data l'indicazione estremamente puntuale delle singole sanzioni (tutte, per inciso, di carattere amministrativo) è possibile procedere con un'interpretazione estensiva delle fattispecie richiamate, o, peggio, interpretarle analogicamente, vigendo in materia amministrativa lo stesso divieto di applicazione analogica *in malam partem* previsto per la legge penale.
Le questioni qui sollevate non devono essere sfuggite in fase di redazione della Circolare del 29 agosto 2005 del Dipartimento della pubblica sicurezza, che in relazione all'art. 7 specificava «per completezza» che «l'esercizio delle attività qui in argomento in assenza di licenza, o in violazione degli obblighi ad esse inerenti, rientra fra le fattispecie previste e punite dall'art. 17 del Testo Unico delle leggi di P.S., appositamente richiamato, fra le disposizioni del Capo IV del Titolo I dello stesso T.U., dal comma 3 dell'art. 7».
L'applicazione dell'art. 17 alla fattispecie *de qua* appare tuttavia estremamente dubbia[150]. Se è vero infatti che tale articolo rappresenta una sorta di clausola generale di applicazione residuale, che assume rilevanza quando non sia «stabilita una pena od una sanzione amministrativa ovvero non provvede il codice penale», è anche vero che le violazioni cui fa riferimento sono solo quelle «alle disposizioni di questo testo unico», e né il TULPS né il D.L. 144/2005 operano un richiamo esplicito o comunque sufficientemente chiaro e univoco alla sanzione da comminarsi in caso di violazione dell'obbligo previsto dall'art. 7.
Se tuttavia si ritenesse di dover applicare comunque l'art. 17 del TULPS, andrebbe ribadito come anche in relazione alla sanzione le norme che riguardano l'obbligo di licenza debbano tenersi distinte da quelle che regolavano gli obblighi di identificazione e monitoraggio delle attività degli utenti: per queste ultime infatti nemmeno la circolare citata (che in ogni caso non avrebbe potuto essere considerata sufficiente a dettare alcunché a riguardo) forniva alcuna indicazione di carattere sanzionatorio.
Dal punto di vista sanzionatario ci si trova dunque, nel complesso, a far fronte alle stesse difficoltà ermeneutiche preesistenti alle modifiche introdotte dal D.L. 225/2010, derivanti dalla violazione di un obbligo a cui può essere correlata una sanzione solo attraverso un'interpretazione piuttosto complessa (e, comunque, giuridicamente opinabile) delle norme vigenti, e va comunque dato atto della soppressione di due obblighi rimasti per lungo tempo del tutto sprovvisti di sanzione.

[149] Si riporta per comodità il testo dell'art. 16: «Gli ufficiali e gli agenti di pubblica sicurezza hanno facoltà di accedere in qualunque ora nei locali destinati allo esercizio di attività soggette ad autorizzazioni di polizia e di assicurarsi dell'adempimento delle prescrizioni imposte dalla legge, dai regolamenti o dall'autorità.»
[150] Si riporta per comodità il testo dell'art. 17: «(1) Salvo quanto previsto dall'art. 17-bis, le violazioni alle disposizioni di questo testo unico, per le quali non è stabilita una pena od una sanzione amministrativa ovvero non provvede il codice penale, sono punite con l'arresto fino a tre mesi o con l'ammenda fino a € 206,00. (2) Con le stesse pene sono punite, salvo quanto previsto dall'art. 17-bis, le contravvenzioni alle ordinanze emesse, in conformità alle leggi, dai prefetti, questori, ufficiali distaccati di pubblica sicurezza o sindaci.»

CAPITOLO TERZO

Identificazione e responsabilità in altri Paesi: case-studies scelti

SOMMARIO: 1. La situazione all'estero. Chiavi di lettura. – 2. Francia. – 2.1. La c.d. «HADOPI 1» (L. 669/2009) e i rilievi del Consiglio Costituzionale. – 2.2. Il progetto «HADOPI 2» e qualche considerazione a margine. – 3. UK: il Digital Economy Act. – 4. Germania: connessioni wi-fi e responsabilità per non aver cambiato la password del router. – 5. Olanda: tutti operatori? – 6. Alcuni altri Paesi europei e OCSE. – 7. Esempi scelti dai Paesi non-OCSE.

1. La situazione all'estero. Chiavi di lettura.

Il «caso» italiano appare, agli occhi di chi si occupa di accesso alla Rete e delle potenzialità che vi sono connesse, come una situazione del tutto peculiare: dall'interno, perché troppo numerosi – e sostanzialmente privi di reali benefici (secondo quanto si è detto finora e, soprattutto, se paragonati con altri tipi di attività, commerciali e non) – erano gli adempimenti di carattere burocratico, le misure di carattere organizzativo e di sicurezza e gli investimenti richiesti per poter offrire connettività (con e senza fili), e dall'esterno, perché sempre più frequentemente, soprattutto nell'ultimo periodo di vigenza del decreto Pisanu, accadeva di confrontarsi con cittadini di altri Paesi che faticano a comprendere il complesso quadro normativo e regolamentare che impediva loro di accedere alla Rete da un caffè o da un parco pubblico, o condizionava tale accesso a procedure che non avevano alcun corrispettivo nel Paese di provenienza.
L'impressione di trovarsi di fronte ad un «caso» è ciò che spinge ad interrogarsi dapprima – ed è ciò che ha costituito oggetto di analisi in particolare del capitolo precedente – sulla concreta utilità ed efficacia di una tale «sovrastruttura» normativa e, successivamente, sull'esistenza di situazioni simili in altre realtà.
L'analisi comparatistica, di cui può darsi conto solo in parte in questa sede[151], ha rivelato che se da un lato la situazione italiana è stata sicuramente un *unicum* nel panorama internazionale, dall'altro vi sono realtà in cui restrizioni anche piuttosto gravi delle libertà individuali sono attuate senza nemmeno fare appello a quei reati «universalmente considerati gravi» e che «scuotono le coscienze» di cui si faceva menzione nei capitoli precedenti. Talvolta fra questi «gravi reati» è infatti inclusa la violazione del diritto d'autore: è il caso di UK e Francia, ma è vero che, non appena ci si sposti leggermente dall'oggetto della presente indagine, anche gli ISP italiani non hanno mancato di denunciare, con particolare riferimento alla vicenda *The Pirate Bay* e, più in generale, al frequente sequestro mediante «oscuramento» di siti Internet localizzati all'estero, un utilizzo del mezzo cautelare che appare improprio, giudicando «inaccettabile e contrario alla normativa comunitaria e italiana che gli operatori di accesso italiani siano

[151] Per ovvie motivazioni di economia del lavoro nel suo complesso: sono perciò stati esaminati solo i casi ritenuti più significativi, o perché ripresi dalla stampa, o perché la situazione in qualche modo ricordava quella italiana, o perché sono stati ritenuti comunque interessanti ad altro titolo o sotto altri profili.

destinatari di provvedimenti relativi a fatti che non li riguardano» e sottolineando come «le norme sul "sequestro" non possono essere utilizzate per attuare quello che in realtà è un "filtraggio" sia in termini tecnici, sia – soprattutto – in termini di impatto sui diritti di cittadini e imprese»[152].
Confrontando l'Italia con altri Paesi si rafforza pertanto la convinzione, già formatasi, di trovarsi a vivere *all'interno di un case study* piuttosto interessante. Uno studio dell'EDRi (*European Digital Rights*) volto ad evidenziare le conseguenze negative del filtraggio e del *web blocking* che Parlamento e Consiglio intendevano introdurre per combattere la pedopornografia online[153], si conclude proprio con l'esempio italiano, e cita non solo il decreto Pisanu, ma numerosi altri provvedimenti (alcuni menzionati anche nel presente lavoro) in qualche modo connessi con la censura online. L'autore di quello studio si schierava apertamente contro il filtraggio (questione affrontata nell'*Introduzione* per la stretta ed evidente connessione con la libertà di espressione), poiché, dichiarava successivamente, «Countries that introduce Web-blocking to target child abuse today, will block to protect gambling monopolies tomorrow and politically unwelcome websites the day after tomorrow»[154], aggiungendo che questo era esattamente ciò che stava avvenendo in Francia.
Proprio dalla Francia, perciò, inizierà l'ultima parte di questo studio.

2. Francia

2.1. La c.d. «HADOPI 1» (L. 669/2009) e i rilievi del Consiglio Costituzionale.

Il 12 giugno 2009, nel contesto legislativo e politico-sociale che si è tentato di delineare nel corso dell'*Introduzione*, veniva promulgata in Francia la L. 669/2009[155] che, in una prima formulazione, prevedeva l'istituzione di un organismo, l'HADOPI («Haute Autorité pour la diffusion des oeuvres et la protection des droits sur internet»), con il compito di controllare i contenuti scambiati in Rete su segnalazione dei titolari dei diritti d'autore e connessi, e di «ammonire» gli utenti che fossero stati scoperti a violare tali diritti. La stessa HADOPI era investita poi, in seguito al terzo richiamo, del potere di escludere gli utenti dall'accesso alla Rete, bloccandoli direttamente a livello di ISP, sulla base dei meri indizi raccolti e al di fuori di qualsiasi giudizio che potesse garantirne i diritti, ponendosi in aperto contrasto con la Raccomandazione del Consiglio d'Europa del 26 marzo 2008 in tema di filtri[156], e obbligando i *provider* dapprima a rivelare i nominativi corrispondenti agli IP raccolti e poi a bloccare le utenze.
Nel periodo in cui l'Assemblea Nazionale ed il Senato francese discutono la L. 669/2009 il Parlamento Europeo affronta il tema della libertà di espressione in tutte le sue forme e manifestazioni, oltre a quello del diritto al rispetto della vita privata e dei dati personali[157], con la Raccomandazione del 26 marzo

---

152 Cfr. Comunicato AIIP – Associazione Italiana Internet Provider, *TLC, gli operatori AIIP ricorrono contro le modalità di sequestro dei siti all'estero*, 24 ottobre 2008, http://www.aiip.it/page.php?id=805&aiip=7a088c50a679e4ff55253c29e06b78aa (23/9/2009). Cfr. anche, in seguito a Cass., sez. III pen., 30 settembre 2009, n. 49437, *AIIP, Il sequestro non si fa con i filtri*, 29 dicembre 2009, http://www.aiip.it/page.php?id=926&aiip=913828c4488c328d7a7590fc4bd245ab (18/1/2010).

153 Cfr. J. MCNAMEE, *Internet Blocking. Crimes should be punished and not hidden*, EDRi, 2010, http://www.edri.org/files/blocking_booklet.pdf (01/03/2011).

154 Dichiarazione di J. McNamee riportata in J. BAKER, *European Parliament considers Web blocking*, in *IDG News*, 10 gennaio 2011, http://www.pcworld.com/businesscenter/article/216370/european_parliament_considers_web_blocking.html (16/01/2011). Cfr. a questo proposito *Introduzione*, p. 7, circa la necessità di non considerare come assoluti taluni concetti onde evitare pericolose derive censorie.

155 Loi n. 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, http://www.legifrance.gouv.fr/ affichTexte.do?cidTexte=JORFTEXT000020735432 (29/9/2009).

156 Cfr. *supra*, Introduzione, nota n. 13.

157 Dopo aver affrontato in vari punti sia la libertà di espressione che il diritto alla protezione dei dati personali, il Considerando O della Raccomandazione del 26 marzo 2009 offre una panoramica di quelli che il Parlamento considera i «diritti fondamentali coinvolti nel mondo di Internet», i quali «comprendono, ma non in via esclusiva, il rispetto per la vita privata (compreso il diritto di cancellare in modo permanente la propria impronta digitale), la protezione dei dati, la libertà di espressione, di parola e di associazione, la libertà di stampa, di espressione politica e di partecipazione, il divieto di discriminazione e l'educazione; considerando che il contenuto di questi diritti, compreso il loro ambito e campo di applicazione, il livello di protezione che forniscono, nonché il divieto di violazione degli stessi, dovrebbe essere disciplinato

2009 destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet[158]. In quel testo si richiede fermamente che una soluzione alla cibercriminalità sia ricercata rispettando il delicato equilibrio fra la tutela dell'individuo e l'esigenza di prevenzione e repressione dei reati, ricordando che «la mera esistenza di tecnologie di sorveglianza non giustifica automaticamente il loro uso, bensì l'interesse preponderante della protezione dei diritti fondamentali dei cittadini dovrebbe determinare i limiti e precisare le condizioni in base alle quali tali tecnologie possono essere utilizzate dai poteri pubblici o da società» (Considerando J), e che «trattandosi di diritti come la libertà di espressione o il rispetto della vita privata, limitazioni all'esercizio di tali diritti possono essere imposte dalle autorità pubbliche solo se conformi alla legge, necessarie, proporzionate e appropriate in una società democratica» (Considerando L).
Alcuni punti della Raccomandazione prendono espressamente in considerazione i diritti di proprietà intellettuale, sottolineando l'esigenza di proteggerli «per quanto sia necessario, proporzionato e adeguato» (Considerando T). In particolare, poi, nell'unico punto delle «raccomandazioni» vere e proprie che si occupa di proprietà intellettuale (lett. l), viene ribadito come la decisione di adottare sanzioni penali debba seguire ad una valutazione di necessità e proporzionalità alla luce delle attuali ricerche sull'innovazione, e debbano nel contempo ritenersi vietati «il controllo e la sorveglianza sistematici di tutte le attività degli utilizzatori su Internet», mentre dovrà garantirsi «che le sanzioni siano proporzionate alle infrazioni commesse», si dovrà rispettare «la libertà di espressione e di associazione dei singoli utilizzatori e combattere l'incitamento alla ciber-violazione dei diritti di proprietà intellettuale, comprese talune eccessive restrizioni di accesso instaurate dagli stessi titolari di diritti di proprietà intellettuale».
I contenuti della Raccomandazione (nonché degli emendamenti del Parlamento Europeo al c.d. «Pacchetto Telecom», che poco tempo dopo ribadiscono come la compressione delle libertà fondamentali non possa avvenire che successivamente ad una pronuncia dell'autorità giudiziaria) sono confermati dalla sentenza n. 2009-580 DC del 10 giugno 2009[159] del Consiglio Costituzionale francese, che censura la prima formulazione della c.d. *Loi Création et Internet* (ora conosciuta anche come *HADOPI 1*), sottolineando come ai sensi dell'art. 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789 «La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme: tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi» e come, considerato lo stato attuale dei mezzi di comunicazione e lo sviluppo dei servizi di comunicazione online, nonché l'importanza di questi ultimi per la partecipazione alla vita democratica e l'espressione di idee ed opinioni, tale diritto implichi la libertà di accedere a detti servizi (par. n. 12).
Di fronte al diritto fondamentale riconosciuto dall'art. 11, il legislatore non è libero, sempre secondo il Consiglio Costituzionale, di conferire poteri sanzionatori come quelli previsti dalla L. 669/2009 ad una autorità amministrativa al fine di proteggere i titolari dei diritti d'autore e connessi, indipendentemente dalle garanzie che accompagnano l'imposizione di tali sanzioni (par. n. 16). In altre parole, riconoscendo alla Rete il ruolo primario di strumento per formare e manifestare il pensiero, lo stesso accesso ad Internet viene elevato a diritto fondamentale, e solo con il parere dell'autorità giudiziaria sarà eventualmente possibile comprimere questo diritto.
Viene inoltre richiamato l'art. 9 della Dichiarazione del 1789 che sancisce il principio generale della presunzione di non colpevolezza, poiché l'art. L 331-38 della L. 669/2009 pone a carico del titolare dell'accesso ad Internet l'onere di produrre gli elementi in grado di dimostrare che la violazione del

---

dalle regole sulla protezione dei diritti dell'uomo e fondamentali garantiti dalle costituzioni degli Stati membri, dai trattati internazionali sui diritti dell'uomo, compresa la CEDU, dai principi generali del diritto comunitario e dalla Carta dei diritti fondamentali dell'Unione europea, e/o da altre pertinenti norme della legislazione nazionale, internazionale e comunitaria, nei rispettivi ambiti d'applicazione».

[158] Raccomandazione del Parlamento europeo del 26 marzo 2009 destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet (2008/2160(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//IT (20/01/2010).

[159] Décision n° 2009-580 DC du 10 juin 2009, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html (29/9/2009).

diritto d'autore o dei diritti connessi che gli viene attribuita è conseguenza della frode di un terzo (che, ad esempio, abbia usufruito a sua insaputa della connessione): «qu'ainsi, en opérant un renversement de la charge de la preuve, l'article L. 331-38 institue, en méconnaissance des exigences résultant de l'article 9 de la Déclaration de 1789, une présomption de culpabilité à l'encontre du titulaire de l'accès à internet, pouvant conduire à prononcer contre lui des sanctions privatives ou restrictives de droit» (par. n. 18).

2.2. Il progetto «HADOPI 2» e qualche considerazione a margine.

Il 22 settembre 2009 il Parlamento francese ha adottato il testo definitivo del progetto di legge «relatif à la protection pénale de la propriété littéraire et artistique sur internet»[160] che modifica ulteriormente la L. 669/2009 in seguito alle censure mosse dal Consiglio Costituzionale.
Spettano all'HADOPI, secondo la nuova formulazione, i poteri di polizia giudiziaria necessari per svolgere le indagini sulle presunte violazioni dei diritti d'autore (art. 1), mentre incomberà sul giudice il compito di irrogare la sanzione finale. L'art. 7 introduce nel Codice della proprietà intellettuale l'articolo L. 335-7 che conferisce al giudice, quando sia accertato che le violazioni di cui agli articoli L. 335-2, L. 335-3 e L. 335-4 sono state commesse per mezzo di un servizio di comunicazione al pubblico online, il potere di applicare ai loro autori, oltre alla **sospensione dell'accesso alla Rete per un massimo di un anno**, anche il **divieto di stipulare nel corso dello stesso periodo un altro contratto per un servizio analogo da qualsiasi operatore**. Si tratta perciò di una vera e propria **interdizione dall'accesso ad Internet**, che va ad aggiungersi, mediante la modifica operata dall'art. 11, alle diverse interdizioni previste dall'art. 434-41 del codice penale (quali, ad esempio, la sospensione della patente di guida o il divieto di detenere un'arma o un animale).
Nonostante l'intervento del Consiglio Costituzionale, le garanzie per l'imputato sono state ripristinate solo in parte: se è vero che l'autorità giudiziaria si sostituisce all'HADOPI al momento di comminare l'eventuale sanzione, è anche vero che a quest'ultima si può giungere mediante ordinanza penale, all'esito di un procedimento che non prevede contraddittorio, nel quale un giudice unico produce una decisione sulla base di elementi probatori, senza obbligo di motivazione e senza che vi siano ragioni di urgenza a giustificarlo (dal momento che, anche nella vigenza del nuovo testo, è necessario percorrere l'iter degli avvertimenti preventivi, inviati al trasgressore in tempi e modi differenti)[161].
Irrisolte sono poi le questioni riguardanti il principio della presunzione di non colpevolezza e la personalità della responsabilità penale sollevate dalla HADOPI 1, poiché il progetto di legge introduce il **reato di «négligence caractérisée»**, che pone a carico del titolare del contratto di accesso ad Internet una **sorta di obbligo di impedire che dal proprio IP siano commessi illeciti**. Infatti, in caso di comprovata «negligenza» (sulla sussistenza della quale sarà chiamato ad esprimersi il giudice), anche chi non si sia reso direttamente colpevole di alcuna violazione dei diritti d'autore, ma abbia consentito – anche non volontariamente, ad esempio per incapacità tecnica – a terzi di compiere dette violazioni, è passibile, oltre che di una multa, della sospensione dell'abbonamento fino ad un mese.
Anche al di là di questi rilievi, sembrerebbe comunque lecito continuare a nutrire forti perplessità nei confronti di una misura sanzionatoria che va ad incidere in maniera così grave sulle libertà della persona, considerata «la peculiarità stessa dell'accesso alla rete in ragione dei suoi stretti e coessenziali addentellati con valori strutturali come il pluralismo informativo e con libertà fondamentali come quelle comunicative»[162]. Diversi Stati impongono filtri alla Rete per controllare il flusso di informazioni in entrata ed in uscita e reprimere quella «resistenza democratica» richiamata recentemente dal Garante per

[160] Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, http://www.legifrance.gouv.fr/telecharger_rtf.do?idTexte=LEGITEXT000021209451&dateTexte=20091030 (12/10/2010).
[161] Va detto tuttavia, come sottolineato in un'analisi effettuata da *La Quadrature du Net*, che la legge HADOPI è stata concepita e fortemente voluta per dare una risposta di massa ad un fenomeno di massa, mentre l'intervento dell'autorità giudiziaria renderà in larga parte inattuabile tale proposito: cfr. *Qui a gagné la bataille Hadopi?*, 24 ottobre 2009, http://www.laquadrature.net/fr/qui-a-gagne-la-bataille-hadopi (18/01/2010).
[162] P. COSTANZO, *L'accesso ad Internet in cerca di autore*, in *Diritto dell'Internet*, n. 3, 2005, p. 251.

la protezione dei dati personali, con effetti, si potrebbe pensare ad una prima analisi, ben più preoccupanti di quelli finora paventati. Si pensi a tutti i provvedimenti sul controllo del Web introdotti con il pretesto di combattere la pedopornografia online, o all'operato dei Governi che Reporter Senza Frontiere ha definito «i 12 nemici di Internet»[163]. Non è semplice però individuare il confine: fino a quando una misura preventiva o a carattere sanzionatorio rappresenta il risultato di un «bilanciamento di interessi» (più o meno equo) e quando invece si trasforma in censura, o, meglio, nella revoca di talune libertà fondamentali?

Se «Internet dà pieno significato alla definizione di libertà di espressione» si potranno forse comprimere le condizioni per il suo utilizzo, in presenza di altri interessi rilevanti, ma non sembra tollerabile una soppressione indiscriminata di tutte le possibilità offerte dallo strumento in parola, seppur temporanea e pronunciata da un'autorità giudiziaria sulla base di una legge, perché comunque di dubbia necessità, proporzionalità e adeguatezza (secondo i principi espressi dal Parlamento Europeo) rispetto alla violazione che si vorrebbe perseguire.

D'altro canto, ci si potrebbe chiedere poi quanto una tale politica repressiva si riveli efficace: il divieto di sottoscrivere un nuovo abbonamento ad Internet da parte dell'utente condannato non sembra (e non si vede come potrebbe essere altrimenti) travolgere effettivamente la possibilità per quest'ultimo di continuare a commettere illeciti servendosi di altri IP, mediante *Virtual Private Network* o spostandosi materialmente su altre macchine (presenti presso *Internet point*, biblioteche pubbliche, aree *wi-fi* «aperte» ma, si potrebbe ipotizzare, anche che richiedano l'iscrizione/identificazione dell'utente, dal momento che quest'ultima non sembrerebbe poter essere assimilata ad un abbonamento e, in ogni caso, non appare una via facilmente praticabile quella di controllare lo *status* di «sospeso dal web» di ogni cittadino francese). Al contrario, il progetto francese sembrerebbe lasciare ampie possibilità di azione a chi probabilmente rappresenta, agli occhi degli estensori della legge, il pericolo principale per i titolari dei diritti d'autore, colpendo al contempo gli utenti più svantaggiati della Rete, coloro che per handicap fisico o limitate conoscenze informatiche non hanno la possibilità di aggirare i divieti loro imposti: coloro, cioè, per i quali Internet come strumento di comunicazione e di informazione ricopre un ruolo ancora più importante e che, nell'ottica condivisa[164] di un progressivo abbattimento del c.d. *digital divide*, dovrebbero rappresentare il principale obiettivo di una politica di libero accesso alla Rete, anziché esserne esclusi.

Il «caso» francese appare interessante e meritevole di approfondimento non tanto per il suo impatto effettivo (nel momento in cui iniziava la redazione di questo scritto risultavano da poco iniziate le prime procedure di applicazione della legge HADOPI – peraltro non senza difficoltà[165] – e, secondo un primo studio volto ad analizzarne gli effetti, la c.d. «pirateria digitale» non era diminuita, ma si registrava semplicemente un cambio di abitudini in relazione ai protocolli utilizzati[166]) particolarmente in relazione

---

163 Cfr. *Internet enemies*, Parigi, 12 marzo 2009, all'URL http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf (5/9/2009).

164 Cfr. fra i vari esempi le Comunicazioni della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni *Verso una società dell'informazione accessibile* (COM/2008/0804 def.), all'URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0804:FIN:IT:HTML, *i2010 – Una società europea dell'informazione per la crescita e l'occupazione* (SEC(2005) 717), all'URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:IT:PDF, nonché *eAccessibilità* (SEC(2005) 1095), all'URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0425:FIN:IT:PDF (4/9/2009). Molte altre iniziative di «e-inclusione» sono poi reperibili all'URL http://europa.eu/legislation_summaries/information_society/index_it.htm (4/9/2009).

165 Dovute al fatto che alcuni ISP rifiutano di inviare le e-mail di «avvertimento» ai propri iscritti, dal momento che la legge non sembra definire con sufficiente precisione quale debba effettivamente essere il loro ruolo. Cfr. G. CHAMPEAU, *Hadopi : Frédéric Mitterrand annonce un décret pour sanctionner Free (MAJ)*, in *Numerama*, 12 ottobre 2010, http://www.numerama.com/magazine/16994-hadopi-frederic-mitterrand-annonce-un-decret-pour-sanctionner-free-maj.html (12/10/2010).

166 Uno dei principali effetti della HADOPI, che di fatto equipara la «pirateria informatica» con l'utilizzo del protocollo P2P, sembrerebbe infatti essere quello di aver indirizzato una larga parte degli utenti di reti P2P verso streaming e servizi HTTP-based. Cfr. S. DEJEAN, T. PENARD, R. SUIRE, Une première évaluation des effets de la loi Hadopi sur les pratiques des Internautes français, M@rsouin, CREM et Université de Rennes 1, Marzo 2010, in Internet all'URL http://recherche.telecom-bretagne.eu/marsouin/IMG/pdf/NoteHadopix.pdf (31/08/2010). Cfr. anche M. VECCHIO, *Se HADOPI ostacola lo spionaggio*, in *Punto Informatico*, 8 ottobre 2010, http://punto-informatico.it/3006777/PI/News/se-hadopi-ostacola-spionaggio.aspx (12/10/2010).

alla «negligenza caratterizzata», che impone al titolare dell'accesso ad Internet di proteggere la propria rete wireless con misure (minime) che siano in grado di metterlo al riparo dall'accusa di non aver evitato la commissione da parte di terzi di infrazioni al diritto d'autore.
Diversi sono i punti di contatto con la situazione italiana. Entrambe le legislazioni si pongono come obiettivo finale la tracciabilità dei comportamenti tenuti online dagli utenti, una per combattere il terrorismo, l'altra, un po' meno pomposamente, per combattere la «pirateria digitale». Lo fanno in maniera diversa: HADOPI non impone obblighi di identificazione poiché vi è una presunzione di responsabilità a carico del titolare dell'accesso ad Internet, sia esso privato (quando non abbia adottato le misure «minime» di sicurezza) o esercente pubblico, mentre in Italia tale presunzione viene a mancare ma, in vigenza del decreto Pisanu, chiunque accedava alla Rete doveva essere previamente identificato (anche se in realtà, come si è visto, le incongruenze non mancavano).
Entrambi i sistemi sembrano mancare gli obiettivi sia per motivi tecnici che giuridici e/o procedurali. In particolare il dibattito in Francia è attualmente aperto (a più di un anno dall'effettiva entrata in vigore della legge) sulla definizione delle suddette misure di sicurezza e, conseguentemente, su *quanto* sicura debba essere una rete wi-fi per mettere al riparo il titolare dell'accesso ad Internet da responsabilità (oggettiva) per fatti commessi da terzi[167]. Per quanto riguarda, poi, gli esercizi pubblici, le minacce per la libertà di espressione dei cittadini francesi giungono non attraverso la soppressione dell'anonimato come avveniva in Italia[168], bensì attraverso un filtraggio a monte dei contenuti che sono considerati «accettabili»: l'art. L. 331-23 stabilisce infatti che l'Alta Autorità (HADOPI) mantenga e aggiorni periodicamente una lista di «etichette» volte ad identificare chiaramente la natura giuridica dei contenuti offerti dai prestatori di servizi di comunicazione al pubblico, anche se non appare del tutto chiaro (data la non obbligatorietà per Internet café e *providers* in genere di implementare tale *white list*) quali possano essere le effettive conseguenze in caso di illecito.
Certamente ci si può aspettare che, nel timore di incorrere in responsabilità per fatti commessi dai propri utenti, i gestori di Internet café e punti di accesso pubblico alla rete limitino il traffico consentito ai soli «siti di Stato» autorizzati da HADOPI.
L'ultimo aggiornamento di cui è qui possibile rendere brevemente conto circa la situazione francese è relativo all'entrata in vigore di un decreto[169] applicativo della LCEN[170] (*Loi pour la Confiance dans l'Economie Numérique* – Legge per la fiducia nell'economia digitale) che sembra richiedere non solo agli ISP ma anche ad altri prestatori di servizi Internet di mantenere i dati identificativi della connessione, del terminale utilizzato dall'utente, la data e l'ora di inizio e fine della connessione e le caratteristiche della linea di accesso. Nonostante tali obblighi richiamino quelli contenuti nel decreto Pisanu e che venivano definitivamente abrogati proprio mentre il decreto francese entrava in vigore, la Francia sembra mantenersi ancora distante dall'eccesso italiano, pur se pericolosamente più vicina di altri Paesi e nonostante la conferma di un certo indirizzo «anti-anonimato» del suo legislatore.

3. UK: il Digital Economy Act

167 C. TAMBURRINO, *HADOPI, le lettere debuttanti*, in *Punto Informatico*, 5 ottobre 2010, http://punto-informatico.it /3004009/PI/News/hadopi-lettere-debuttanti.aspx (12/10/2010).
168 Ma i tempi non sono favorevoli all'anonimato nemmeno in Francia: agli inizi del mese di maggio 2010 il senatore Jean-Louis Masson ha infatti presentato un disegno di legge (il testo è reperibile all'URL http://www.senat.fr/leg/ppl09-423.html) per imporre ai *bloggers* di rendere noti sui loro blog i propri dati personali (nome, numero di telefono e indirizzo). «The senator justified his proposal with the argument of protecting Internet users from deceit, lies or defamation. In an interview for France 3, the senator stated he wanted bloggers to take the responsibility of their statements. In his opinion, a person who does not reveal his identity has something to hide, while generally bloggers choose anonymity out of reasons related to their professional or personal life»: cfr.. *The end of bloggers' anonymity in France?*, EDRi-gram - Number 8.11, 2 June 2010, http://www.edri.org/edrigram/number8.11/law-annonimity-bloggers-france (01/09/2010).
169 Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, http://www.legifrance.gouv.fr/affichTexte.do? cidTexte=JORFTEXT000023646013&categorieLien=id (01/03/2011).
170 Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, http://www.legifrance.gouv.fr/affichTexte .do?cidTexte=LEGITEXT000005789847&dateTexte=vig (01/03/2011).

Nel Regno Unito, già prima dell'entrata in vigore del *Digital Economy Act* (DEA), un primo esempio di responsabilità dei titolari della connessione ad Internet per fatti di terzi si è verificato ai danni del titolare di un pub, condannato a pagare un'ingente somma di denaro, in quanto ritenuto responsabile del download di materiale protetto dal diritto d'autore effettuato da un suo cliente attraverso la rete wi-fi aperta dell'esercizio[171].

Approvato in tempi piuttosto brevi e in circostanze particolari (negli ultimi giorni di vigenza della House of Commons prima delle nuove elezioni, dopo che il Primo Ministro aveva annunciato la data delle nuove elezioni[172], con un numero esiguo di partecipanti all'unica sessione dibattimentale e un elevato numero di non votanti in fase di approvazione finale del testo di legge) il DEA sembrerebbe destinato a sortire effetti molto simili a quelli dell'HADOPI francese, condividendone il modello c.d. *three-strikes* («three-stage notification process»), ma sulla base di un separato provvedimento («*Obligation Code*») ancora in fase di elaborazione da parte di Ofcom, l'autorità britannica per le comunicazioni.

L'insieme delle disposizioni contenute nel DEA e nella bozza di codice elaborata[173] prevede che il detentore del copyright che ritenga che sia in atto una violazione dei propri diritti da parte di un certo indirizzo IP possa contattare l'ISP di riferimento spedendogli un «copyright infringement report» (CIR), che deve contenere i dati necessari a «circostanziare» la denuncia di violazione[174]. L'ISP deve quindi procedere a notificare la violazione al *subscriber* (sulla cui nozione si tornerà in seguito) che risultava titolare dell'indirizzo IP assegnato al momento della violazione stessa, e questi può «appellarsi» (anche se il procedimento di contestazione dell'addebito non appare al momento ben definito). Se il *subscriber* non si appella, o se le motivazioni addotte sono ritenute non fondate, l'ISP deve tenerne traccia, insieme al numero di CIR ricevuto e, oltre una certa soglia (non ancora definita: di CIR, di notifiche effettuate, ecc.), inserire il *subscriber* in una *copyright infringement list* (CIL) che i detentori del copyright possono chiedere di conoscere. Questa informazione tuttavia non consente direttamente ai detentori del copyright di conoscere l'identità dei *subscribers*, ma permette l'associazione fra un numero *n* di CIR inviati e uno stesso *subscriber* a cui le violazioni sarebbero riferibili, mentre l'identificazione vera e propria dovrebbe essere conseguenza di un provvedimento dell'autorità giudiziaria. Allo stato attuale, dunque, tali disposizioni non configurano una sanzione di tipo diretto a carico del *subscriber*, quanto piuttosto il suo inserimento in una sorta di *watch list*, che può eventualmente sfociare, in un momento successivo, in una sanzione.

Fra le notevoli questioni controverse (che in questa sede non è possibile approfondire, e tra cui potrebbero essere annoverate le modalità di notifica – via mail – ai *subscribers*, nonché il ruolo attivo che dovrebbe essere assunto dagli ISPs, trasformati – con una probabile infrazione delle norme comunitarie che limitano la responsabilità e gli obblighi di tali intermediari della comunicazione – in «guardiani» del rispetto dei diritti d'autore) merita sicuramente attenzione quella relativa alla nozione di *subscriber* e della responsabilità di quest'ultimo.

La sezione 124A (1) (b) introdotta dal DEA nel *Communication Act* del 2003 stabilisce che le disposizioni ivi contenute si applichino quando il detentore del copyright ritenga («it appears to a copyright owner that») che: «(a) a subscriber to an internet access service has infringed the owner's copyright by means of the service; or (b) a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner's copyright by means of the service»[175]. Le disposizioni riguardanti *subscribers* e ISPs permettono di distinguere abbastanza chiaramente i primi dai

---

171 Cfr. L. EDWARDS, *In the thick of it: how the Digital Economy bill is trying to kill open Wi-Fi networks*, in *The Guardian*, 30 Novembre 2009, http://www.guardian.co.uk/technology/2009/nov/30/open-wi-fi-digital-economy-bill-government (01/09/2010).

172 Si tratta del c.d. *wash-up period*: solitamente vi vengono affrontate unicamente questioni di «ordinaria amministrazione» e sulle quali vi è un largo consenso di entrambi gli schieramenti.

173 Consultabile all'URL http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf (02/09/2010).

174 Il testo del Digital Economy Act è reperibile all'URL http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf (02/09/2010). I requisiti che deve possedere un *copyright infringment report* sono elencati alla sezione 124A (3), introdotta dal DEA nel Communication Act del 2003.

175 «Subscriber», ai sensi del successivo par. 124N, è una persona che, in relazione ad un servizio di accesso ad Internet «(a) receives the service under an agreement between the person and the provider of the service; and (b) does not receive it as a communications provider».

secondi sulla base di un accordo, che deve sempre sussistere, in base al quale viene fornito il servizio di accesso ad Internet. Individuato, perciò, come «subscriber» il proprietario di una rete wi-fi, e come tale non soggetto alle disposizioni del DEA rivolte agli ISPs (quali ad esempio le «obligations to limit internet access» di cui alla sez. 124G e ss., volte a prevenire o ridurre le violazioni del copyright a mezzo Internet), rimane da chiarire se egli possa legalmente mantenere aperta la propria rete wi-fi e, in caso affermativo, a quale tipo di responsabilità eventualmente si esponga in caso di reati commessi da terzi attraverso il proprio IP.

L'Obligation Code di Ofcom è, sul punto, abbastanza dettagliato, e prende in considerazione non solo le reti wi-fi facenti capo a privati, ma anche quelle messe a disposizione da pubblici esercizi e altri «operatori» che offrono il servizio di accesso ad internet senza fili unitamente ad un altro (sono ad esempio espressamente citati hotel e *coffee shops*). Dalla bozza è possibile ricavare che:

a) i gestori di reti wi-fi aperte e gratuite, in cui non può essere individuato alcun accordo fra il titolare dell'accesso ad internet e chi eventualmente ne usufruisca sono considerati «subscribers» (par. 3.22);
b) i gestori che forniscono connettività come servizio aggiuntivo rispetto ad un altro (hotel, caffetterie, altri pubblici esercizi per i quali, comunque, si suppone vi sia un accordo fra titolare ed utenti che si estende all'utilizzo della rete) ricadrebbero nella definizione di ISP ma ne vengono espressamente esclusi, almeno in un primo momento, poiché il numero dei relativi subscribers non è ritenuto significativo rispetto agli intenti perseguiti dalla legge (par. 3.23).

Il par. 3.30 affronta ulteriormente, in relazione al primo punto qui elencato, la «questione critica» posta dagli utenti che rendono disponibile a terzi l'accesso ad Internet, mentre al par. 3.31 «suggerisce» a tali soggetti l'adozione di misure atte a proteggere le reti: «Those who wish to continue to enable others to access their service will need to consider whether take steps to protect their networks against use for infringement, to avoid the consequences that may follow». Contemporaneamente, in altre parti dello stesso documento (sezioni 7.5 e 7.11) viene precisato che qualora il subscriber appelli la notifica di violazione del copyright negando il proprio coinvolgimento dovrà anche dimostrare di aver adottato «reasonable steps to prevent other persons infringing copyright by means of the internet access service». E tali «reasonable steps» sembrano, in definitiva, risolversi nella cifratura della rete wi-fi, dal momento che se la rete è aperta, *firewall* e *port blocking* si rivelano misure del tutto insufficienti a bloccare, ad esempio, il traffico di tipo *torrent*. Va comunque notato che al momento non è rinvenibile alcuna definizione di «reasonable steps».

L'approccio britannico è formalmente diverso rispetto a quello francese, ma la sostanza non sembra mutare sensibilmente: la negligenza caratterizzata che fonda la responsabilità oggettiva introdotta da HADOPI diviene con il DEA mancanza di elementi idonei a giustificare il titolare dell'indirizzo IP «incriminato» qualora venga commesso un reato, stante, in entrambi i casi, l'inversione dell'onere della prova a carico dell'«indagato» che, una volta accusato della violazione in quanto titolare dell'IP, avrà l'onere di dimostrare la propria estraneità ai fatti. In entrambi i casi non c'è un vero e proprio divieto di fornire connettività attraverso una rete wifi aperta, ma tale scelta viene fortemente scoraggiata dalle possibili conseguenze per il titolare.

Rispetto al modello francese, e per certi versi anche al modello italiano, quello britannico appare tuttavia, limitatamente agli aspetti finora menzionati, meno repressivo: gli ISPs a cui può applicarsi la normativa *de qua* sono infatti solo quelli «fissi» (e sono perciò esclusi i fornitori di accesso ad Internet mobile) che abbiano più di 400.000 iscritti, e nonostante le (fondate) preoccupazioni per la sorte del wi-fi in luoghi quali biblioteche e università, tale requisito appare al momento sufficiente a mantenere in vita gli ormai «storici» baluardi di libertà di accesso alla Rete[176]. I quali se da un lato si pongono come

[176] Sembrerebbe tuttavia di fondamentale importanza la qualificazione come ISP (sebbene non «qualifying», ovvero non soggetto all'applicazione del DEA) e, perciò, l'offerta della connettività wi-fi come conseguenza di un qualunque tipo di accordo, sia esso anche una semplice pagina di *Terms of use* che l'utente deve visualizzare ed accettare. Si veda anche il documento *Online Infringement of Copyright: Libraries, Universities and Wi-Fi Providers*, febbraio 2010, all'URL http://interactive.bis.gov.uk/digitalbritain/wp-content/uploads/2010/02/Example-infringement-notifications.pdf (06/08/2010). La data di rilascio del documento è precedente alla bozza di Ofcom e alla consultazione pubblica, ma appare interessante poiché si focalizza in particolare su università e biblioteche che offrono una connessione wi-fi. Si veda inoltre *The Digital Economy Act 2010 – Implications for UK Colleges and Universities*, JISC Legal, luglio 2010,

opportuno (ma non sufficiente) contrappeso alla rigidità del *three-stage notification process*, dall'altro appaiono comunque minacciati dalla provvisorietà della bozza proposta da Ofcom, non ancora operativa e, dunque, suscettibile di essere ancora modificata sensibilmente, anche in *malam partem* e nonostante, quasi contemporaneamente all'approvazione del DEA, l'allora Primo Ministro inglese avesse riconosciuto pubblicamente[177] come «The internet revolution is quite literally creating a different world», aggiungendo successivamente: «just imagine if you weren't part of that world. Imagine if you had never accessed the Internet. Imagine if you had no access to the best deals on the virtual high street […]». Il discorso di Gordon Brown si focalizzava sulla necessità di ampliare la copertura della banda larga e indicava in circa un quinto la frazione di popolazione che non aveva accesso alla Rete, definendo tale esclusione «unfair, economically inefficient and wholly unacceptable». Ma se a «fundamental freedom in the modern world» è «to be part of the internet and technology revolution», forse non andrebbero esclusi da questa rivoluzione tecnologica nemmeno i rimanenti quattro quinti di popolazione che attualmente hanno accesso alla Rete e che in virtù del DEA potrebbero vedere la loro capacità di muoversi ed interagire nel «modern world» grandemente scemata.
Nei primi mesi del nuovo cabinet non risultano novità significative da segnalare.

4. Germania: connessioni wi-fi e responsabilità per non aver cambiato la password del router

Nel mese di maggio 2010 la Prima sezione civile della Corte federale tedesca emetteva una sentenza[178] che, secondo quello che fu poi riportato dalla stampa, sembrava istituire un obbligo per i titolari di reti wi-fi di proteggere le proprie connessioni per non incorrere in multe a seguito di fatti illeciti commessi da terzi[179].
Si trattava in realtà di un procedimento civile nel quale veniva espressamente esclusa dalla Corte una sorta di corresponsabilità per i danni richiesti dai titolari dei diritti d'autore di un brano musicale che era stato immesso da un terzo in un circuito di *file sharing* utilizzando la rete wi-fi non adeguatamente protetta del convenuto.
La «multa» alla quale il convenuto è stato condannato dovrebbe in realtà costituire una parziale compensazione per le spese legali sostenute dall'attore (*Abmahnkosten*), mentre è stata espressamente esclusa dalla Corte ogni forma di responsabilità per violazione del diritto d'autore del proprietario della rete lasciata «incustodita». La sentenza in questione è tuttavia singolare poiché, nel compensare le spese legali, sostiene che era ragionevole aspettarsi dal convenuto che al momento dell'installazione della rete wi-fi nella propria abitazione cambiasse la password «di fabbrica» (impostata di *default* su ogni *router* venduto) con una personalizzata, a tutela anche dei propri dati. E ciò, sembrerebbe, in assenza di norme che regolino se e come una rete debba (giuridicamente) essere protetta e come.
Né si rinviene, con riferimento più generale all'accesso ad Internet tramite wi-fi in aree pubbliche o messe a disposizione del pubblico, alcun obbligo di identificazione degli utenti o di registrazione degli stessi. La Germania si è inoltre espressamente opposta al modello «three-strikes».

---

http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DEA%20Guidance.pdf (15/10/2010).
177 G. BROWN, *Speech on Building Britain's Digital Future*, Londra, 22 marzo 2010, trascrizione reperibile sul sito ufficiale dell'Ufficio del Primo Ministro (http://www.number10.gov.uk), all'URL http://webarchive.nationalarchives.gov.uk/+/number10.gov.uk/news/speeches-and-transcripts/2010/03/speech-on-building-britains-digital-future-22897 (07/09/2010).
178 Bundesgerichtshofs (BGH), I. Zivilsenats, Urteil vom 12. Mai 2010 - I ZR 121/08 - Sommer unseres Lebens, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&anz=101&pos=0&nr=52202&linked=urt&Blank=1&file=dokument.pdf (07/09/2010).
179 Associated Press diffonde la notizia con il titolo «German court orders wireless passwords for all - Users can be fined if a third party takes advantage of an open connection»: cfr. ad esempio http://www.msnbc.msn.com/id/37107291 (07/09/2010). Nell'articolo si fa inoltre espresso riferimento ad una responsabilità di tipo penale: «Germany's top criminal court ruled Wednesday that Internet users need to secure their private wireless connections by password to prevent unauthorized people from using their Web access to illegally download data. Internet users can be fined up to euro100 ($126) if a third party takes advantage of their unprotected WLAN connection to illegally download music or other files, the Karlsruhe-based court said in its verdict».

5. Olanda: tutti operatori?

In Olanda, dove – come in tutti gli altri Paesi europei – una norma sull'identificazione degli utenti di reti wi-fi non esiste, l'OPTA, l'autorità per le telecomunicazioni nazionale, ha recentemente paventato[180] la possibilità di introdurre un obbligo per gli hotel di registrarsi come «public electronic communications providers». L'interpretazione (in verità piuttosto fantasiosa) fornita da OPTA è che dal momento in cui un soggetto offre al pubblico l'accesso ad Internet, diviene operatore di una rete pubblica di telecomunicazioni, e deve quindi registarsi come tale e sottostare alle previsioni della Direttiva sulla *data retention*.
Le organizzazioni di categoria considerano quella che per il momento è una comunicazione a cui non risulta sia stato dato seguito come un modo per OPTA di ottenere nuove fonti di finanziamento in un momento di crisi per il settore delle telecomunicazioni, mentre la Commissione Europea non ha ufficialmente espresso una posizione in merito.
È interessante citare la suddetta comunicazione poiché i risultati dell'assimilazione fra hotel e ISP porterebbero all'identificazione degli utenti e all'obbligo, per gli esercizi ricettivi olandesi, di sostenere costi aggiuntivi del tutto sproporzionati rispetto all'attività esercitata, con la motivazione (ormai prevedibile) «to monitor crime and terrorism».

6. Alcuni altri paesi europei e OCSE

In **Spagna** si rileva l'approvazione, lo scorso 9 febbraio, della c.d. *ley Sinde* (*Ley de Economia Sostenible*), che affida al governo spagnolo (ed in particolare ad un'apposita Commissione della Proprietà Intellettuale costituita presso il Ministero della Cultura) il compito di vigilare sul rispetto dei diritti di proprietà intellettuale. Il Governo potrà in definitiva chiudere le pagine web contenenti link a materiali protetti dal diritto d'autore con una semplificazione estrema del ruolo attribuito all'autorità giudiziaria (che deve essere coinvolta per le ovvie implicazioni in tema di libertà di espressione e per autorizzare l'identificazione dei titolari dei siti), e si differenzia dal modello francese poiché non mira a colpire direttamente gli utenti che scaricano dalla Rete, ma i gestori delle piattaforme P2P.
In **Finlandia** è stato presentato un progetto di legge volto a depenalizzare il reato di uso non autorizzato di wi-fi aperte altrui, probabilmente perché data la diffusione delle stesse l'utilizzatore può non essere in grado di sapere se in un dato momento sta utilizzando «abusivamente» la Rete di qualcuno oppure se tale utilizzo è consentito dal proprietario. Questa notizia[181] chiarisce evidentemente ogni dubbio relativo all'eventuale sussistenza di norme sull'identificazione.
In **Giappone** ad inizio luglio 2010 fu introdotto l'obbligo di mostrare un documento di identità per accedere agli Internet Cafè, ma tale obbligo non ha nulla a che vedere con l'accesso ad Internet: dal momento che gli Internet Cafè forniscono anche servizi per potervi pernottare a basso costo, il documento di identità è il mezzo ideato dal Governo per evitare che gli *homeless* vi si affollino (e quindi per presunti problemi di sicurezza «offline», non online).
Gli **USA** meriterebbero probabilmente una trattazione separata ma, ai presenti fini, è sufficiente ricordare che ogni provvedimento che ha inciso, anche in maniera molto pervasiva, sulla privacy dei cittadini (*Echelon*, *Carnivore*, *TIA* o il *Patriot Act*, introdotto dopo l'11 settembre come misura antiterrorismo e teso a rafforzare i poteri dei corpi di polizia e di spionaggio: tutti volti ad intercettare il contenuto delle comunicazioni dei cittadini anche in assenza di un'autorizzazione preventiva dell'autorità giudiziaria) non ha mai riguardato restrizioni di alcun tipo dell'accesso alla Rete.

---

180 J. BAKER, *Hotels May Be Subject to Strict EU Rules for Providing Wi-Fi, in IDG News, 14 ottobre 2010*, http://www.pcworld.com/businesscenter/article/207821/hotels_may_be_subject_to_strict_eu_rules_for_providing_wifi.html (27/10/2010).
181 Cfr. *Finland Plans To Decriminalize Using Open WiFi*, http://www.techdirt.com/blog/wireless/articles/20100611/1234429783.shtml#comments (15/06/2010).

7. Esempi scelti dai Paesi non-OCSE

All'estero, l'esempio più simile (e più vicino, se si escludono alcuni Paesi arabi di cui si dirà in seguito) al modello di identificazione e monitoraggio introdotto in Italia dal decreto «Pisanu» è quello della **Bielorussia**. Già dal 10 febbraio 2007 sono infatti operanti norme relative al monitoraggio dei siti a cui gli utenti hanno accesso, ed alla conservazione dei relativi dati, ma dal 1° luglio 2010 è entrato in vigore il decreto n. 60 del febbraio 2010 «On measures for improving use of the national Internet network»[182], che richiede agli ISPs di registrarsi presso il Ministero e di identificare tutti i *devices* (inclusi computer e telefoni cellulari) utilizzati per la connessione ad Internet. Chiunque voglia navigare all'interno un Internet café o utilizzando un'altra connessione condivisa (ad esempio, in un condominio) deve essere identificato, e le informazioni relative a tutti i collegamenti Internet devono essere conservate per un anno. Tali misure scoraggeranno inevitabilmente le persone dal visitare siti indipendenti e di opposizione. Il decreto crea anche un Centro, alle dirette dipendenze del presidente bielorusso, che avrà il compito di monitorare i contenuti prima della loro messa online. È inoltre stato introdotto un sistema di filtraggio per il controllo dell'accesso ai siti web che sono considerati pericolosi, tra cui quelli «estremisti», a carattere pornografico, violenti o riguardanti il traffico di armi, di stupefacenti o di esseri umani.

Dal 1° luglio anche la **Cina** richiede agli avventori degli Internet Cafè di mostrare un documento d'identità per poter accedere ad Internet, onde evitare che vi entrino minori. Al documento di identità può essere sostituito, a scelta degli operatori, l'accesso tramite smart card. La norma, apparentemente in linea con il decreto Pisanu italiano, non ha in realtà nulla a che vedere con la navigazione e, più in generale, con quello che gli utenti facciano dopo l'accesso all'Internet Cafè: l'unica preoccupazione è quella di non fare entrare i minori, e il documento mostrato non viene in alcun modo fotocopiato o annotato dai titolari e gestori di tali luoghi[183].

In **Algeria**[184], dopo gli attacchi terroristici dell'aprile 2007 sono state introdotte misure di monitoraggio degli utenti degli Internet Cafè, che dal 2008 sono previamente identificati, ed i loro nomi e numeri di documento devono essere comunicati dai gestori alla polizia, così come ogni attività sospetta.

In **Giordania**, dal 2008, i gestori di Internet Cafè sono tenuti ad installare videocamere per monitorare gli utilizzatori, e devono mantenere dati relativi alle connessioni quali indirizzo IP, dati personali degli utilizzatori, il tempo di utilizzo e altri dati relativi ai siti Web visitati. Misure simili sono state introdotte fra 2007 e 2008 anche in **Siria** e nello **Yemen**.

Anche in **Arabia Saudita**[185] dal 2009 sono state introdotte le videocamere, nonché un insieme di altre misure di carattere amministrativo e organizzativo volte a comprimere le libertà degli utenti (e dei gestori di Internet Cafè di conseguenza). In particolare, per ciò che qui maggiormente interessa, i gestori devono mantenere un registro nel quale sono annotati i nomi degli utenti che sono stati identificati ed è vietato l'accesso ad Internet attraverso carte prepagate o per mezzo di connessione satellitare senza apposita autorizzazione rilasciata dall'autorità competente.

In **Kuwait** i gestori sono obbligati ad identificare i clienti e a mantenerne i nomi in un apposito registro a disposizione, su richiesta, del Ministero delle Comunicazioni. In **Egitto**, dal 2008, la procedura di identificazione degli utenti degli Internet Cafè prevede che l'accesso ad Internet sia consentito solo dopo aver fornito nomi, indirizzi e-mail e numeri di cellulare (utilizzati per consegnare il pin d'accesso).

Negli **Emirati Arabi Uniti** è necessario ricevere l'approvazione ministeriale e possedere una licenza commerciale valida per poter aprire un Internet Cafè. L'attrezzatura tecnologica deve essere acquistata da Etisalat, la società monopolista nel settore delle telecomunicazioni, che ovviamente fornisce anche

---

l[182] Cfr. Reporters Without Borders, *Authorities step up Internet restrictions, harassment of online journalists*, 6 luglio 2010, http://en.rsf.org/belarus-authorities-step-up-internet-06-07-2010,37867.html, nonché *Belarusian government adopts regulations on computer clubs and internet cafes*, http://www.e-belarus.org/news/200702151.html, e *New Belarus Internet regulations require compulsory web registration*, EDRi, 19 maggio 2010, http://www.edri.org/edrigram/number8.10/censorship-belarus-registration-websites (tutte le URL verificate il 15/10/2010).

[183] Cfr. S. ABRAMS, *China's Internet Cafes Respond to ID Check Rules*, 26 luglio 2010 (01/03/2011).

[184] I dati che seguono, dove non diversamente precisato, sono tratti dal report *Internet Filtering in the Middle East and North Africa*, OpenNet Initiative, 2009, http://opennet.net/sites/opennet.net/files/ONI_MENA_2009.pdf (27/07/2010).

[185] Cfr. anche http://www.openarab.net/en/node/902 (27/07/2010).

l'accesso ad Internet. Ad Etisalat il proprietario deve anche spedire una lettera specificando l'identità e la qualifica di chi gestisce l'Internet Cafè. In un primo tempo non erano previste restrizioni né misure identificative per gli avventori, ma dal 2006 la situazione è mutata e attualmente gli Internet Cafè sono identificati mediante photo-ID (necessario per poter ricevere username e password) e viene annotata la durata della navigazione, poiché «the internet cafe is where people go if they want to do bad things like hacking or sending threatening e-mails. All over the world, most cyber crime is done from public places»[186]. Vale la pena ricordare, in relazione ai «cybercrimes», che nel gennaio 2006 è stata emanata una legge in materia di crimini informatici, informazione e privacy (la prima in questi settori nei Paesi Arabi) nella quale può leggersi, ad esempio, che «if any person or group of persons construct a website, post online information, or make use of information technology tools to advocate, facilitate, or promote programs or ideas that would result into public disorder and disrupt morals, shall be liable to a penalty not exceeding five years»[187].

Nessuna forma di identificazione preventiva o di controllo è invece prevista, ad esempio, in **Bahrein**, o in **Iraq**, in **Israele** o nella tormentata **Palestina**, dove, data la proliferazione dei checkpoints militari (specialmente dal 2000 in poi) Internet è diventata un mezzo fondamentale per comunicare con parenti e amici, nonostante si registri qualche forma di «autocensura» sui contenuti da parte dei titolari degli Internet Cafè. Un esempio simile è quello della **Tunisia**[188], in cui pur in assenza di un vero e proprio obbligo per gli Internet Cafè di registrare gli utenti, i titolari si trasformano spesso volontariamente in censori poiché sono ritenuti responsabili per le attività online degli avventori.

Vi sono poi esempi, come quello dell'**Egitto**, in cui gli abusi da parte delle forze di polizia sono resi possibili proprio dall'inesistenza di una qualsiasi forma di regolamentazione[189], e altri invece (**Marocco**[190]) in cui, seppure una certa «diffidenza» verso lo strumento Internet emerga piuttosto chiaramente (la licenza necessaria si ottiene con più difficoltà rispetto ad altri esercizi pubblici, e può essere ritirata per contrarietà alla morale), gli Internet Cafè sono in aumento, il loro uso è diffuso fra la popolazione e la censura sui contenuti non appare particolarmente pervasiva nonostante le pressioni esercitate dalle autorità governative e religiose.

---

186 La dichiarazione è di Abdullah Hashem, senior manager di Etisalat: cfr. D. BARDSLEY, *Internet cafes to keep records of customers*, in *gulfnews.com*, 6 marzo 2006, http://gulfnews.com/news/gulf/uae/general/internet-cafes-to-keep-records-of-customers-1.227379 (08/09/2010). Cfr. anche, per approfondimenti, AA.VV., *Implacable Adversaries: Arab Governments and the Internet*, United Arab Emirates, http://www.openarab.net/ar/node/348 (08/09/2010).

187 Cfr. op. ult. cit., art. 20.

188 Cfr. op. ult. cit., Tunisia, http://www.openarab.net/ar/node/351(08/09/2010).

189 Cfr. op. ult. cit., Egypt, http://www.openarab.net/ar/node/363 (08/07/2010).

190 Cfr. op. ult. cit., Morocco, http://www.openarab.net/ar/node/364 (08/07/2010).

Ringraziamenti:
Il presente lavoro costituisce uno dei risultati della ricerca *Identificabilità delle persone sulla rete Internet: analisi tecnica, giuridica ed economica delle conseguenze sulla privacy, sulle libertà fondamentali, sull'innovazione e sui modelli di business*, condotto presso il **Centro Nexa su Internet & Società** del Politecnico di Torino nel corso del 2010. Desidero ringraziare i Direttori del Centro Nexa, prof. Juan Carlos De Martin e prof. Marco Ricolfi per avermi dato la possibilità di occuparmi di questi temi e per i continui stimoli ricevuti nel mio anno di ricerca. Un grazie collettivo a tutto lo staff (presente e passato) e ai fellows del Centro Nexa (Simone Basso e Federico Morando in particolare – tra i «residenti» – per le lunghe discussioni tecniche, oltre a Mauro Alovisio, Carlo Blengino, Marco Ciurcina, Alessandro Cogo e Massimo Travostino, tra i «non residenti»), nonché a Monica Alessia Senor e Fabio De Vito, rispettivamente, per i sempre preziosi suggerimenti e per la sperimentazione «sul campo». Un grazie particolarmente sentito agli amici (oltre che, in questo caso e in molti altri, maestri) Juri Monducci, Pierluigi Perri e Giorgio Spedicato, e ai proff. Alberto Artosi e Giovanni Ziccardi per la loro disponibilità e pazienza. Grazie, infine, a tutti coloro che a vario titolo mi hanno supportato in questo lavoro (chiedendo anticipatamente venia per i nomi che sicuramente dimenticherò): AIB (*Associazione Italiana Biblioteche*), Assoprovider, Lorenzo Benussi, Michael Billinger, Francesca Bosco, Phillip W. Brunst, Rafik Danmak, Andrea Glorioso, Giacomo Natali, Andrea Rivetti, Tanya Tropina.