UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Scienze Giuridiche

QUADERNI DEL DIPARTIMENTO

59

2006

ISBN 88-8443-152-2
978-88-8443-152-3

Stampato in Italia - Printed in Italy
Settembre 2006

Litotipografia Alcione S.r.l. – Trento

SICUREZZA INFORMATICA: REGOLE E PRASSI

Atti del Convegno
tenuto presso la Facoltà di Giurisprudenza di Trento
il 6 maggio 2005

a cura di
ROBERTO CASO

Contributi di

Roberto Caso
Andrea Gelpi
Paolo Guarda
Nicola Lugaresi
Giulia M. Lugoboni
Andrea Rossato

INDICE

PREMESSA

Questo libro raccoglie gli atti del convegno “La sicurezza informatica: regole e prassi” svoltosi il 6 maggio del 2005 presso la Facoltà di Giurisprudenza di Trento. Si tratta di una traccia che si aggiunge alle riprese dei lavori disponibili nell’archivio video del sito “Jus.unitn.it” all’URL:

http://www.jus.unitn.it/services/arc/2005/0506/home.html

Il convegno ha rappresentato un’occasione di confronto tra studiosi, tecnici dell’Università, rappresentanti dei mondi delle imprese e delle istituzioni attorno ad un tema cruciale del diritto dell’era digitale.

Quali problemi giuridici si pongono a ridosso della formula “sicurezza informatica”? Tali problemi si differenziano da quelli innescati dalla sicurezza in ambito non digitale? Come conciliare nel contesto digitale esigenze di sicurezza e diritti fondamentali come il diritto alla privacy? Le scelte sulla politica di sicurezza vanno prese a livello accentrato o decentrato?

Questi sono solo alcuni dei rilevanti quesiti emersi dalla discussione del maggio 2005. Per tentare di rispondervi occorrerà impegnare notevoli energie. Il convegno trentino ha dimostrato ancora una volta che buona parte di queste energie dovrà essere profusa nel tentativo di accrescere il dialogo tra saperi sempre più complessi.

Il testo che segue è suddiviso in due parti. Nella prima sono raccolte le trascrizioni o le rielaborazioni di alcune delle relazioni presentate durante il convegno. Nella seconda sono racchiusi due contributi aggiuntivi.

Un ringraziamento particolare va a chi ha permesso la realizzazione dell’iniziativa. Ai relatori e agli autori dei contributi aggiuntivi. Alla nominata Facoltà di Giurisprudenza e al

Dipartimento di Scienze Giuridiche di Trento che, assieme al Presidio per i servizi Informatici Telematici e Multimediali di Giurisprudenza (articolazione della Direzione Informatica e Telecomunicazioni dell'Ateneo trentino), hanno promosso e finanziato il convegno nonché la pubblicazione di questo libro. Allo staff del Dipartimento di Scienze Giuridiche che ha curato sia l'organizzazione della giornata del maggio 2005, sia l'editing di questo volume. Ai tecnici del Presidio ITM che hanno effettuato le riprese video e la pubblicazione sul Web delle stesse. Ad Andrea Gelpi che ha partecipato attivamente alla programmazione dell'evento. A Paolo Guarda che mi ha aiutato a comporre le pagine seguenti.

Trento, settembre 2006

Roberto Caso

ATTI DEL CONVEGNO

UN "RAPPORTO DI MINORANZA": ELOGIO DELL'INSICUREZZA INFORMATICA E DELLA FALLIBILITÀ DEL DIRITTO. NOTE A MARGINE DEL *TRUSTED COMPUTING*

Roberto Caso

1. Introduzione: approccio preventivo alla sicurezza informatica e problemi giuridici

In questa relazione che introduce i lavori del convegno, vorrei mettere in risalto l'importanza e la complessità dei problemi giuridici che ruotano attorno al tema della sicurezza informatica. Non mi cimenterò nel compito (inane) di definire il concetto di sicurezza informatica e passare in rassegna le questioni che essa porta all'attenzione del giurista. Prenderò invece una scorciatoia, soffermandomi su quella che appare l'ultima frontiera del tema in discussione. Il riferimento è al *Trusted Computing* (TC). "Trusted Computing" è una delle molteplici (cangianti) espressioni usate per denominare il coordinamento di alcune iniziative che fanno capo ad imprese leader del settore dell'hardware e del software. Il nucleo iniziale di queste iniziative risiedeva nella *Trusted Computing Platform Alliance* (TCPA) fondata da Compaq, HP, IBM, Intel e Microsoft. I compiti della TCPA sono stati poi assorbiti ed ampliati dal *Trusted Computing Group* (TCG), un'organizzazione no profit promossa da sette imprese (le cinque fondatrici della TCPA più Sony

Corporation e Sun Microsystems, Inc.)[1].

Nella presentazione sul sito Web di riferimento si legge che il TCG è un'organizzazione no profit costituita allo scopo di sviluppare, definire e promuovere [specifiche per] standard aperti di hardware con funzioni di *Trusted Computing* e di tecnologie per la sicurezza, che comprendono componenti hardware e interfacce software per differenti piattaforme, periferiche e dispositivi [quali computer, palmari e cellulari]. Le specifiche TCG sono destinate a creare ambienti informatici più sicuri di quelli attuali senza compromettere l'integrità funzionale [dei sistemi informatici], la privacy ed i diritti individuali. Lo scopo principale è quello di aiutare gli utenti a proteggere il proprio patrimonio di informazioni sia dagli attacchi compiuti mediante software sia dagli attacchi fisici[2].

Il TC si presenta dunque come un approccio assolutamente innovativo alla sicurezza informatica. L'obiettivo non è quello di produrre nuovi strumenti software (come antivirus, *antispyware* e *firewall*) di reazione ad attacchi ai sistemi informatici ed utilizzi impropri dei computer o delle reti, ma al contrario di promuovere la costruzione di sistemi hardware e software non abilitati a determinate funzioni potenzialmente in grado di comprometterne la sicurezza, nonché di promuovere il controllo – attraverso Internet – del rispetto delle limitazioni di funzionalità da parte degli utenti dei sistemi.

I principali produttori di microprocessori (Intel e AMD) si stanno muovendo velocemente verso l'incorporazione di specifiche TC nei propri apparecchi. Si pensi in particolare all'Intel LaGrande Technology[3]. D'altra parte, anche la Microsoft va nella stessa direzione. In questa prospettiva si spiega l'azione volta a sviluppare la Next-Generation Secure Computing Base (NGSCB)[4], prima nota

[1] V. il sito Web: https://www.trustedcomputinggroup.org

[2] V. l'URL: https://www.trustedcomputinggroup.org/about/

[3] V. il sito Web: http://www.intel.com/technology/security/

[4] V. il sito Web: http://www.microsoft.com/resources/ngscb/default.mspx

come Palladium, destinata ad essere incorporata nella prossima generazione di Windows, denominata inizialmente "Longhorn" e da ultimo "Vista". Insomma la NGSCB costituisce una delle possibili e delle più importanti – stante la posizione di Microsoft sul mercato informatico – applicazioni del TC[5]. Persino Linux nelle sue ultime versioni incorpora funzionalità TC[6]. In sintesi, a partire dal 2004, vi è una diffusa tendenza da parte dei produttori di hardware e degli sviluppatori a convergere verso l'architettura TC[7].

La logica sottesa al TC è quella del "prevenire è meglio che punire". Si tratta di una logica che può preoccupare il giurista.

Nel racconto fantascientifico intitolato "Minority Report" (in italiano: "Rapporto di minoranza") il genio visionario di Philip Dick racconta di un futuro nel quale il connubio tra mutazioni genetiche

[5] V. il sito Web: http://www.microsoft.com/resources/ngscb/default.mspx

Sulla sostanziale convergenza di NGSCB e standard elaborati dal TCG v. S. SCHOEN, *Trusted Computing: Promise and Risk*, (reperibile all'URL: http://www.eff.org/ Infrastructure/trusted_computing/20031001_tc.php), il quale rileva che "[w]hile these projects are still distinct, it is reasonable to speak of a single 'trusted computing architecture' toward which both projects are headed. (Only a portion of this architecture is described by the most recently published TCG specification, and, as TCG notes, additional software will be required to make use of many of these features.) Less well known trusted computing projects under development by processor vendors (and TCG members) Intel and AMD may fill in some of the gaps between what TCG has so far specified and what NGSCB would require. Intel's LaGrande Technology (LT) and AMD's Secure Execution Mode (SEM), for example, provide hardware support needed for all the major feature groups in NGSCB. The Intel and AMD projects are not discussed as separate entities here, but their features would build on TCG features to provide the hardware support demanded by NGSCB. One important similarity between the NGSCB design and the existing TCG specification is that both contain a 'remote attestation' feature, which we will criticize extensively below. Even though there are differences between Microsoft's and TCG's technical descriptions of remote attestation, both can, given proper operating system support, be used in functionally equivalent ways".

[6] V. la voce *Trusted computing* della versione inglese di Wikipedia all'URL: http://en.wikipedia.org/wiki/Trusted_computing

[7] V. la voce *Trusted computing* della versione inglese di Wikipedia all'URL: http://en.wikipedia.org/wiki/Trusted_computing

degli uomini e computer conferisce alla polizia il potere di conoscere in anticipo la commissione di un crimine, consentendo in questo modo di usare la forza repressiva prim'ancora che il reato venga consumato[8]. Il giudizio prognostico (o, nella terminologia di Dick, "precognitivo") sulla commissione del delitto si basa su un meccanismo che fa leva sulle premonizioni di tre esseri umani geneticamente mutati – i "precog" – e sulle macchine (computer). Questo giudizio prognostico può basarsi sulla completa convergenza delle premonizioni, oppure molto più frequentemente su due premonizioni (che vedono il delitto) ed una invece dissonante (il "rapporto di minoranza" appunto). La morale del racconto sembra risiedere nella ferma condanna della repressione preventiva, vista come potere conferito dal progresso tecnologico. La conclusione del racconto è pessimista: il protagonista, comandante della sezione specializzata della polizia che si occupa della repressione preventiva – Precrimine –, viene a sapere di essere accusato dalle premonizioni di un futuro omicidio, ma successivamente scopre un (veritiero?) rapporto di minoranza che lo assolve. Tuttavia, per non screditare (e consegnare allo smantellamento) la sua polizia, decide di commettere ugualmente l'omicidio per confermare il rapporto di maggioranza.

La logica del TC è simile a quella delle macchine premonitrici di Dick: invece di intervenire *ex post*, si crea *ex ante* un ambiente sicuro. Nel caso del TC si tratta "solo" di un ambiente digitale, un ambiente *trusted* ("fidato" o "sicuro") che diminuisce o addirittura azzera il rischio di attacchi ai sistemi informatici o "utilizzi impropri" del computer. Però, come nell'inquietante futuro di Dick, la sicurezza è ottenuta al prezzo della compressione della libertà delle persone. Infatti alla base della logica del TC vi è la limitazione delle funzionalità e la dislocazione del controllo del

[8] P. K. DICK, *Rapporto di minoranza*, in P. K. DICK, *Rapporto di minoranza e altri racconti*, Roma, 2002, 27.

computer dall'utente a chi gestisce la sicurezza informatica. Il fatto che nel caso dell'ambiente digitale sia in gioco "solo" la sicurezza informatica non deve rassicurare. Il computer è sempre più uno strumento nel quale proiettiamo quelle attività quotidiane (come l'ascolto di una musica e la visione di un film o come la raccolta di dati personali) che presuppongono libertà fondamentali (quali la libertà di pensiero e di autodeterminazione). Inoltre, l'approccio TC alla sicurezza informatica pone due problemi di fondo che sono assai rilevanti sul piano giuridico:

a) l'elaborazione degli standard tecnologici dell'architettura TC (così come la gestione della sicurezza sui cui si basa il TC) è nelle mani di privati i quali non necessariamente procedono in base a processi trasparenti o democratici;

b) la sicurezza dipende dall'architettura informatica la quale incorpora non diversamente dalle architetture fisiche alcune regole implicite le quali sono rigide, predeterminate e potenzialmente infallibili; mentre il diritto per sua natura è fatto di regole elastiche, verificate *ex post* e sempre potenzialmente fallibili (per tornare alla metafora dickiana: nel diritto quel che oggi è un'opinione di minoranza può trasformarsi domani in opinione di maggioranza).

Su questi ed altri problemi conviene soffermarsi. A questo scopo il ragionamento si articola come segue. Nel paragrafo 2 si descrivono i tratti fondamentali del TC, nel paragrafo 3 si mette in evidenza come il TC sia un'architettura digitale che limitando preventivamente le funzionalità del sistema informatico e dislocando il suo controllo dall'utente ad altri soggetti pone serie minacce alla privacy dello stesso utente, nel paragrafo 4 si discute della compatibilità della dislocazione del controllo del sistema informatico con i principi della normativa comunitaria in materia di protezione dei dati personali, nel paragrafo 5 si traggono alcune brevi conclusioni.

2. Lineamenti essenziali del Trusted Computing

Nell'ambito informatico, l'espressione *trusted system* (traducibile approssimativamente con "sistema fidato" o "sistema sicuro") è usata in varie accezioni. Secondo una prima accezione che deriva dall'ingegneria della sicurezza, un sistema si definisce "trusted" quando si è costretti a farvi affidamento[9]. Il fallimento di un *trusted system* mette a rischio l'intera politica sicurezza[10].

[9] V. la voce *Trusted systems* della versione inglese di Wikipedia (all'URL: http://en.wikipedia.org/wiki/Trusted_system) nella quale si legge: "[i]n security engineering, a trusted system is a system that you have no choice but to trust. The failure of a trusted system will compromise security. In general, the number of trusted components in a system should be minimized".

[10] Su questa accezione di "trusted" v. R. ANDERSON, *'Trusted Computing' Frequently Asked Questions*, versione 1.1 2003 (agosto), disponibile all'URL: http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html, secondo il quale: "[i]t's almost an in-joke. In the US Department of Defense, a 'trusted system or component' is defined as 'one which can break the security policy'. This might seem counter-intuitive at first, but just stop to think about it. The mail guard or firewall that stands between a Secret and a Top Secret system can – if it fails – break the security policy that mail should only ever flow from Secret to Top Secret, but never in the other direction. It is therefore trusted to enforce the information flow policy. Or take a civilian example: suppose you trust your doctor to keep your medical records private. This means that he has access to your records, so he could leak them to the press if he were careless or malicious. You don't trust me to keep your medical records, because I don't have them; regardless of whether I like you or hate you, I can't do anything to affect your policy that your medical records should be confidential. Your doctor can, though; and the fact that he is in a position to harm you is really what is meant (at a system level) when you say that you trust him. You may have a warm feeling about him, or you may just have to trust him because he is the only doctor on the island where you live; no matter, the DoD definition strips away these fuzzy, emotional aspects of 'trust' (that can confuse people). During the late 1990s, as people debated government control over cryptography, Al Gore proposed a 'Trusted Third Party' – a service that would keep a copy of your decryption key safe, just in case you (or the FBI, or the NSA) ever needed it. The name was derided as the sort of marketing exercise that saw the Russian colony of East Germany called the 'German Democratic Republic'. But it really does chime with DoD thinking. A Trusted Third Party is a third party that can break your security policy".

Secondo un'altra accezione – più vicina a quella utilizzata anche nella *policy analysis*[11] – un sistema è reso "trusted" dal fatto che l'hardware ed il software sono obbligati ad operare secondo "regole" predeterminate[12]. Questa seconda accezione identifica la sicurezza o l'affidabilità con la limitazione preventiva di funzionalità del sistema, in quanto il rischio maggiore deriverebbe dalla libertà d'azione gli agenti (persone o software)[13]. In termini rovesciati: un

[11] V. la definizione contenuta nella pagina di presentazione del "Trusted Systems Project" (http://trusted-systems.info/), nella quale si legge: "[t]rusted systems for purposes of this research are systems in which some conditional prediction about the behavior of people or objects within the system has been determined prior to authorizing access to system resources. For example, trusted systems include the use of 'security envelopes' in national security and counterterrorism applications, 'trusted computing' initiatives in technical systems security, and the use of identity or credit scoring systems in financial and anti-fraud applications; in general, they include any system (i) in which probabilistic threat or risk analysis is used to assess 'trust' for decision-making before authorizing access or for allocating security resources against likely threats (including their use in the design of systems constraints to control behavior within the system), or (ii) in which deviation analysis or systems surveillance is used to insure that behavior within systems complies with expected or authorized parameters".

[12] Cfr. M. STEFIK, *Shifting the Possible: How Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 *Berkeley Tech. L.J.* 138 (1997), p. 2 della versione in formato pdf (disponibile all'URL: http://btlj.boalt.org/data/articles/12-1_spring_1997_symp_6-stefik.pdf). Sulle implicazioni giuridiche dell'idea dei *trusted systems* elaborate da Stefik v. J. WEINBERG, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 *Stan. L. Rev.* 1251 (2000); J. ZITTRAIN, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 *Stan. L. Rev.* 1201 (2000); L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999, 129; M. GIMBEL, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property*, 50 *Stan. L. Rev.* 1671 (1998).

[13] Secondo D. KUHLMANN, R. A. GEHRING, *Trusted Platforms, DRM, and Beyond*, in E. BECHER, W. BUSHE, D. GÜNNEVIG, N. RUMP (eds.), *Digital Rights Management. Technological, Economic, Legal and Political Aspects*, Berlin, 2003, 178, 187-190, quella formalizzata da Stefik è solo una recente concezione dei *trusted systems*. In realtà l'idea dei *trusted systems* affonderebbe le sue radici in ricerche militari condotte dagli Stati Uniti negli anni '60. Lo sviluppo dei *Trusted Computer System Evaluation Criteria* (TCSEC) dal 1983 al 1999, conosciuto anche

sistema informatico è insicuro se gli agenti possono controllarlo e modificarlo liberamente.

A questa visione dei *trusted systems* rispondono sia i sistemi di *Digital Rights Management* (DRM)[14], cioè quelle architetture informatiche finalizzate a mettere le imprese nella condizione di poter distribuire in forma protetta i propri contenuti predeterminando dove come e quando gli stessi possono essere fruiti (ad esempio, si può decidere di distribuire un file musicale che può essere ascoltato solo 10 volte, o può essere letto solo con alcuni apparecchi, o ancora che può funzionare solo in una determinata zona geografica), sia il *Trusted Computing* (TC)[15].

Attualmente il TC risponde alla seguente logica[16]. Un

---

sotto il nome di *Orange Book*, rappresenterebbe il culmine di queste risalenti ricerche.

[14] Sui profili giuridici del DRM v., nella letteratura italiana, R. CASO, *Digital rights management – Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004 (ristampa digitale, Trento, 2006, scaricabile all'URL: http://www.jus.unitn.it/users/caso/pubblicazioni/drm/home.asp?cod=roberto.caso).

[15] Sui nessi tra DRM e TC v. CASO, *Digital rights management – Il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 44; R. ROEMER, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, *UCLA J. L. Tech.* 8 (2003); S. BECHTOLD, *The Present and Future of Digital Rights Management. Musings on Emerging Legal Problems*, in BECHER, BUSHE, GÜNNEVIG, RUMP (eds.), *Digital Rights Management. Technological, Economic, Legal and Political Aspects*, cit., 597 (versione in formato pdf disponibile all'URL: http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf); KUHLMANN, GEHRING, *Trusted Platforms, DRM, and Beyond*, cit., 187 ss.

[16] La logica di base del TC vien fatta solitamente risalire a W. A. ARBAUGH, D. J. FARBER, J. M. SMITH, *A Secure and Reliable Bootstrap Architecture*, in *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, 1997, 65, disponibile all'URL: http://www.cs.umd.edu/~waa/pubs/oakland97.pdf

Sull'influenza dell'articolo Arbaugh, Farber e Smith v. ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.: "[t]he TC concept of booting a machine into a known state is implicit in early PCs where the BIOS was in ROM and there was no hard drive in which a virus could hide. The idea of a trusted bootstrap mechanism for modern machines seems to have first appeared in a paper

sistema è sicuro o affidabile se il suo hardware ed il suo software sono concepiti e costruiti in modo da essere costretti a funzionare nel modo voluto dai produttori e non dagli utenti finali.

Dunque il primo fondamento di questa logica sta nella limitazione preventiva delle funzionalità del sistema informatico. L'enfasi deve esse posta sul fatto che si tratta di limitazioni non solo logiche, ma anche fisiche, in quanto riguardano l'hardware[17]. Si tratta di uno dei tanti approcci alla sicurezza informatica, che parte dalla constatazione della notevole vulnerabilità dei computer attuali proni di fronte ad attacchi esterni (come i virus) ed utilizzi impropri.

---

by Bill Arbaugh, Dave Farber and Jonathan Smith, 'A Secure and Reliable Bootstrap Architecture', […]. It led to a US patent: 'Secure and Reliable Bootstrap Architecture', U.S. Patent No. 6,185,678, February 6th, 2001. Bill's thinking developed from work he did while working for the NSA on code signing in 1994, and originally applied to rebooting ATM switches across a network. The Microsoft folk have also applied for patent protection on the operating system aspects. (The patent texts are here and here.) There may be quite a lot of prior art. Markus Kuhn wrote about the TrustNo1 Processor years ago, and the basic idea behind a trustworthy operating system – a 'reference monitor' that supervises a computer's access control functions – goes back at least to a paper written by James Anderson for the USAF in 1972. It has been a feature of US military secure systems thinking since then".

[17] S. SCHOEN, *Trusted Computing: Promise and Risk*, 2003, disponibile su EFF all'URL: http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php: "[t]here is a widespread perception that personal computer security is in an unfortunate state and that something must be done to fix it. There are many promising approaches to improving security – redesigning operating systems, changing programming methodologies, or altering the PC's hardware itself. It is well known that a comprehensive defense against the security threats faced by PC users will involve several approaches, not just one. An insecure system can't magically become 'secure' with the addition of a single piece of technology. Changes to the design of PC hardware are one useful tool among many for improving security. While hardware changes aren't a prerequisite for increased security, they're undeniably helpful – for example, by providing a way to store private keys (and therefore the private documents protected by those keys) safely. One family of projects to add security to PCs through hardware changes is known as 'trusted computing'".

Il secondo fondamento della logica TC sta nella dislocazione del controllo del sistema informatico dall'utente finale a chi produce l'hardware ed il software, nonché a chi è deputato a sorvegliare che siano rispettate le limitazioni di funzionalità imposte dal produttore. Sotto quest'ultimo profilo, il sistema è monitorato (attraverso la rete Internet) allo scopo di verificare che funzioni secondo le "regole" prestabilite dai produttori[18].

Esula dall'ambito di questo scritto un'analisi approfondita dei profili tecnici del TC. Tuttavia, è necessario offrire una spiegazione semplificata dei lineamenti essenziali di questa architettura informatica.

L'ingrediente di base del TC è rappresentato dalla crittografia digitale. La crittografia è lo studio delle tecniche utilizzate per trasformare un testo leggibile (c.d. testo in chiaro) in crittogramma (processo che viene detto anche "crittazione" o "cifratura") e viceversa (processo che viene detto anche "decrittazione" o "decifratura")[19], uno studio che fa leva su una storia millenaria[20]. Nell'era digitale l'utilizzo della crittografia è diventato pervasivo, ponendo anche complessi problemi giuridici[21].

---

[18] ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.

[19] Il formulario utilizzato per rendere illeggibile il testo e per effettuare l'operazione inversa (cioè, mettere in chiaro il testo precedentemente reso illeggibile) è detto "cifrario".

[20] Per una guida alla crittografia v. W. STALLINGS, *Crittografia e sicurezza delle reti. Standard, tecniche, applicazioni*, Milano, 2004.

[21] Cfr. L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999, 35-36, secondo il quale "here is something that will sound very extreme but is at most, I think, a slight exaggeration: encryption technologies are the most important technological breakthrough in the last thousand years. No other technological discovery – from nuclear weapons (I hope) to the Internet – will have more significant impact on social and political life. Cryptography will change everything. […] Cryptography is Janus-faced: it has an ambiguous relationship to freedom on the Internet. As Stewart Baker and Paul Hurst put it, cryptography 'surely is the best of technologies and the worst of technologies. It will stop crimes and it will create new crimes. It will undermine dictatorships, and it will drive them to new excesses.

Posto che non esistono sistemi crittografici assolutamente inviolabili, si pone il problema di misurare il grado di (relativa) sicurezza di una determinata tecnologia crittografica. Esiste poi un *trade off* tra sicurezza e praticabilità della crittografia, nel senso che sistemi crittografici molto affidabili possono essere costosi e difficili da utilizzare. Sul piano della sicurezza, tra i molti parametri che vengono utilizzati per valutare il grado di resistenza di un algoritmo di crittografia ve ne sono due ritenuti preminenti:

a) il tempo necessario a risolvere (in gergo informatico: rompere, "to crack") il sistema crittografico, cioè quello che viene anche definito "forza bruta" (ad esempio, le c.d. chiavi crittografiche di accesso, cioè i codici che servono a decifrare il contenuto digitale, sono maggiormente sicure quando sono lunghe e presentano sequenze di simboli differenti, come numeri misti a lettere)[22];

b) il grado di esposizione dell'algoritmo a forme di analisi che rendono non necessario il ricorso alla forza bruta[23].

It will make all anonymous, and it will track our every transaction'".

Nella letteratura giuridica italiana v. G. ZICCARDI, *Crittografia e diritto*, Torino, 2003.

[22] Cfr. B. ROSENBLATT, B. TRIPPE, S. MOONEY, *Digital Rights Management. Business and Tecnology*, New York, 2002, 91 ss. La lunghezza della chiave rappresenta il numero di chiavi possibili in un sistema crittografico. In termini binari, se la chiave si basa su N bit, il numero delle possibili chiavi è 2 all'ennesima potenza. Ad esempio, una chiave di lunghezza 20 dà 2^{20}, cioè 1.048.576 di possibili chiavi.

Il protocollo Secure Socket Layer (SSL) si basa su chiavi a 128 bit. Una chiave a 128 bit è 309.485.009.821.345.068.724.781.056 (2^{88}) più forte di una chiave a 40 bit che si basa sul medesimo algoritmo.

[23] Il profilo della sicurezza si interseca con il carattere segreto o pubblico delle procedure che generano il sistema di crittografia. Molti studiosi di crittografia ritengono che l'unico modo per valutare la sicurezza di una data tecnologia sia quello di analizzare le procedure sulle quali essa si basa (l'atteggiamento dei crittografi si basa sul c.d. principio di Kerckhoffs, in base al quale la sicurezza di un sistema di crittografia non dovrebbe fondarsi sulla segretezza dell'algoritmo, ma sulla segretezza delle chiavi: v., nella letteratura giuridica, ZICCARDI, *Il diritto d'autore dell'era digitale*, Milano, 2001, 174). In generale, più il sistema

Nel panorama attuale, la tecnica basata sugli algoritmi a chiavi asimmetriche, detta anche crittografia a *Public Key Infrastructure* (PKI), è quella che offre il migliore compromesso tra sicurezza e praticabilità[24]. Il sistema è detto asimmetrico perché è basato su una coppia di chiavi: una privata (destinata a rimanere segreta e custodita) e l'altra pubblica (destinata ad essere diffusa)[25]. Dati cifrati con una determinata chiave pubblica possono essere decifrati solo con la corrispondente chiave privata e viceversa (cioè, dati cifrati con una determinata chiave privata possono essere decifrati solo con la corrispondente chiave pubblica). Il sistema è altamente sicuro in quanto è "virtualmente" impossibile ricavare la chiave privata da quella pubblica[26]. La crittografia a chiavi asimmetriche combinata con altre tecnologie – il riferimento è in particolare all'algoritmo di hash – è poi in grado di consentire la creazione di firme digitali (qui intese in senso informatico).

---

crittografico è ritenuto resistente, più è sottoposto a verifiche della comunità scientifica ed attacchi di soggetti indipendenti. Ciò ha un riflesso sul mercato della crittografia, poiché solo sistemi che si basano su algoritmi pubblici e sottoposti a scrutinio dovrebbero essere appetibili.

[24] L'implementazione del sistema a chiavi asimmetriche si basa in particolare sull'algoritmo RSA (acronimo che richiama le iniziali dei cognomi degli ideatori dell'algoritmo: Ronal Rivest, Adi Shamir, e Leonard Adleman). Ma l'intuizione originaria si deve agli studi di Whitfield Diffie e Martin Hellman volti a superare i limiti dei sistemi a chiavi simmetriche (per le prime informazioni v. ROSENBLATT, TRIPPE, MOONEY, *Digital Rights Management. Business and Technology*, cit., 94).

[25] Molte delle applicazioni commerciali attualmente in uso, che si fondano sull'algoritmo RSA, fanno leva su chiavi a 1024 bit. Tuttavia, la sicurezza di tali applicazioni non può essere misurata solo in termini di forza bruta. Esistono metodologie che riducono la grandezza del numero di tentativi astrattamente necessari a violare una chiave a 1024 bit (cfr. ROSENBLATT, TRIPPE, MOONEY, *Digital Rights Management. Business and Technology*, cit., 95).

[26] Il sistema è solo altamente sicuro ma non assolutamente sicuro, in quanto sono necessarie immense capacità di calcolo per ricavare la chiave privata da quella pubblica. Tuttavia, com'è noto le capacità di calcolo di computer crescono velocemente ed inoltre è sempre più agevole moltiplicare le capacità computazionali mediante il calcolo distribuito di macchine connesse in rete.

L'esistenza di un ente, la *Certification Authority* (CA), che certifica la corrispondenza univoca tra chiave pubblica e chiave privata consente di generare *trust* ("fiducia") circa le seguenti finalità:

- segretezza dei dati;
- integrità dei dati;
- identificazione di hardware, software e dati, nonché di soggetti (anche persone fisiche)[27].

Al fine di rendere operative queste finalità, l'architettura TC deve far leva sull'interazione di tre elementi: l'hardware, il software e l'infrastruttura (PKI) per la gestione della certificazione crittografica[28].

La componente hardware fondamentale dell'architettura è rappresentata dal *Trusted Platform Module* (TPM) un microchip che svolge funzioni crittografiche[29]. Nel TPM infatti vengono generati e

[27] Nella letteratura giuridica v., per tutti, A. M. FROOMKIN, *The essential Role of Trusted Third parties in Electronic Commerce*, 75 *Or. L. Rev.* 49 (1996).

[28] V. KUHLMANN, GEHRING, *Trusted Platforms, DRM, and Beyond*, cit., 182 ss. Come rilevato da R. A. GHERING, *Trusted Computing for Digital Rights Management*, in *Indicare Monitor*, vol. 2, 2006, 387, 389, disponibile all'URL: http://www.indicare.org/tiki-download_file.php?fileId=178; attualmente le specifiche TCG riguardano i seguenti elementi:

- infrastruttura;
- PC Client;
- Trusted Platform Module (TPM);
- Trusted Network Connect (TNC);
- TPM Software Stack (TSS);
- Server Specific.

[29] Secondo i documenti ufficiali del TCG (v. il documento intitolato *Embedded Systems and Trusted Computing Security* disponibile all'URL: https://www.trustedcomputinggroup.org/groups/tpm/embedded_bkgdr_final_sept_14_2005.pdf): "[t]he basis of Trusted Computing is the Trusted Platform Module, or TPM. The TPM is a small piece of silicon affixed in a device. It securely stores digital keys, certificates and passwords and is more difficult to attack virtually or physically. TPM functions include:

- Asymmetric key functions for on-chip key pair generation using a hardware random number generator; private key signatures; and public key encryption and

custoditi i certificati, le password e le chiavi crittografiche. Tra le chiavi crittografiche riveste una fondamentale importanza la c.d. *Endorsement Key* che è finalizzata ad identificare il TPM come originale (cioè non manipolato o contraffatto)[30].

---

private key decryption of keys enable more secure storage of files and digital secrets. This is accomplished through hardware-based protection of (1) the symmetric keys associated with software-encrypted files (data, passwords, credit card numbers, etc.) and (2) private keys used for digital signatures. This includes use of the TPM random number generator to create keys and performance of operations on private keys created by the TPM (digital signatures, public key encryption for storage, decryption) in the TPM. Private keys created in the TPM are protected by the TPM even when in use.

- Secure storage of HASH values representing platform configuration information in Platform Control Registers (PCRs) and secure reporting of these values, as authorized by the platform owner. These features allow and enable verifiable attestation of the platform configuration based on the chain of trust used in creating the HASH values. This includes creation of Attestation Identity Keys (AIKs) that cannot be used unless a PCR value is the same as it was when the AIK was created.

- An Endorsement Key which can be used by an owner to anonymously establish that identity keys were generated in a TPM, thus enabling confirmation of the quality of the key without identifying which TPM generated the identity key.

- Initialization and management functions that allow the owner to turn functionality on and off, reset the chip, and take ownership, with strong controls to protect privacy. The system owner is trusted and must opt-in. The user, if different from the owner, may opt-out if desired.

An Endorsement Credential, in conjunction with Conformance and Platform Credentials, can be used, as authorized by the owner, to create Attestation Identity Key (AIK) Credentials that can be attested to by a certificate authority. TCG specifications describe the creation of these credentials in order to enable their use, but TCG will not issue credentials itself".

[30] V. il documento del TCG intitolato *TCG Specification Architecture Overview - Specification Revision 1.2*, 28 April 2004, disponibile all'URL: https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf: "TPMs can be shipped with an embedded key called the Endorsement Key (EK). The EK is used in a process for the issuance of AIK credentials and to establish a platform owner. The platform owner can create a storage root key. The storage root key in turn is used to wrap other TPM keys". Secondo il glossario del TCG (all'URL: https://www.trustedcomputinggroup.org/groups/glossary/) l'*Endorsement Key* è una "an RSA Key pair composed of a public key (EKpu) and private (EKpr). The EK is

Le componenti software sono destinate ad essere incorporate sia nel sistema operativo sia nel BIOS (cioè nel firmware)[31], al fine di interagire con il TPM e attivare il processo di verifica ("Attestation") dell'integrità del sistema informatico[32]. Questo processo è innescato ad ogni avvio ("boot") del computer o di altra piattaforma (ad esempio un telefono cellulare) che risponda agli standard TC[33].

---

used to recognize a genuine TPM. The EK is used to decrypt information sent to a TPM in the Privacy CA and DAA protocols, and during the installation of an Owner in the TPM".

[31] KUHLMANN, GEHRING, *Trusted Platforms, DRM, and Beyond*, cit., 184.

[32] V. *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[a] TPM can be used to ensure that each computer will report its configuration parameters in a trustworthy manner. Platform boot processes are augmented to allow the TPM to measure each of the components in the system (both hardware and software) and securely store the results of the measurements in Platform Configuration Registers (PCR) within the TPM. Emergency response personnel can use these measurements to determine which computers are vulnerable to virus attacks. IT managers may install system processes that use the PCR values in a TPM to identify unsafe configurations at system boot thereby preventing inadvertent network connection while in an unsafe mode".

[33] V. il documento TCG intitolato *Trusted Platform Modules Strengthen User and Platform Authenticity*, gennaio 2005, reperibile all'URL: https://www.trustedcomputinggroup.org/specs/TPM/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf: "[o]ne frequent system attack involves making unauthorized changes to a platform's configuration. This allows misuse of the device and its contents as well as access to the networks to which the device is connected. In devices that use TPM chips, platform integrity is protected by secure storage of the platform configuration values and by secure reporting of the values. This enables attestation of the device by verifying that its configuration is intact. The mechanism is based on the chain of trust used in creating the hash values of the pre-boot information of the platform. It is common industry practice to check the integrity of a platform by comparing configuration settings when a platform is rebooted against the settings when it was set up. A 'hash' algorithm is used to calculate a value from information stored in the Platform Configuration Registers (PCRs) when the platform is setup. When the platform is re-booted, a new hash value is calculated and compared against the original. If the values match, the computer or cell phone or other platform starts up and login proceeds. In unprotected systems, PCRs are accessible and the hash values are stored in system

L'infrastruttura è basata su una PKI ed in particolare su un soggetto (*Certification Authority*), il quale, mediante la gestione di chiavi, firme digitali e certificati, è in grado di svolgere la funzione di "attestazione" dell'integrità del sistema[34].

Nell'architettura TC l'interazione dei tre elementi ora sommariamente descritti serve a rendere operative alcune funzioni di sicurezza e a limitare altre funzioni che sono normalmente

memory that is subject to compromise. In TPM-capable platforms, the hash value is calculated using the SHA-1 algorithm, access to the PCRs requires trusted authorization, and the hash values are stored within the TPMs in secure, non-volatile memory. These values are used to create Attestation Identity Keys (AIKs) that cannot be used unless a hash value is the same at the time of use as when the AIK was created. This makes it possible to determine if trusted-state configuration parameters are corrupted. If they are corrupted, use of the device may be denied".

[34] V. *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[a]ttestation is the process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. All forms of attestation require reliable evidence of the attesting entity. Attestation can be understood along several dimensions, attestation by the TPM, attestation to the platform, attestation of the platform and authentication of the platform. Attestation by the TPM is an operation that provides proof of data known to the TPM. This is done by digitally signing specific internal TPM data using an attestation identity key (AIK). The acceptance and validity of both the integrity measurements and the AIK itself are determined by a verifier. The AIK is obtained using either the Privacy CA or via a trusted attestation protocol. Attestation to the platform is an operation that provides proof that a platform can be trusted to report integrity measurements; performed using the set or subset of the credentials associated with the platform; used to issue an AIK credential. Attestation of the platform is an operation that provides proof of a set of the platform's integrity measurements. This is done by digitally signing a set of PCRs using an AIK in the TPM. Authentication of the platform provides evidence of a claimed platform identity. The claimed identity may or may not be related to a user or any actions performed by the user. Platform Authentication is performed using any non-migratable signing key. Certified keys (i.e. signed by an AIK) have the added semantic of being attestable. Since there are an unlimited number of non-migratable keys associated with the TPM, there are an unlimited number of identities that can be authenticated".

riconducibili alla malleabilità della parte logica (software) del computer. La letteratura che si riferisce agli attuali sviluppi delle applicazioni TC individua le seguenti funzioni come le più rilevanti[35].

a) "Secure Input/Output" o "Secure Paths to the User": mediante questa funzione è possibile evitare che appositi software possano intercettare i dati che viaggiano dalle periferiche hardware (come la tastiera) al processo svolto dal computer (questa funzione per esempio neutralizza programmi come i *keyboard loggers* in grado di intercettare le sequenze di caratteri digitate sulla tastiera allo scopo, per esempio, di appropriarsi di password)[36];

b) "Memory Curtaining" o "Strong Process Isolation": questa funzione consente di proteggere una zona della memoria volatile (RAM) in modo da evitare che appositi software possano accedere ad essa (ad esempio, se il sistema operativo è compromesso da un virus, questa funzione impedisce al virus di accedere ai dati processati dalla zona sicura della memoria)[37];

---

[35] Le funzioni elencate sono solo quelle principali e si ricavano oltre che dalle specifiche TC anche dalla applicazione che ne fa Microsoft nella sua NGSCB. V. SCHOEN, *Trusted Computing: Promise and Risk*, cit.; C. FLICK, *The Controversy of Trusted Computing*, 2004, disponibile all'URL: http://luddite.cst.usyd.edu.au/~liedra/misc/Controversy_Over_Trusted_Computing.pdf; ROEMER, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, cit.

[36] Cfr. il documento Intel intitolato *LaGrande Technology Architectural Overview*, settembre 2003: "Protected Input: [p]rovides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments from being observed or compromised by any other unauthorized software running on the platform. For USB input, LT does this by cryptographically encrypting the keystrokes and mouse clicks with an encryption key shared between a protected domain's input manager and an input device. Only applications that have the correct encryption key can decrypt and use the transported data".

[37] Cfr. *LaGrande Technology Architectural Overview*, cit.: "Protected Execution: [p]rovides applications with the ability to run in isolated protected

c) "Sealed Storage": tramite questa funzione è possibile proteggere i dati riservati registrati sulle memorie non volatili (in particolare sull'hard disk) in modo che possano essere letti solo da quello stesso computer (o meglio da quella stessa combinazione di hardware e software)[38];

d) "Remote Attestation" o "Attestation": mediante questa funzione – alla quale già si è accennato sopra – è possibile verificare eventuali cambiamenti nello stato di "sicurezza" o "integrità" del computer nonché dei dati in esso contenuti e dunque evitare che appositi software (ad esempio, virus) possano intaccare quello stato; in altri termini, questa funzione permette all'utente o ad altri soggetti che siano collegati al computer tramite rete di comparare lo stato attuale dello stesso computer con quello predefinito come sicuro o integro[39]. Alla funzione di *attestation* si riconnette quella di *secure boot* (avviamento sicuro) mediante la quale il sistema verifica il proprio stato di sicurezza al momento dell'avvio[40].

---

execution environments such that no other unauthorized software on the platform can observe or compromise the information being operated upon. Each of these isolated environments has dedicated resources that are managed by the processor, chipset and OS kernel".

[38] Cfr. *LaGrande Technology Architectural Overview*, cit.: "Sealed storage: [p]rovides for the ability to encrypt and store keys, data or other secrets within hardware on the platform. It does this in such a way that these secrets can only be released (decrypted) to an executing environment that is the same as when the secrets were encrypted. This helps prevent attacks exploiting the vulnerability where the encrypted data has been transferred to other platforms either for normal use (thereby become decrypted) or for malicious attack".

[39] Cfr. *LaGrande Technology Architectural Overview*, cit.: "Attestation: [e]nables a system to provide assurance that the LT protected environment was correctly invoked. It also provides the ability to provide a measurement of the software running in the protected space. The information exchanged during an attestation function is called an Attestation Identity Key credential and is used to help establish mutual trust between parties".

[40] Cfr. *LaGrande Technology Architectural Overview*, cit.: "Protected Launch: [p]rovides for the controlled launch and registration of the critical OS and system software components in a protected execution environment"; nonché la pagina Web

Per dare l'idea di queste funzioni si faccia il caso della compilazione e memorizzazione, mediante il computer TC, di un diario privato[41]. La funzione *sub* a) garantisce che il contenuto del diario non venga intercettato nel momento in cui si digitano le parole sulla tastiera, quella *sub* b) fa in modo che il diario venga protetto da eventuali attacchi nel momento in cui si sta operando con il software di scrittura, quella *sub* c) assicura che il diario non possa essere alterato dal momento in cui è archiviato sull'*hard disk*, ed infine quella *sub* d) abilita solo il computer (o meglio solo la combinazione di hardware e software giudicata sicura) che ha generato il diario a modificarlo ed impedisce altresì che il file contenente il diario possa essere modificato anche quando sia processato su un altro computer.

La funzione *sub* d) cioè quella di *remote attestation* riveste un'importanza cruciale nella logica TC – non a caso è stato sopra definito come il secondo fondamento della logica TC – ed è fra quelle che pongono i problemi giuridici di maggiore rilievo. Infatti la funzione di "Remote Attestation" implica un collegamento a Internet e lo scambio dei dati crittografici (chiavi crittografiche e certificati) ai quali sono associabili e normalmente associati dati personali.

Gli scenari dell'utilizzo di architetture TC sono numerosi. Lo stesso TCG indica in via esemplificativa i seguenti possibili utilizzi:

- la gestione delle risorse informatiche e dei rischi a cui esse sono esposte (rischi come la perdita accidentale o il furto di dati di

---

del sito di Microsoft dedicata NGSCB (all'URL: http://www.microsoft.com /resources/ngscb/default.mspx): "[o]ur first delivery on the vision is a hardware based security feature in Longhorn called Secure Startup. Secure Startup utilizes a Trusted Platform Module (TPM 1.2) to improve PC security and it meets some of the most critical requirements we heard from our customers-specifically, the capability to ensure that the PC running Longhorn starts in a known-good state, as well as protection of data from unauthorized access through full volume encryption".

[41] L'esempio del diario è tratto da SCHOEN, *Trusted Computing: Promise and Risk*, cit.

persone fisiche o imprese)[42];

- il monitoraggio dei problemi di sicurezza e la risoluzione in emergenza degli stessi[43];

[42] *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[t]he goal of risk management is to minimize the risk to corporate and personal assets due to malicious and accidental loss or exposure. Risk management processes help assess and mitigate risk. An element of risk management is vulnerability assessment. Asset owners seek to understand techniques employed to protect their assets and identify vulnerabilities associated with the protection mechanisms. TCG technologies such as Protected Storage can be applied to reduce the risk to information assets Protected storage can be used for securing public, private and symmetric keys that may be especially threatened since access to these represents access to a broader class of information assets. Since protected storage is based on mechanisms that are implemented in an isolated sub-system, the keys can be made less vulnerable to attack. To minimize risk, information managers naturally seek to protect information assets. This can be accomplished with cryptographic hashing to detect loss of integrity; public and secret key encryption to prevent unauthorized disclosure and digital signing to authenticate transmitted information. The TCG Protected Storage mechanisms rooted in hardware can then be used to protect keys, secrets and hash values. The vulnerability factor (used when computing Loss Expectancy) will decrease when information assets are protected in this way.

[...] Asset managers seek to prevent theft and unauthorized use of computing assets. Asset tracking can be an effective tool in achieving asset management objectives. TCG-defined Trusted Platform Modules (TPM) are manufactured such that ownership of a platform can be asserted by asset managers while allowing users ability to perform job functions. Under owner control the TPM can be used to create and protect an identity for the system that is not intended to be physically removed or replaced. Asset databases may use this identity to more reliably associate platform asset information. If an asset is stolen, the thief cannot gain access to information assets, hence may not profit from the consumption or brokering of stolen information".

[43] *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "IT managers expend a great deal of their time responding to virus attacks and threats. Emergency response teams must react quickly to isolate and inoculate vulnerable systems. Often they are required to scan the configurations and settings of all the enterprise connected systems to determine which systems need to be updated. A TPM can be used to ensure that each computer will report its configuration parameters in a trustworthy manner. Platform boot processes are augmented to allow the TPM to measure each of the components in the system (both hardware and software) and securely store the results of the measurements in

- il commercio elettronico[44].

Alcuni commentatori rilevano che uno degli utilizzi più promettenti è rappresentato dall'*Enterprise Rights Management* (ERM), cioè dal controllo accentrato dell'accesso ai documenti all'interno di un'organizzazione[45]. Ad esempio, l'ERM può essere

---

Platform Configuration Registers (PCR) within the TPM. Emergency response personnel can use these measurements to determine which computers are vulnerable to virus attacks. IT managers may install system processes that use the PCR values in a TPM to identify unsafe configurations at system boot thereby preventing inadvertent network connection while in an unsafe mode".

[44] *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[c]ustomer loyalty and vendor trust are important ingredients in electronic commerce interactions. Vendors build trust, in part, when transactions go smoothly and customer preferences are accurately reflected. Repeat business and loyalty is more likely when customers are able to recall the context of prior positive on-line transactions with vendors. TCG technology gives platforms the ability to define an e-commerce context in which customer and vendor may establish a relationship based on information exchange. Customers are able to control preferences that may be important to both customer and vendor. If the customer desires, a vendor can identify repeat customers and trust customer-managed preferences; by verifying the relationship context dynamically. The Trusted Platform Module (TPM) can report platform configuration information, that can be used to define the customer relationship context. The report is cryptographically verifiable enabling both parties the opportunity to be assured that the e-commerce transaction occurs in the context of the previously established relationship".

[45] V., fra gli altri, ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.: "TC can also be used to implement much stronger access controls on confidential documents. These are already available in a primitive form in Windows Server 2003, under the name of 'Enterprise rights management' and people are experimenting with them. One selling point is automatic document destruction. […] It can also be used to ensure that company documents can only be read on company PCs, unless a suitably authorised person clears them for export. TC can also implement fancier controls: for example, if you send an email that causes embarrassment to your boss, he can broadcast a cancellation message that will cause it to be deleted wherever it's got to. You can also work across domains: for example, a company might specify that its legal correspondence only be seen by three named partners in its law firm and their secretaries. (A law firm might resist this because the other partners in the firm are jointly liable; there will be many interesting negotiations as people try to reduce traditional trust relationships to programmed

utilizzato per programmare la distruzione di documenti confidenziali, o per evitare che i documenti prodotti dai computer dell'organizzazione possano essere letti da altri sistemi informatici.

Inoltre, sono in molti a ritenere che vi sia una stretta relazione tra TC e DRM. Benché si tratti di architetture differenti[46], è certo che le misure tecnologiche di protezione incorporate nei sistemi di DRM risulterebbero più efficaci in un ambiente TC. Chi spinge per un controllo assoluto rigido e accentrato dell'informazione, cioè per la diffusione dei sistemi di DRM, ha interesse all'affermazione dell'architettura TC[47]. In questa prospettiva, il TC può essere visto come un cambio di strategia che punta al controllo assoluto rigido e accentrato dell'informazione attraverso il controllo delle infrastrutture (i sistemi informatici) sulle quali la stessa informazione viaggia[48].

3. Architettura Trusted Computing, limitazioni preventive di funzionalità, dislocazione del controllo del computer e minacce alla privacy

I progetti volti all'affermazione di standard TC hanno

---

rules.)".

[46] KUHLMANN, GEHRING, *Trusted Platforms, DRM, and Beyond*, cit.; GHERING, *Trusted Computing for Digital Rights Management*, cit.

[47] Cfr. ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.; SCHOEN, *Trusted Computing: Promise and Risk*, cit.; ROEMER, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, cit.; FLICK, *The Controversy of Trusted Computing*, cit.; C. WOODFORD, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 *U. Colo. L. Rev.* 253 (2004).

[48] Si tratta dello scenario disegnato da R. CASO, *Il "Signore degli anelli" nel ciberspazio: controllo delle informazioni e Digital Rights Management*, in atti del convegno "Proprietà digitale: diritto d'autore, nuove tecnologie e Digital Rights Management" (Università Bocconi, Milano, 18 novembre 2005), in corso di pubblicazione. Sul punto cfr. R. STALLMAN, *Can You Trust Your Computer?*, 2002, disponibile all'URL: http://www.gnu.org/philosophy/can-you-trust.html

sollevato una legione di critiche provenienti sia dall'informatica sia da altri saperi (compreso quello giuridico). In particolare si rimprovera alla logica del TC:

- di essere basata su un linguaggio ambiguo e fuorviante nell'ambito del quale i termini utilizzati non corrispondono alle accezioni comuni o a quelle giuridiche (ad esempio, la parola "owner" può anche indicare un software e non la persona fisica o giuridica proprietaria del computer)[49];

- di far leva su un approccio che non necessariamente porta ad un ambiente informatico più sicuro[50] (in proposito occorre altresì

[49] A proposito del termine "owner" FLICK, *The Controversy of Trusted Computing*, cit., rileva che: "[t]he 'owner' of a Trusted Computing platform is another ambiguous term in the Trusted Computing Group specification. It is defined, in different places in the specification, as:

a) Any entity that knows a particular shared secret that is stored in a shielded location on the _TPM, and that may be required to prove their ownership status by producing the knowledge of this shared secret, or, if human, through asserting their physical presence to the machine, by pressing a button or otherwise.

b) The entity or person that controls the TPM, that is, the person (or human organisation) who bought and legally owns the computer. This person or their representative should be able to be verified through physical presence. It is important to note that in some places, 'physical presence' means a human being actually at the computer, while in other places it is noted that 'the manufacturer of a platform determines the exact definition of physical access' [Trusted Computing Group, 2003].

[…] If the manufacturer adheres to the part of the specification which says that 'the manufacturer of a platform determines the exact definition of physical access' [Trusted Computing Group, 2003], it could potentially allow programs to assert themselves as owner, taking control of 'ownership' functions such as the high level administration of the TPM keys, meaning that programs could control the TPM administration of the computer independently of the computer's owner. In this way, objects (programs) become agents in a much stronger and more insidious sense than ever intended by Latour! This could impact the human owner's ability to control their own computer and, furthermore, would almost certainly place trust in the appropriate functioning of the computer with the software writers […]".

[50] ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.: "[t]he question is: security for whom? You might prefer not to have to worry about viruses, but TC won't fix that: viruses exploit the way software applications (such as

considerare che mentre le specifiche del TCG sono pubbliche, le applicazioni possono invece rimanere segrete e dunque il loro livello di sicurezza può rimanere insondabile);

- di creare le condizioni per un ambiente informatico dove possono essere commessi illeciti al riparo dall'*enforcement* statale[51];

- di rendere possibili restrizioni alla concorrenza nel mercato

---

Microsoft Office and Outlook) use scripting. You might get annoyed by spam, but that won't get fixed either. (Microsoft claimed that it will be fixed, by filtering out all unsigned messages – but you can already configure mail clients to filter out mail from people you don't know and putting it in a folder you scan briefly once a day.) You might be worried about privacy, but TC won't fix that; almost all privacy violations result from the abuse of authorised access, and TC will increase the incentives for companies to collect and trade personal data on you".

SCHOEN, *Trusted Computing: Promise and Risk*, cit.: "[t]rusted computing technology can't prevent computer security holes altogether. In general, it seeks to contain and limit the damage that can result from a particular flaw. For instance, it should not be possible for a coding flaw in one application (like a web browser) to be abused to copy or alter data from a different application (like a word processor). This sort of isolation and containment approach is an important area of computer security research and is used in many different approaches to computer security, including promising techniques outside of trusted computing".

[51] FLICK, *The Controversy of Trusted Computing*, cit.: "Trusted Computing offers much in its arsenal for keeping data secure from tampering and unwanted viewing by third parties. As well as being attractive to honest applications, its capabilities could be used by those wishing to keep their information secure due to the anti-social nature of that information. Whistleblowing could be prevented if incriminating documents could not be passed on to outsiders, and terrorist organisations would be more at liberty to use the Internet to perform document exchanges without fear of monitoring by international agencies. Secure distributed efforts to crack encryption could also use the anonymous key generation capabilities of Trusted Computing to remain anonymous. Virus and malware writers could also use such networks to distribute information regarding the creation of such software, or for people who attempt to use such scripts to attack hosts to congregate anonymously. In these cases, it might be reasonable to expect that international agencies would require a 'back door' to Trusted Computing mechanisms so that monitoring of illegal activity could, in fact, occur. Microsoft, at least, claims it 'will never voluntarily place a back door in any of its products and would fiercely resist any attempt to require back doors in products'".

informatico[52];

[52] ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.: "TC will enable application software vendors to engage in product tying and similar business strategies to their hearts' content. As the application vendor will control the security policy server, he can dictate the terms under which anyone else's software will be able to interoperate with his own […]".

SCHOEN, *Trusted Computing: Promise and Risk*, cit.: "[s]oftware interoperability is also at risk. A developer of a web server program, file server program, e-mail server program, etc., could program it to demand attestations; the server could categorically refuse to deal with clients that had been produced by someone other than the server program's publisher. Or the publisher could insist on licensing fees from client developers, and make its server interoperate only with those who had paid the fee. (It is similarly possible to create proprietary encrypted file formats which can only be read by 'approved' software, and for which the decryption keys must be obtained from a network server and are extremely difficult to recover by reverse engineering.) The publisher in this case could greatly increase the switching costs for its users to adopt a rival's software. If a user has a large amount of important data stored inside a proprietary system, and the system communicates only with client software written by the proprietary system's publisher, it may be extremely difficult for the user to migrate his or her data into a new software system. When the new system tries to communicate with the old system in order to extract the data, the old system may refuse to respond. […] Unfortunately, the TCG design provides powerful new tools to enable lock-in. Attestation is responsible for this problem; sealed storage can exacerbate things by allowing the program that originally created a file to prevent any other program from reading it. Thus, both network protocols and file formats can be used to attack software interoperability".

D. L. BURK, *Market Regulation and Innovation: Legal and Technical Standards in Digital Rights Management*, 74 *Fordham L. Rev.* 537, 556-557 (2005): "[i]n a secured, rights-managed environment, therefore, interoperation and the ability to produce viable interoperative products depend not only on the standard for technical compatibility, but on the standard for defining and implementing 'trust'. A full discussion of the technical and operational parameters of trust management lies well beyond the scope of this paper, but since security is never absolute, such parameters are not necessarily objective in all dimensions, requiring at minimum a judgment as to how secure is secure enough. Where interoperation is at issue, the potential for considerable anticompetitive mischief may lie in such judgments; one can well imagine the possessor of a dominant market position protecting that position by excluding rival products from interoperation, ostensibly on security concerns, but clandestinely on strategic criteria. Even if the alleged security concerns leading to exclusion are wholly legitimate, concealing no illegitimate anticompetitive motivation, the practical effect of the exclusion may be the same, barring entry to

- di conferire un inedito potere di censura[53];

- di dislocare il controllo del computer dall'utente ad altri soggetti;

- di minacciare la privacy degli utenti.

Non è possibile in questa sede soffermarsi su tutte le critiche elencate. Ci si concentrerà solo sugli ultimi due profili. Si tratta di profili strettamente connessi.

Sebbene il TCG presenti l'architettura TC come uno strumento per proteggere i propri dati personali (si veda l'esempio sopra riportato relativo al diario privato), dal ragionamento che segue dovrebbe risultare evidente come essa costituisca invece una notevole minaccia alla privacy degli utenti.

Lo logica TC parte dall'idea che la sicurezza di un computer (e anche dell'ambiente digitale in cui si colloca) può essere messa a rischio dal proprietario o dall'utente dello stesso computer. Di là dalle critiche che possono essere mosse ad un approccio alla

---

innovative complementary or competing products".

[53] ANDERSON, *'Trusted Computing' Frequently Asked Questions*, cit.: "[o]ne of the worries is censorship. TC was designed from the start to support the centralised revocation of pirate bits. Pirate software won't run in the TC world as TC will make the registration process tamper-resistant. But what about pirated songs or videos? How do you stop someone recording a track – if necessary by putting microphones next the speakers of a TC machine, and ripping it into an MP3? The proposed solution is that protected content will contain digital watermarks, and lawful media players that detect a watermark won't play that song unless it comes with an appropriate digital certificate for that device. But what if someone hacks a Fritz chip and does a transaction that 'lawfully' transfers ownership of the track? In that case, traitor tracing technology will be used to find out which PC the track was ripped from. Then two things will happen. First, the owner of that PC will be prosecuted. (That's the theory, at least; it probably won't work as the pirates will use hacked PCs.) Second, tracks that have been through that machine will be put on a blacklist, which all TC players will download from time to time. Blacklists have uses beyond music copying. They can be used to screen all files that the application opens – by content, by the serial number of the application that created them, or by any other criteria that you can program. […] The potential for abuse extends far beyond commercial bullying and economic warfare into political censorship".

sicurezza che vede nel proprietario o nell'utente del computer il nemico da combattere, vanno ora riconsiderati i due fondamenti di questa logica ai quali si è prima accennato.

Il primo fondamento sta nella limitazione preventiva (e fisica) delle funzionalità del sistema informatico.

Il secondo fondamento sta nella dislocazione del controllo del sistema informatico dall'utente finale a chi produce l'hardware ed il software, nonché a chi è deputato a sorvegliare – mediante Internet e dunque mediante la gestione di dati relativi allo stesso sistema informatico – che siano rispettate le limitazioni di funzionalità imposte dal produttore.

Per valutare l'impatto di questa logica sui diritti dell'utente, occorre considerare entrambi i suoi fondamenti e prendere le mosse da una visione pluridimensionale del concetto di privacy. Si tratta dell'impostazione avanzata da una suggestiva ricostruzione di una giurista d'oltreoceano a proposito del DRM[54]. Occorre qui riprendere il filo di quel ragionamento, in quanto la logica TC ripropone su più vasta scala la logica del DRM. Infatti limitazione delle funzionalità del sistema informatico e dislocazione del suo controllo sono risvolti dell'idea dei *trusted systems* dalla quale derivano sia il DRM sia il TC.

Il consumo intellettuale, legato alla fruizione di opere dell'ingegno e di altre informazioni, chiama in causa due fondamentali dimensioni del concetto di privacy: la prima, "informazionale"; la seconda, spaziale[55].

Da sempre, la lettura di un testo letterario o l'ascolto di una musica rappresentano attività nelle quali si rispecchiano i tratti più intimi della personalità di un uomo, come i gusti artistici o le idee politiche e religiose. La riproducibilità in serie dell'opera

[54] J. E. COHEN, *DRM and Privacy*, 13 *Berkeley Tech. L. J.* 575 (2003).
[55] COHEN, *DRM and Privacy*, cit., 576 ss.

dell'ingegno ha poi esaltato la possibilità di rendere private e anonime tali attività. Nell'era predigitale, il contratto tra fornitore e fruitore dell'opera dell'ingegno avviene usualmente prescindendo dall'identificazione di quest'ultimo.

Invece nell'era del DRM il consumo intellettuale implica l'acquisizione e la registrazione da parte di terzi di dati personali mettendo in gioco la dimensione informazionale della privacy. Queste attività di acquisizione e registrazione, quando diventano persistenti e sistematiche, possono condizionare il comportamento, l'identità e la dignità dell'individuo. Ad essere minacciato è l'aspetto della privacy funzionale all'autodeterminazione della propria personalità. In buona sostanza, la dimensione informazionale della privacy delinea uno spazio (intellettuale) nel quale il pensiero può liberamente esprimersi[56].

La dimensione spaziale concerne, invece, quei luoghi (fisici) privati – non necessariamente oggetto di proprietà – nei quali i comportamenti della persona sono liberi dal condizionamento altrui. Tali comportamenti possono includere quelli che risultano aberranti per le norme sociali dominanti e quelli che semplicemente non sono destinati ad essere assunti in pubblico. Tra questi comportamenti vi

[56] COHEN, *DRM and Privacy*, cit., 577-578: "[s]urveillance and compelled disclosure of information about intellectual consumption threaten rights of personal integrity and self-definition in subtle but powerful ways. Although a person cannot be prohibited from thinking as she chooses, persistent, fine-grained observation subtly shapes behavior, expression, and ultimately identity. The inexorable pressure toward conformity generated by exposure, and by loss of control over uses of the gathered information, violates rights of self-determination by coopting them. Additionally, surveillance and exposure devalue the fundamental dignity of persons by reducing the exposed individuals to the sum of their 'profiles'. For these reasons, in circumstances where records of intellectual consumption are routinely generated – libraries, video rental memberships, and cable subscriptions – society has adopted legal measures to protect these records against disclosure. Privacy rights in information about intellectual activities and preferences preserve the privacy interest in (metaphoric) breathing space for thought, exploration, and personal growth".

sono molte forme di consumo intellettuale. In definitiva, la seconda dimensione della privacy delimita uno spazio (fisico) nel quale la persona è libera di esplorare i propri interessi intellettuali[57].

Le dimensioni informazionale e spaziale sono messe in gioco dalle funzionalità di base e supplementari dei sistemi di DRM. Questi condizionano il (comportamento legato al) consumo (intellettuale) del contenuto digitale e rendono possibile l'acquisizione – in forme che sovente non sono trasparenti e visibili al consumatore – di informazioni dettagliate e permanenti, cioè la creazione di banche dati su tale consumo[58].

Il condizionamento del consumo intellettuale è evidente nei sistemi di DRM che pongono limiti al (cioè restringono direttamente il) comportamento dei fruitori di contenuti digitali[59]. Ad esempio, alcuni formati audio o video possono escludere la copia o possono limitare le tipologie di apparecchi di lettura. Tecnologie di questo genere restringono lo spazio di libertà tradizionalmente legato al consumo intellettuale, riducendo l'autonomia con la quale un soggetto decide le condizioni di uso e godimento di un contenuto informativo. In altri termini, esse dislocano dal fruitore al titolare dei contenuti la scelta relativa al consumo intellettuale.

Occorre poi aggiungere che, oltre alla restrizione diretta e al

[57] COHEN, *DRM and Privacy*, cit., 579-580: "[s]patial privacy affords the freedom to explore areas of intellectual interest that one might not feel as free to explore in public. It also affords the freedom to dictate the circumstances – the when, where, how, and how often – of one's own intellectual consumption, unobserved and unobstructed by others. In many nonprivate spaces, this freedom is absent or compromised. For example, one may enter a library or a bookstore only during business hours, and copyright law restricts the ability to watch movies on the premises of video rental establishments. The essence of the privacy that private space affords for intellectual consumption is the absence of such limits. The interest in unfettered intellectual exploration includes an interest in the unfettered ability to use and enjoy intellectual goods within those spaces".

[58] COHEN, *DRM and Privacy*, cit., 580.

[59] COHEN, *DRM and Privacy*, cit., 580 ss.

monitoraggio del consumo digitale, i sistemi di DRM possono essere dotati di un'ulteriore funzionalità: l'autotutela. L'autotutela ha implicazioni in tema di privacy[60]. Tecnologie per la restrizione dell'uso del contenuto digitale possono essere dotate di funzionalità atte a sanzionare o disabilitare gli usi non autorizzati. Tali funzionalità possono operare anche in *tandem* con quelle di monitoraggio e possono altresì essere attivate automaticamente senza il bisogno di comunicare con un sistema informativo esterno a quello dove gira il file protetto dal DRM.

Ebbene, le funzionalità di autotutela minacciano la privacy legata al consumo intellettuale in modo peculiare. Esse, in primo luogo, identificano un particolare fruitore di contenuti digitali come il bersaglio di una misura di autotutela. Tale fruitore in questo modo non è più uno dei tanti anonimi consumatori di contenuti digitali, ma subisce una classificazione. In secondo luogo, le funzionalità di autotutela distruggono quello spazio di libertà che la privacy conferisce a chi assume comportamenti che sono condannati solo da norme sociali e non da norme giuridiche[61], o ancora che sono solo eventualmente sanzionati dall'apparato statale. In questo senso,

[60] COHEN, *DRM and Privacy*, cit., 586 ss.

[61] COHEN, *DRM and Privacy*, cit., 587-588: "[b]y inserting automatic enforcement functions into private spaces and activities, these technologies elide the difference between public/rule-governed behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms. Some offenses, most notably crimes against persons, are so severe that they may justify such elision. In other cases, however, looseness of fit between public rules and private behavior serves valuable purposes. Where privacy enables individuals to avoid the more onerous aspects of social norms to which they may not fully subscribe, it promotes tolerance and pluralism. Where the precise contours of legal rules are unclear, or the proper application of legal rules to particular facts is contested, privacy shields a range of experimentation with different behaviors that furthers the value-balancing goals of public policy. Highly restrictive DRM technologies do not permit this experimentation, and eliminate public policy and privacy alike from the calculus of infraction and enforcement".

sistemi di DRM altamente restrittivi assistiti da funzionalità di autotutela possono rappresentare una nuova forma di autoritarismo privato.

Tutte queste considerazioni possono essere riproposte per il TC. Le limitazioni preventive di funzionalità e la dislocazione del controllo del sistema informatico (le quali implicano tra l'altro il trattamento costante di dati personali e l'autotutela tecnologica) minacciano la privacy dell'utente sia nella dimensione informazionale sia in quella spaziale. Nello scenario TC la sicurezza è affidata principalmente al potere di imprese private (e solo eventualmente a quello degli Stati) che si estrinseca nella compressione dei margini di libertà di utilizzo del sistema informatico, nella sorveglianza costante (messa in atto secondo il principio del "guardare senza essere visti") e nella punizione a distanza del comportamento non consentito. Non a caso questo scenario è stato accostato alla società prefigurata da Foucalt nella sua famosa rilettura dell'idea benthamiana del Panopticon[62].

[62] FLICK, *The Controversy of Trusted Computing*, cit.: "[i]n the Trusted Computing field, the meanings of 'trust' and 'control' overlap significantly with each other. Foucault [Foucault, 1975], in his famous dissertation on panopticism, introduces the concept that the two are closely related, united in the practise of discipline. He describes disciplinary power as being '...exercised through its invisibility; at the same time it imposes on those whom it subjects a principle of compulsory visibility. In discipline it is the subjects who have to be seen. Their visibility assures the hold of the power that is exercised over them'".

V. inoltre il sito Web del *Trusted Systems Project* all'URL: http://trusted-systems.info/, nel quale si legge: "Trusted systems for purposes of this research are systems in which some conditional prediction about the behavior of people or objects within the system has been determined prior to authorizing access to system resources. For example, trusted systems include the use of 'security envelopes' in national security and counterterrorism applications, 'trusted computing' initiatives in technical systems security, and the use of identity or credit scoring systems in financial and anti-fraud applications; in general, they include any system (i) in which probabilistic threat or risk analysis is used to assess 'trust' for decision-making before authorizing access or for allocating security resources against likely threats

È dunque la logica di fondo dell'architettura TC a minacciare la privacy. Peraltro, singoli profili legati alla dislocazione del controllo del computer comportano un massiccio e persistente trattamento di dati personali la cui compatibilità con la normativa dell'Unione europea è oggetto di discussione. Di questa discussione si intende brevemente dar conto nel paragrafo che segue.

4. Trusted Computing e dislocazione del controllo del sistema informatico: questioni relative alla compatibilità con la normativa europea

La pubblicazione delle varie versioni delle specifiche TC ha sollevato questioni relative al trattamento dei dati personali. Nell'Unione europea sono stati avanzati dubbi sulla compatibilità delle architetture TC con il quadro normativo derivante dalle direttive 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e 2002/58/CE del Parlamento europeo e del Consiglio del 12

(including their use in the design of systems constraints to control behavior within the system), or (ii) in which deviation analysis or systems surveillance is used to insure that behavior within systems complies with expected or authorized parameters. The adoption of these authorization-based security strategies (where the default state is DEFAULT=DENY) for counterterrorism and anti-fraud is helping accelerate the ongoing transformation of modern societies from a notional Beccarian model of criminal justice based on accountability for deviant actions after they occur, see Cesare Beccaria, On Crimes and Punishment (1764), to a Foucauldian model based on authorization, preemption, and general social compliance through ubiquitous preventative surveillance and control through system constraints. See Michel Foucault, Discipline and Punish (1975, Alan Sheridan, tr., 1977, 1995). In this emergent model, 'security' is geared not towards policing but to risk management through surveillance, exchange of information, auditing, communication, and classification. These developments have led to general concerns about individual privacy and civil liberty and to a broader philosophical debate about the appropriate forms of social governance methodologies. Our work in this area examines these issues".

luglio 2002 relativa al trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche. La discussione che ne è nata ha suscitato l'interesse del Gruppo di Lavoro per la Tutela dei Dati Personali istituito in base all'art. 29 della dir. 95/46/CE, il quale il 23 gennaio 2004 ha adottato il "Documento di lavoro sulle piattaforme fidate, in particolare per quanto riguarda il lavoro effettuato dal Trusted Computing Group (Gruppo TCG)"[63].

In questo documento il Gruppo di Lavoro, pur partendo dalla consapevolezza che non è ancora possibile sapere come le specifiche elaborate dal TCG saranno utilizzate, quali applicazioni o sistemi operativi saranno sviluppati, quali operatori saranno interessati o quali modelli commerciali saranno prodotti, e pur esprimendo soddisfazione per il dialogo avviato con il TCG nonché per l'accoglimento di alcuni suggerimenti nella versione 1.2 delle specifiche, continua a svolgere alcune considerazioni critiche circa l'impatto del TC sulla protezione dei dati personali[64].

Le più rilevanti considerazioni si concentrano sui due profili più critici della dislocazione del controllo del sistema informatico:

a) la differenziazione del ruolo del proprietario da quello dell'utente;

b) la funzione di *remote attestation* che si riconnette all'*Endorsement Key* e al ruolo della *Privacy Certification Authority* (che sarebbe uno degli strumenti deputati, nell'ambito delle

[63] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, adottato il 23 gennaio 2004, 11816/03/EN, WP 86, disponibile all'URL: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_en.pdf

[64] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, cit., 4.

specifiche TCG, a garantire la privacy degli utenti)[65].

Sul profilo *sub* a) il Gruppo osserva quanto segue.

Le specifiche dei TPM distinguono tra il ruolo del "proprietario dei diritti" e il ruolo dell'utente. Tale distinzione non ha conseguenze nell'ambito privato, nel quale il proprietario si identifica con l'utente, ma potrebbe sollevare talune questioni a livello di imprese. Nell'impresa il dipendente è l'utente, mentre il datore di lavoro è il proprietario. Il proprietario può prendere una serie di decisioni che riguardano il dipendente ed i dati personali che vengono trattati. In questo caso è responsabilità del proprietario (datore di lavoro) informare l'utente e garantire una tutela adeguata degli individui. La versione 1.2 delle specifiche ha introdotto alcuni miglioramenti di questa situazione aggiungendo un sistema di delega per le decisioni relative alle varie funzioni del TPM. Tuttavia, il proprietario dispone sempre del controllo finale e può decidere di delegare o no talune funzioni chiave. In tal caso non è possibile affermare (come fanno talune società TCG sul proprio sito Internet o nelle comunicazioni ufficiali) che gli individui hanno la totale libertà di accettare o no l'impiego del sistema. Allo stato attuale delle

[65] V. il documento del TCG intitolato *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[o]ne objective of attestation is to allow the Challenger to determine that some TPM has signed a message. It may also be used to determine 'which' TPM signed the message. A Privacy CA may be employed to issue AIK credentials that vouch for the trustworthiness of a platform without disclosing EK unique values to a Challenger. The TPM enrolls AIK public keys with a Privacy CA. The Privacy CA may then distribute a credential certifying the AIK. Enrollment with a Privacy CA requires the TPM to prove AIK keys are exclusively bound to the TPM. The platform accomplishes this by decrypting the AIK credential using the EK private key in the TPM. Only the TPM with the EK private key will be able to perform the decryption. The Privacy CA is trusted not to reveal sensitive information. This includes the public EK or PII derived from it. It is also trusted not to misrepresent the trust properties of platforms for which AIK credentials are issued. A TPM can be configured to require owner authorization before participating in AIK credential issuance protocols. A TPM can further be disabled or deactivated to further control TPM use".

specifiche, la possibilità dell'utente di decidere di utilizzare o no una piattaforma con un TPM esisterebbe solo al di fuori dell'ambiente delle imprese. Peraltro occorre chiedersi per quanto tempo ancora. L'impiego di TPM, incoraggiato dall'industria, potrebbe diventare uno standard di fatto, un presupposto necessario per partecipare alla società dell'informazione. Ciò potrebbe avere conseguenze non solo per la tutela dei dati, ma anche per i diritti fondamentali come la libertà d'espressione[66].

Sul profilo *sub* b) il Gruppo svolge le seguenti considerazioni.

Per limitare la trasmissione di identificatori e quindi la compilazione da parte di terzi di profili dell'utente, il gruppo TCG prevede la possibilità d'intervento da parte di un terzo fidato che certifica l'identità degli utenti e li conferma al corrispondente senza rivelare l'identità dell'utente. Il ruolo del terzo fidato (denominato anche "Privacy Certification Authority" dal TCG) deve essere studiato in dettaglio. La concentrazione di dati comporta sempre rischi supplementari e quindi vanno prese le dovute precauzioni. Per quanto riguarda i TPM esistono scenari in cui un unico terzo fidato controlla enormi quantità di informazioni di autenticazione. La versione 1.2 delle specifiche consente di evitare il terzo fidato mediante l'utilizzo della funzione di "Direct Anonymous Attestation (DAA)", che consente all'utente di creare una "Attestation Identity Key" (AIK-chiave di attestazione dell'identità) senza presentare la chiave di approvazione (*Endorsement Key*, EK), che è un identificatore univoco. Il Gruppo di Lavoro ritiene che si tratti di un miglioramento, ma sottolinea che la scelta tra terzo fidato e DAA sarà fatta a livello di applicazioni. Le specifiche attuali permettono

[66] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, cit., 6.

ancora le due funzioni. La DAA è quindi una possibilità supplementare, ma non una caratteristica standard del sistema. Il Gruppo di Lavoro ritiene che l'introduzione della funzione DAA costituisca un miglioramento, ma ricorda che non si può più parlare di anonimato quando è possibile creare un legame con l'identità dell'utente o delineare profili degli utenti. Il Gruppo di Lavoro invita il TCG a promuovere l'impiego di tale funzione in modo da tutelare la privacy ed i dati, cioè facendo leva su *random identifiers* e limitando l'uso dei nomi al periodo più breve possibile nei casi in cui sia necessaria la revoca o l'identificazione. Il Gruppo di Lavoro ribadisce l'importanza della fiducia nei sistemi basati sui TPM. La fiducia deve esistere in tutta la catena degli operatori interessati, da chi realizza specifiche, al venditore delle applicazioni fino all'utente del sistema. È necessario tutelare i dati in tutte le fasi[67].

Il documento del Gruppo di Lavoro si conclude con l'invito a muoversi secondo alcune linee-guida tra le quali spiccano le seguenti:

- fornire agli utenti informazioni complete e facili da comprendere ("[e]siste una catena di responsabilità che va da chi elabora le specifiche ai produttori, agli addetti allo sviluppo di nuovi sistemi operativi o applicazioni, a chi li commercializza" […]; in particolare "[l]'impiego dei TPM deve essere trasparente per l'utente, in particolare a livello dell'applicazione"[68];

- introdurre meccanismi volti a controllare che l'applicazione delle specifiche TCG rispettino le leggi in materia di tutela dei dati personali (ad esempio, "[l]a creazione di un logo o di un programma

[67] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, cit., 7-8.

[68] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, cit., 8-9.

di certificazione riguardante la conformità dei prodotti è stata proposta nel corso del dialogo con i membri del gruppo TCG")[69].

Successivamente, il TCG ha pubblicato nel maggio 2005 un documento intitolato "Design, Implementation, and Usage Principles for TPM Based Platforms" che in qualche modo risponde alle critiche avanzate da più parti[70].

In materia di protezione dei dati personali il documento parte da una raccomandazione di massima nella quale si invita a disegnare ed implementare le componenti TCG in modo da garantirne la compatibilità con la lettera e con lo spirito di tutti gli atti rilevanti quali leggi, regolamenti e linee-guida (comprese le OECD *Guidelines*, le *Fair Information Practices* e la direttiva 95/46/CE).

Vengono poi enunciate le seguenti linee-guida[71].

- Informativa ("Notice"): dovrebbe essere fornita un'informativa esplicita circa la raccolta e la conservazione dei dati personali.

- Scelta ("Choice"): il proprietario di sistemi TCG dovrebbe disporre di una reale scelta e del controllo circa il trasferimento di informazioni personali. Gli utenti di sistemi TCG dovrebbero poter

[69] V. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, cit., 9.

[70] V. il documento del TCG Best Practices Committee intitolato *Design, Implementation, and Usage Principles for TPM-Based Platforms*, *version* 1.0, maggio 2005. Nel dicembre 2005 è stata emanata una seconda versione del documento (*version* 2.0) disponibile all'URL: https://www.trustedcomputinggroup.org/specs/bestpractices/Best_Practices_Principles_Document_V2_0.pdf (la parte relativa alla privacy di cui si discute nel testo è rimasta sostanzialmente invariata). Il TCG aveva peraltro dato una prima risposta al documento del Gruppo di Lavoro per la Tutela dei Dati Personali con un breve documento del 6 febbraio 2004 reperibile all'URL: https://www.trustedcomputinggroup.org/press/feb_6_art_29_report_QA.pdf

[71] V. il documento intitolato *Design, Implementation, and Usage Principles for TPM-Based Platforms*, *version* 1.0, maggio 2005, 6.

disabilitare le funzionalità TCG in modo da non violare le policy del proprietario e al tempo stesso da avere il controllo sul trasferimento di informazioni personali.

- Limitazione dello scopo ("Purpose Limitation"): le informazioni personali raccolte per uno scopo non dovrebbero essere utilizzate per altre finalità. Tutte le implementazioni delle componenti TCG dovrebbero assicurare che la tecnologia TCG non si presti ad abusi nella raccolta di informazioni personali.

- Controllo ("Control"): le informazioni private relative al proprietario dovrebbero essere nel controllo dello stesso proprietario. Le informazioni private relative all'utente dovrebbero essere nel controllo dello stesso utente.

- Qualità dei dati ("Data Quality"): ogni informazione memorizzata dovrebbe essere ordinata secondo criteri temporali e, di conseguenza, ogni informazione personale fornita da una tecnologia TCG dovrebbe essere aggiornata.

- Accesso ("Access"): se funzionalità TCG sono utilizzate per raccogliere e memorizzare dati personali relativi ad un individuo, ciò deve essere fatto con modalità che consentano allo stesso individuo di verificare e correggere gli stessi dati ove necessario.

- Proporzionalità ("Proportionality"): i dati personali raccolti e trasferiti attraverso funzionalità TCG devono essere rilevanti e non eccessivi rispetto agli scopi per i quali sono stati raccolti. Le chiavi private, che giocano un ruolo fondamentale nella piattaforma, non dovrebbero mai essere rivelate. La proporzionalità è parte fondamentale del modello di sicurezza rispondente alle specifiche TCG. Il TPM TCG incorpora un unico duraturo e stabile identificatore chiamato *Endorsement Key* (EK). Dal momento che il TPM è legato alla piattaforma, la EK diventa un'informazione relativa ad una persona identificabile. Al fine di ridurre la capacità di aggregare dati personali, le specifiche TCG proibiscono l'uso

generalizzato della EK. Le stesse specifiche richiedono che la EK sia invece utilizzata per generare degli *alias* che non devono essere riconducibili esplicitamente all'EK. Questo obiettivo può essere raggiunto in vari modi, tra i quali figurano l'utilizzo di *zero-knowledge protocols*, di una *Privacy Certification Authority*, l'utilizzo congiunto di *zero-knowledge protocols* e di una *Privacy Certification Authority*, etc. L'uso di questi strumenti protegge la privacy dell'utente rendendo più difficile l'aggregazione dei dati. Il TCG raccomanda che le implementazioni e gli sviluppi di sistemi TCG consentano il più alto livello di anonimato da ritenersi appropriato rispetto ad una determinata situazione.

Le linee-guida del TCG rappresentano certamente un passo in avanti sulla via del rispetto della privacy. Tuttavia, esse presentano limiti evidenti[72]. Si tratta infatti di principi generici che riecheggiano (piuttosto confusamente) alcuni cardini della normativa comunitaria sulla protezione dei dati personali. Per quel che più conta, poi, esse rappresentano una lampante dichiarazione di ammissione del fatto che l'architettura TC costituisce intrinsecamente una minaccia alla privacy. Come si può infatti lasciare la possibilità di disabilitare le funzionalità TC all'utente e pretendere che questo sia compatibile con la policy di sicurezza del proprietario, policy di cui l'architettura TC fa parte integrante? Inoltre, si dice esplicitamente che attraverso vari strumenti (rispetto ai quali il TCG, peraltro, non indica una preferenza)[73] quali gli *zero-knowledge protocols* e le *Privacy Certification Authorities* si può solo rendere più difficile (ma non

[72] Per alcune critiche alla bozza del documento intitolato *Design, Implementation, and Usage Principles for TPM-Based Platforms* v. S. SCHOEN, *EFF Comments on TCG Design, Implementation and Usage Principles 0.95*, ottobre 2004, disponibile all'URL: http://www.eff.org/Infrastructure/trusted_computing/20041004_eff_comments_tcg_principles.pdf

[73] Cfr. S. BECHTOLD, *Comments on the TCG Best Practices Committee Document*, giugno 2005, disponibile all'URL: http://cyberlaw.stanford.edu/blogs/bechtold/archives/003155.shtml

eliminare) l'aggregazione dei dati personali, in quanto la EK costituisce necessariamente un identificatore univoco al quale sono riconducibili informazioni personali.

5. Conclusioni

Le architetture informatiche sono state paragonate a quelle fisiche. Il codice informatico alle regole giuridiche[74]. Come le architetture fisiche (si pensi ai dossi artificiali per ridurre la velocità dei veicoli sulle strade), le architetture digitali recano in sé stesse regole implicite. Come le regole giuridiche, il codice binario condiziona il comportamento umano.

Tuttavia, occorre rimarcare le differenze che corrono tra regole informatiche e regole giuridiche.

a) Nelle architetture informatiche il codice digitale assomiglia più alle regole implicite incorporate nella materia che alle regole giuridiche verbalizzate da un uomo. Le regole delle architetture digitali sono rigide e predeterminate[75]. Quelle giuridiche sono per loro natura elastiche, cioè soggette ad una formulazione o ad un'interpretazione variabile nel tempo.

b) Inoltre, il processo di produzione delle regole informatiche è differente da quello che è alla base della produzione di regole di diritto. Le regole informatiche sono scritte da tecnici e non da giuristi. Gli obiettivi politici che stanno a ridosso del processo di produzione delle regole non sempre sono trasparenti[76].

c) La forza di una regola giuridica dipende da vari fattori, tra

[74] Il riferimento è a L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999. Nella letteratura italiana, v. A. ROSSATO, *Diritto ed architettura nello spazio digitale – Il ruolo del software libero*, Padova, 2006.

[75] Sulla natura delle regole incorporate in architetture digitali v., da ultimo, D. L. BURK, *Market Regulation and Innovation: Legal and Technical Standards in Digital Rights Management*, 74 *Fordham L. Rev.* 537 (2005).

[76] Cfr. G. PASCUZZI, *Il diritto dell'era digitale – Tecnologie informatiche e regole privatistiche*, II ed., Bologna, 2006, 304 ss.

i quali spicca il grado di condivisione che la stessa incontra nella comunità di riferimento. La forza di una regola informatica dipende essenzialmente dalla sua efficacia tecnologica (ad esempio, l'architettura TC può essere considerata efficace solo se è virtualmente impossibile "rompere" gli algoritmi crittografici sui quali si basa), nonché dal suo grado di diffusione (ad esempio, l'architettura TC potrà dirsi davvero condizionante del comportamento umano solo se e quando assurgerà a standard tecnologico accettato da una moltitudine di utenti). La diffusione di uno standard è cosa diversa dalla condivisione di una regola giuridica.

d) La regola informatica – soprattutto quando corrisponde ad uno standard tecnologico – è per sua vocazione globale, mentre quella giuridica spesso è a vocazione locale[77].

e) La regola informatica è espressa in un linguaggio che deve essere comprensibile anche alle macchine e che in ultima analisi si identifica in una sequenza di 0 e 1. In definitiva, il linguaggio informatico (o meglio la sua forma ultima che è rappresentata dal codice binario) è unico e privo di ambiguità. La regola giuridica (successiva all'epoca del diritto muto) è verbalizzata, cioè espressa nell'ambiguità tipica del linguaggio umano e nella specificità di ciascuna lingua parlata.

Un emergente filone di ricerche interdisciplinari si dedica allo studio dell'incorporazione di valori giuridici condivisi nelle regole informatiche (c.d. *value-centered design*). Tuttavia, per le caratteristiche che si sono evidenziate nei punti a) ed e), lo stato attuale delle tecnologie è molto lontano dalla possibilità di tradurre nel codice binario la flessibilità di un principio generale o di una consuetudine.

[77] Cfr. PASCUZZI, *Il diritto dell'era digitale – Tecnologie informatiche e regole privatistiche*, cit., 273 ss.

L'architettura TC costituisce la dimostrazione paradigmatica di quanto ora rilevato circa la natura delle regole informatiche e del processo che le produce. Il lavoro del TCG e dell'organizzazione che l'ha preceduto è iniziato lontano dai riflettori dei media e dalla discussione politica. Sebbene il TCG si occupi del primissimo stadio di sviluppo dell'architettura informatica, cioè delle specifiche che poi dovranno essere tradotte nelle molte componenti tecnologiche di riferimento, le sue decisioni delineano i valori che prevalgono all'interno della stessa architettura. Nonostante l'ambiguità del linguaggio utilizzato nelle specifiche, risulta evidente che i valori che sono a ridosso della privacy sono sacrificati a vantaggio di una certa visione della sicurezza informatica. In particolare, la limitazione preventiva di funzionalità e la dislocazione del controllo dei sistemi informatici delineano un ambiente digitale dove la sicurezza è ottenuta al prezzo della compressione *ex ante* dei margini di libertà legati alle dimensioni spaziale e informazionale della privacy. Si tratta di scelte di fondo che ben difficilmente potranno essere riviste, se non nell'ottica di rivoluzionare la logica TC e dare avvio ad una nuova architettura della sicurezza. D'altra parte, il processo di traduzione in applicazioni hardware e software è già in moto (inerziale) da tempo e segue le dinamiche di standardizzazione tipiche dell'industria informatica. Il dialogo avviato tra TCG ed alcune istituzioni politiche (come il Gruppo di Lavoro per la Tutela dei Dati Personali) può portare solo ad alcuni miglioramenti marginali dell'architettura. Ad esempio, la possibilità di disattivare le funzionalità TC, che viene spesso indicata come la garanzia del mantenimento del controllo del TC, appare come un'arma tanto irrinunciabile quanto spuntata. In un ambiente digitale colonizzato dalla logica TC e dunque dalla limitazione (fisica e) preventiva dei margini di manipolabilità dei sistemi informatici, tale possibilità potrebbe rivelarsi del tutto illusoria.

Se così è, al diritto non rimane che cercare di difendere la "biodiversità" dell'ambiente digitale e di garantire la convivenza tra differenti visioni della sicurezza. Si tratta di un obiettivo politico di primaria importanza che passa attraverso vari strumenti. Se non dovesse essere raggiunto, ci troveremo a rimpiangere – almeno nella dimensione digitale – la fallibilità delle regole giuridiche.

LE PROBLEMATICHE DELLA SICUREZZA INFORMATICA DALLA PROSPETTIVA TECNICA

Andrea Gelpi

1. Introduzione

Volendo parlare di sicurezza informatica la prima domanda da porsi è quale definizione dare di sicurezza informatica. Delle molte disponibili anche su Internet a me piace particolarmente la seguente:

"insieme di 'norme', 'regole', 'tecniche' e comportamenti per l'uso di sistemi informatici e di comunicazione".

Innanzitutto, è da notare come in questa definizione sia compreso l'uso di strumenti di comunicazione che vanno oltre il semplice elaboratore elettronico ed includono anche telefono, fax e simili.

Che cosa intendo per "norme" nella definizione appena data? Mi riferisco a tutte quelle leggi e regolamenti che provengono dall'esterno della struttura organizzativa della cui sicurezza si tratta: sono quindi incluse le leggi dello stato, le leggi regionali e provinciali, ecc.

Per "regole" invece bisogna intendere proprio quelle che nascono all'interno della struttura: il regolamento interno per l'uso del telefono è forse la misura più nota, un'altra potrebbe essere

l'utilizzo del computer per navigare su Internet, ecc. Tutte le aziende che utilizzano computer per il loro lavoro dovrebbero dotarsi, se già non lo fanno, di un documento di regole, chiamato documento delle politiche di sicurezza aziendali (*security policy*).

Le "tecniche" sono, poi, quelle soluzioni di natura (appunto) tecnologica che aiutano gli utenti e gli amministratori a far rispettare sia le norme che le regole.

Per ultimo, ma sicuramente tra gli aspetti più significativi, restano i comportamenti degli utenti finali, dai quali dipende la reale sicurezza della struttura. Infatti, anche se si prevedono regole e soluzioni tecniche molto sofisticate, è sufficiente il comportamento "insicuro" di un unico utente per vanificare tutto il lavoro svolto. Un semplice esempio credo aiuterà a capire meglio. Se in una struttura si è deciso che le parole chiave devono sottostare a tutta una serie di regole molto complicate e poi gli utenti scrivono le *password* su foglietti che appiccicano ai computer, è evidente che il comportamento degli utenti vanifica tutto il lavoro fatto precedentemente.

A mio avviso, quindi, è importantissimo non trascurare la formazione degli utenti che solo se resi edotti degli eventuali comportamenti a rischio potranno essere d'aiuto alle aziende. Per cercare di comprendere meglio di che cosa sto parlando provate ad immaginare Internet come un grosso centro commerciale dove è possibile trovare di tutto. Ebbene, se ci pensate, quando andiamo in un grande centro commerciale molto affollato, siamo abituati da sempre ad adottare alcune precauzioni onde evitare di essere scippati o truffati: ad esempio, le signore si tengono la borsa bella stretta e nessuno di noi si sognerebbe di girare con banconote che sbucano dalle tasche. A volte, però, ci "muoviamo" su Internet lasciando dietro di noi una striscia impressionante di dati che ci riguardano: non solo l'indirizzo IP del nostro computer, ma anche dati personali,

come il nome, i numeri di telefono, i numeri di carte di credito e, nei casi più gravi, anche i codici d'accesso a siti e servizi. Il tutto spesso viaggia in Internet "in chiaro" e chiunque sappia come fare è in grado di catturare queste informazioni e servirsene. Ancora una volta è fondamentale acquisire consapevolezza sui problemi a cui si va incontro quando si naviga su Internet.

2. Misure tecniche implementabili dagli utenti privati e dalle aziende

Vediamo ora alcuni esempi di comportamenti degli utenti che possono portare a rischi ben specifici. Ci sono utenti che tengono i dati sui loro portatili perché li ritengono più al sicuro che sui *server* dell'azienda dove magari qualcuno potrebbe accedervi. Poi, se il portatile viene rubato, non solo i dati sono finiti in mano di chissà chi, ma, non esistendo nemmeno una copia di *back-up* in azienda, il danno può essere enorme. Per non parlar poi dei codici d'accesso ai computer o alle applicazioni: troppo spesso questi codici risultano conservati in luoghi facilmente rintracciabili, ad esempio sotto la tastiera, in un cassetto o maldestramente nascosti fra i numeri di telefono della propria agenda cartacea. In altri casi c'è chi si domanda perché mai il proprio computer dovrebbe essere a rischio, in fondo si dice "non ci sono dati importanti". Sono proprio questi, invece, i computer più appetibili da malintenzionati per fini più diversi (spesso accade, ad esempio, che vengano poi utilizzati per nascondersi, in quanto si è sicuri che nessuno verificherà cosa sta succedendo). Manca, quindi, una cultura della sicurezza, intesa come consapevolezza dello strumento che viene utilizzato, manca ancora il concetto di "chi ha fatto che cosa", cioè il concetto di responsabilità, qui intesa non tanto come strumento per attribuire colpe, ma come mezzo per risolvere velocemente problemi e migliorare, quindi, l'efficienza del lavoro di tutti. Se invece di perdere tempo a rintracciare chi ha fatto una qualche operazione, si fosse in grado di

sapere subito cosa è realmente accaduto, molti problemi sarebbero risolti letteralmente “al volo”.

Una domanda importante che ogni azienda dovrebbe porsi è se la propria struttura organizzativa sia compatibile con i livelli di sicurezza che si vuole raggiungere. Troppo spesso a noi tecnici vengono chieste soluzioni estremamente laboriose e complicate, mentre nella maggior parte dei casi basterebbe modificare la struttura organizzativa per semplificare o, addirittura, per eliminare i problemi. Ad esempio, prevedere che ci siano sempre almeno due dipendenti che possono operare su una certa base dati o che siano in grado di leggere e smistare una determinata casella di posta è sicuramente molto più semplice ed efficace di qualsiasi altra soluzione che si basi solamente sulla tecnologica.

È importante, e più efficiente, prevedere che ci siano più persone che accedono agli stessi dati ed evitare che siano assenti contemporaneamente, piuttosto che organizzare opportunamente i dati sui *server*, verificare che cosa fanno i tecnici quando lavorano sui sistemi in azienda, fare attenzione ai dati e alle configurazioni dei computer portatili. È normale, infatti, che quest’ultimi siano collegati a più reti, ad esempio quella casalinga (oltre che quella aziendale) dove tipicamente il firewall non c’è e quindi non sono presenti quelle protezioni utilizzate invece in azienda, oppure dove l’antivirus non può aggiornarsi in quanto non trova il *server* aziendale quando è collegato ad Internet da casa. Non va nemmeno dimenticato il fatto che i computer portatili possono essere più facilmente rubati e risulta, poi, facile che si rompano proprio perché vengono trasportati nei luoghi più disparati. I dati in essi memorizzati vanno perciò curati maggiormente che in altre situazioni.

È, inoltre, fondamentale che i locali dove si trovano i *server* siano chiusi a chiave e che l’accesso sia consentito solo al personale addetto, onde evitare danni anche accidentali ai sistemi oltre ad

azioni di natura dolosa. Tali locali, poi, devono essere posizionati tenendo conto dei rischi di allagamento anche per semplici perdite di acqua dai locali soprastanti e ben areati, al fine di evitare che la temperatura salga troppo e danneggi i *server* stessi.

Altro punto importante è il verificare che i dati siano memorizzati sui *server* e non nelle singole postazioni di lavoro. In caso di guasto di una postazione di lavoro risulterà molto difficile recuperare i dati in essa contenuti, mentre di norma i dati presenti sui *server* vengono salvati periodicamente su appositi supporti, garantendo una più facile strategia di recupero delle informazioni perse.

3. Codici d'accesso

Ho già accennato prima al problema dei codici d'accesso a computer ed applicazioni. Questi codici devono essere determinati secondo un metodo che permetta di renderli estremamente difficili da individuare, ma nel contempo facili da ricordare. Ci si potrebbe domandare perché utilizzare codici d'accesso complicati. Il motivo è presto detto. Su Internet esistono programmi in grado di provare infinite *password* al fine di accedere al sistema informatico: normalmente questi prodotti utilizzano dei dizionari in cui sono elencate molte se non tutte le parole di senso compiuto di una lingua, comprese le declinazioni dei verbi e le differenze fra maschile, femminile, singolare e plurale. Ad esempio, la lingua italiana è composta da circa settecentomila lemmi ed un programma di quelli citati prima non impiega moltissimo tempo a provarli tutti. Se però ho usato una parola che non ha senso compiuto in italiano, questi programmi falliscono nei loro tentativi e possono solo basarsi su tecniche di forza bruta (provo tutte le combinazioni di caratteri possibili): secondo tale modalità, però, impiegano moltissimo tempo. Ecco quindi spiegato perché è anche molto importante sostituire i

propri codici d'accesso periodicamente, in modo da vanificare il lavoro svolto da questi programmi fino a quel momento, costringendoli a ricominciare il tutto da capo.

4. Problemi di sicurezza all'interno del sistema informatico

In molti sono convinti che i problemi di sicurezza arrivino principalmente dall'esterno, invece oramai la maggior parte dei problemi arriva dall'interno dei sistemi informatici. Un virus che apre le porte dall'interno può fare molti danni, così come un programma che "cattura" tutto quello che viene digitato sulla tastiera e poi spedisce il risultato all'esterno, fornendo così, ad esempio, codici d'accesso a siti e sistemi che poi diventano facilmente preda di pirati informatici. Una volta che si ha accesso dall'esterno ad uno solo dei computer collegati ad una rete locale non è difficile accedere ad altri sistemi e ai *server* visto che solitamente le difese in questo caso sono basse, se non nulle e ci si fida dei computer della rete locale. Se poi i sistemi operativi usati sui computer in rete non sono stati pensati per attività lavorative, ma, ad esempio, sono versioni pensate per casa o per giocare, la cosa diventa ancora più facile e quindi pericolosa. Non parliamo dei problemi a cui si può andare incontro se i *server* o i computer sono accessibili fisicamente e non sono adeguatamente protetti come accennato poco fa. Qualcuno potrebbe portarsi un CD con un sistema operativo, riavviare un computer e trovarsi sulla rete locale con un sistema ricco di strumenti comodi per attività illecite o comunque non previste dai gestori della rete locale. Inoltre avendo accesso fisico ai *server* un malintenzionato potrebbe rubare dati anche prelevando un disco, e la cosa non è detto che crei problemi immediati, nel senso che il *server* potrebbe continuare a lavorare ugualmente.

5. Problemi di sicurezza derivanti dall'esterno del sistema informatico

Vediamo ora alcune cose sulla sicurezza perimetrale. Capita di sentir affermare che i *firewall*, cioè quei sistemi che fanno da filtro fra la rete locale e l'esterno, sono la soluzione ai problemi di sicurezza. Purtroppo non è così: infatti, i *firewall* fanno solo da filtro su quali operazioni sono permesse e quali no, ma su quelle permesse non fanno ulteriori controlli. Mi spiego meglio con un esempio. Se è stato deciso che il *firewall* deve lasciar passare la posta elettronica, questa passa tutta compresa quella che ha allegati contenenti virus. Il *firewall* non è in grado di fermare i virus: a tale attività è, infatti, preposto l'antivirus.

È poi di fondamentale importanza mantenere aggiornati tutti i sistemi in uso, in quanto tutti sono soggetti a problemi di sicurezza e tutti i giorni gli esperti del settore scoprono nuovi metodi per aggirare le protezioni che i singoli prodotti e i sistemi hanno. Le case produttrici di software rilasciano periodicamente dei correttivi, chiamati in gergo *patch*, da applicare ai sistemi in modo da mantenerne alto il livello di sicurezza. Sicuramente ricorderete che qualche anno fa un virus bloccò per una intera giornata la maggior parte degli uffici postali italiani. Ebbene se sui computer delle poste fossero stati installati i correttivi che erano disponibili, il virus non avrebbe attecchito.

Nella gestione dei *firewall* è molto importante curare la configurazione non solo delle protezioni dall'esterno verso l'interno, ma anche nella direzione opposta. Esempio: se si vieta ai computer della rete locale di inviare posta direttamente su Internet e li si costringe a passare per il *server* di posta aziendale, si migliora subito la sicurezza. Infatti un eventuale virus che cercasse di propagarsi tramite posta elettronica non ci riuscirebbe, trovando la strada d'uscita bloccata. Lo stesso discorso vale per tutti quei *malware*

(programmi dal contenuto maligno) che si possono installare all'insaputa dell'utente e cercano poi di inviare informazioni su Internet. Se il *firewall* è ben progettato, tali operazioni non potranno funzionare e ciò permetterà di aumentare alquanto la sicurezza della rete locale. Inoltre, con questa tecnica è possibile bloccare eventuali malintenzionati che cercano di entrare nella rete. Infatti, anche se riuscissero ad entrare, le risposte non arriverebbero (in quanto bloccate dal *firewall*) e il loro attacco sarebbe comunque vano.

Per quanto riguarda i virus può sembrare strano che ancora se ne parli. Oramai tutti sanno che l'antivirus è indispensabile, ma a giudicare dalla quantità di virus che circolano, ci deve essere qualche cosa che ancora non funziona. Troppi sono i computer su cui l'antivirus, pur essendo installato, o non è in funzione o non è stato adeguatamente aggiornato. In questi casi gli utenti hanno un falso senso di sicurezza in quanto sono convinti di essere protetti e non si rendono conto che invece il loro computer è esposto, se non già contagiato, dall'ultimo virus di recente diffusione. I virus non andrebbero sottovalutati, come purtroppo troppo spesso si fa, in quanto c'è il rischio che uno di essi in uscita da un computer causi dei danni presso terzi e ci si potrebbe trovare costretti a risarcire il danno causato. Nel nostro ordinamento i danni causati da virus sono considerati reato (art. 615-*quinquies* c.p.). Di più, dopo l'11 settembre negli Stati Uniti l'attività di danneggiamento di sistemi informatici, ad esempio causata da un virus, potrebbe essere equiparata ad un atto terroristico (vedasi il *Patriot Act* del 2001). È quindi fondamentale che gli utenti abbiano la consapevolezza e la capacità di capire se l'antivirus sia in funzione o meno e quindi essere loro stessi a segnalare ai tecnici responsabili che qualche cosa non funziona. Gli utenti finali possono in questo caso essere di grande aiuto per migliorare il livello di sicurezza dell'azienda. Rendere consapevoli gli utenti che non si deve fare "clic" su tutto ciò

che arriva per posta elettronica (statistiche dicono che almeno il 15% degli utenti non si pone domande e apre qualsiasi allegato) è sicuramente un modo per ridurre drasticamente i problemi legati ai virus e non solo.

6. La posta indesiderata

Parliamo ora di *spam*, la posta spazzatura, divenuta una "piaga mondiale". Negli Stati Uniti ci sono utenti che hanno smesso di utilizzare la posta elettronica proprio per via del troppo tempo perso a discriminare fra i vari messaggi. Lo *spam* è l'unica forma di pubblicità che viene pagata da chi la riceve e non da chi la invia. Infatti il mittente manda un solo messaggio di posta che poi raggiunge milioni di altre caselle. È l'utente finale che perde tempo e spende dei soldi per scaricare e visualizzare messaggi che non gli interessano e che non ha mai chiesto.

La prima domanda che gli utenti si pongono è dove hanno trovato gli indirizzi di posta elettronica a cui questi soggetti scrivono. La risposta è semplice: su Internet. Nella navigazione sulla rete, nel partecipare a *forum* di discussione, nell'inviare posta elettronica ad amici e conoscenti si lasciano tracce che possono poi essere ricercate da appositi programmi che "spazzolano" il Web a caccia di indirizzi di posta elettronica da inserire in banche dati che vengono poi vendute a personaggi senza troppi scrupoli. I virus, le catene di "Sant'Antonio", i messaggi inviati a molti utenti possono trasformarsi inconsapevolmente in metodi per fornire a terzi il proprio indirizzo di posta elettronica. Si deve quindi fare molta attenzione ad esempio a chi si invia una mail ricevuta e sarebbe buona norma ripulirla degli indirizzi di posta elettronica se questi non sono funzionali alla comunicazione.

Spesso i messaggi di *spam* contengono un *link* o un indirizzo di posta a cui è possibile chiedere di non ricevere più comunicazioni

del genere. È importantissimo non rispondere mai a questo genere di messaggi. La finalità di chi li manda è che essi vengano letti da qualsivoglia persona in quanto quella casella rappresenta un ottimo candidato per l'invio di ulteriore pubblicità. In pratica rispondere ad un messaggio di *spam* è equivalente a chiederne molti altri.

Un altro problema legato allo *spam* è dato dalla visualizzazione dei messaggi di posta elettronica in formato "html" (come se fossero pagine Web). Tale modo di visualizzazione, anche solamente nell'anteprima, è pericoloso in quanto esistono messaggi che contengono immagini che devono essere prelevate su Internet e permettono ai gestori dei siti di ricostruire chi ha visualizzato il messaggio di posta elettronica inviato. Sarebbe molto opportuno abilitare il proprio programma di posta alla visualizzazione esclusivamente di ciò che è contenuto nel messaggio, senza la possibilità di collegarsi all'esterno (ad esempio, per prelevare immagini).

7. Punti di accesso alla rete locale

Da quanto detto finora credo sia evidente come si debba fare attenzione anche ai punti d'accesso alla rete locale, onde evitare che qualcuno colleghi un computer, di cui non si conoscono i livelli di sicurezza, e "porti in casa", anche involontariamente, dei problemi. Le minacce oggi più diffuse sono sicuramente i virus, come i cosiddetti "troiani", cioè programmi che si collegano all'esterno e aprono un canale all'eventuale malintenzionato il quale riesce così ad entrare in una rete locale anche se dotata di discrete protezioni periferiche.

Le reti senza fili (*wireless*) si stanno diffondendo sempre più, ma capita di trovare reti senza fili con problemi di sicurezza. Una delle caratteristiche principali di una rete senza fili è proprio quella di non avere confini ben delimitati ed è perfettamente normale che la

rete sia presente anche nei palazzi vicini. Proprio per questa sua caratteristica è necessario far sì che alla rete possano accedere solo persone o dispositivi noti. È necessario quindi utilizzare livelli di sicurezza molto elevati, visto che non è possibile sapere a priori chi e da dove si connetta ad essa.

Un altro aspetto da non sottovalutare è la presenza di modem o apparati per il collegamento verso altre reti esterne. Tali apparati vanno controllati periodicamente e si deve lavorare per cercare di ridurne il più possibile il numero. Essi rappresentano un buco di sicurezza nella struttura aziendale permettendo collegamenti non protetti ad altre reti. Come già rilevato ad altro proposito questo tipo di debolezza rischia di vanificare tutta l'attività fatta per proteggere la rete aziendale.

8. Copie per ripristino dati

Abbiamo visto in questa veloce carrellata tutta una serie di possibili problemi che potrebbero portare al danneggiamento di dati. Diventa quindi fondamentale avere una copia dei dati archiviata da qualche parte. Salvare i dati, con un qualsiasi sistema, non è tuttavia sufficiente, in quanto ci si deve chiedere dove tali dati vengano poi conservati. Capita infatti con una frequenza preoccupante di trovare i supporti con i dati salvati che rimangono se non dentro i *server* stessi nelle immediate vicinanze. Ciò non è sicuro in quanto, così facendo, si è protetti solo da errori del *server* e non da eventuali problemi più seri, come ad esempio un incendio del locale dove si trovano i *server*. In questo caso oltre ai dati si rischia di perdere anche le copie di salvataggio. Un altro problema abbastanza frequente è la mancata verifica che quanto salvato sia effettivamente tutto quello che serve per un eventuale ripristino. Una tale verifica serve ad evitare di scoprire, quando è ormai troppo tardi, che qualche cosa che serviva sui supporti di salvataggio non c'è. Vanno quindi previste ed

eseguite prove di recupero dati. Altra importante verifica da fare è che sui supporti vengano effettivamente scritti dati che poi possano essere letti. Anche in questo caso capita di trovare sistemi di salvataggio che sembrano scrivere sui supporti, ma che in realtà si rivelano inefficaci. Da ultimo è importante che qualcuno periodicamente controlli il buon funzionamento del sistema di salvataggio.

9. Problemi connessi alla navigazione

I problemi legati alla navigazione Internet nelle aziende sono simili a quelli elencati sopra a cui si aggiunge la navigazione su siti non consoni all'attività lavorativa. Le ditte produttrici di prodotti di controllo della navigazione affermano che l'accesso ai siti pornografici avviene per oltre il 50% dal lunedì al venerdì tra le 9 e le 17, quindi in pieno orario di lavoro. Inoltre capita con una certa frequenza che gli utenti si colleghino a siti di vario tipo per scopi personali e non legati alla loro attività professionale. Per non parlare di chi utilizza le risorse aziendali per scaricare materiale di vario tipo. Esistono poi utenti che, quando hanno necessità di installare qualche applicativo, anziché chiedere ai propri superiori si arrangiano scaricando dalla rete ciò di cui hanno bisogno. È evidente che tutti questi comportamenti sono potenziali fonti di problemi, sia di natura legale, nel caso di accesso a siti di un certo tipo o di scaricamento di materiale protetto da diritto d'autore, ma anche da un punto di vista della sicurezza dell'azienda (ad esempio, l'installazione di programmi gratuiti o in prova che molte volte al loro interno contengono programmi di pubblicità non sempre sono rispettosi della riservatezza degli utenti). In questo caso è possibile vengano inviate all'esterno informazioni preziose o riservate dell'azienda. Tutta questa attività si traduce in costi, i quali derivano sia dal tempo distratto all'attività lavorativa, sia (soprattutto) da costi

della banda di connessione alla rete Internet, risorsa ancora limitata e piuttosto cara. Alcune aziende hanno cercato di risolvere il problema non concedendo più l'accesso ad Internet ai propri collaboratori, ma ritengo sia una strada sbagliata. È preferibile, anche se un po' più laborioso, dare delle regole e poi perseguire chi eventualmente queste regole non le rispetta. Il primo passo resta comunque quello di preparare delle regole e spiegarle ai propri utenti.

10. Truffe on-line

Come nel mondo reale, anche su Internet avvengono diverse truffe. Fra queste ultimamente il cosiddetto *phishing* ha assunto proporzioni preoccupanti. Questa è una tecnica che rientra fra quelle denominate "*social engeenering*", cioè delle tecniche che fanno leva su meccanismi psicologici per cercare di convincere l'utente a consegnare spontaneamente codici d'accesso, in questo caso del proprio sistema bancario, piuttosto che i dati della carta di credito o altro. Tipicamente il *phishing* viene posto in essere con l'invio a milioni di utenti di un messaggio di posta elettronica che sembra essere partito da una banca o da altro istituto con cui i destinatari dei messaggi potrebbero avere rapporti per via informatica, nel quale si chiede di accedere al *link* indicato nel messaggio per riconfermare i propri codici d'accesso, piuttosto che per accedere ad un nuovo *server* più sicuro e cose del genere. Se l'utente fa "clic" sul sito indicato nel messaggio si ritrova su un altro che assomiglia molto a quello originale, ma il cui nome è leggermente diverso: questo è in realtà una copia preparata *ad hoc* per perpetrare la truffa. Immettere i propri dati in questi siti equivale a consegnarli a malintenzionati che provvedono immediatamente ad utilizzarli per svuotare conti correnti, carte di credito o per accedere a siti. L'unica difesa da questi tipi di attacchi è il non fidarsi mai ed evitare di fare clic all'interno di messaggi, ma a volte i messaggi sono così ben fatti che

è veramente difficile anche per un esperto capire se si tratta di una truffa o di un messaggio reale. Tuttavia se si vuole controllare la veridicità del messaggio, è meglio collegarsi al proprio sito bancario come si fa normalmente, partendo da un *link* memorizzato non nel messaggio e verificare se lì ci sono informazioni dello stesso tenore di quelle presenti nel messaggio ricevuto. In alternativa prima di immettere dati è bene fare una telefonata e verificare se quanto richiesto nel messaggio corrisponde a verità.

Una variante del *phishing* ancora più subdola è il cosiddetto *pharming*, una tecnica che sfrutta delle vulnerabilità del DNS, quel sistema che permette di usare dei nomi anziché numeri sulla rete *Internet*, allo scopo di far finire gli utenti su siti costruiti appositamente senza che essi se ne accorgano.

11. Firma digitale, smart card *ed altri dispositivi di verifica dell'identità dell'utente*

La firma digitale è uno strumento che si sta lentamente diffondendo. Anche se le *smart card* sono sicure potrebbero non esserlo i computer usati per apporre la firma o per verificarla. Infatti il meccanismo di firma digitale si basa su una chiave, detta privata, che non deve per nessun motivo circolare. Tuttavia l'accesso alla *smart card*, dove tale chiave è conservata, avviene mediante un "codice pin" inviato dal computer in uso. Se il computer non è sicuro, è possibile che il "pin" venga catturato da malintenzionati che potrebbero utilizzare la carta, allorquando essa venisse inserita nel lettore per firmare documenti fasulli o modificare documenti. Inoltre, la *smart card* è molto simile ad una tessera bancomat o ad una carta di credito ed è quindi soggetta agli stessi problemi che tutti già conosciamo, come ad esempio lo smarrimento o il furto della carta stessa. Ricordiamoci però che su questa carta è memorizzata la firma dell'utente e non solo l'accesso ad una parte dei suoi soldi. Credo sia

molto illuminante in questo caso un film di fantascienza intitolato "*The Net*" in cui si intravedono scenari futuri abbastanza inquietanti.

RFID è la sigla di una tecnologia che permette a dei dispositivi piccolissimi e flessibili, che quindi possono essere messi praticamente dappertutto senza essere visibili, di identificare oggetti e/o persone. Tali dispositivi vengono attivati da un apposito lettore che provvede a leggerne il contenuto. È importante notare che il lettore non necessita di contatto fisico con il dispositivo, ma solo che i due apparati siano relativamente vicini. Tali dispositivi sono oggi utilizzati ad esempio nel *Telepass* per l'addebito del costo della tratta autostradale, su moltissimi prodotti come sistema anti-taccheggio, nei biglietti e abbonamenti per l'accesso ad impianti sportivi, piuttosto che per l'accesso a spettacoli. I rischi che questa tecnologia nasconde sono dovuti *in primis* al fatto che, essendo il dispositivo molto piccolo, è possibile nasconderlo: di conseguenza una persona potrebbe averne addosso uno senza rendersene conto. Tenuto conto che non è necessario un contatto fisico con il lettore, essendo sufficiente entrare nel suo campo, non è possibile accorgersi quando il dispositivo viene letto. Ancora, la capacità della memoria interna al dispositivo è in aumento e a breve potrà contenere molti più dati del solo numero identificativo. È evidente quindi come non sia difficile tracciare la posizione e gli spostamenti delle persone anche a loro insaputa. Diventa dunque necessario disporre di meccanismi che permettano a tali dispositivi di essere identificabili e disattivabili dall'utente, in modo da poter tutelare la riservatezza.

12. Conclusioni

In conclusione i problemi legati alla sicurezza nell'uso degli strumenti informatici e di comunicazione di cui abbiamo visto una veloce carrellata sono principalmente legati all'organizzazione ed alla consapevolezza che gli utenti hanno dello strumento che stanno

utilizzando. La tecnologia, che in se non è né buona né cattiva, dovrebbe essere utilizzata in modo consapevole e dovrebbe essere vista sempre come un aiuto e non come la panacea per risolvere ogni problema. La tecnologia non deve sostituirsi alle scelte che spettano alle persone.

SICUREZZA: IL RUOLO DEL SOFTWARE LIBERO E DEL SOFTWARE OPEN SOURCE

Andrea Rossato

SOMMARIO: *1. Software libero e software open source. - 2. Software libero come modello di* governance. *- 3. Globale e locale. - 4. End-to-end. - 5.* Governance *e sicurezza.*

1. Software libero e software open source

Il software libero nasce tra il finire degli anni settanta ed il cominciare degli ottanta come una reazione ad un mutato quadro giuridico che vede, sostanzialmente, l'inserimento del software tra le categorie di opere tutelate dal diritto d'autore ai sensi della Convenzione di Berna[1].

Tale mutamento snatura quello che era stato precedentemente il modo di concepire le scienze informatiche le quali, all'interno delle comunità accademica, in modo particolare dei grandi centri di ricerca nord americani, erano caratterizzate da una forma tipica, nella ricerca scientifica, di condivisione del sapere. Era quindi pratica comune, tra i ricercatori e gli scienziati che affollavano prestigiose università come il MIT o Berkeley, scambiare il software così come, in altri ambiti scientifici, ci si scambiano articoli, pareri e quant'altro.

Il mutato quadro giuridico ed il contestuale svilupparsi di una vera e propria industria del software, la quale si accompagna alla nascita di un mercato dell'informatica di massa a seguito della produzione dei primi modelli di personal computer a partire dalla seconda metà degli anni settanta, hanno l'effetto di modificare la

[1] Per una ricostruzione più dettagliata di queste vicende ci permettiamo di rinviare al nostro *Diritto e architettura nello spazio digitale – Il ruolo del software libero*, Padova, 2006, spec. cap. 3.

percezione che, nell'ambito di questa comunità scientifica, si ha del software.

Non è quindi un caso che sia un ricercatore del MIT, Richard Stallman, a maturare la convinzione che, per preservare le idealità che avevano caratterizzato l'informatica come una disciplina accademica in cui si mescolano ricerca di base e ricerca applicata, fosse necessario, visto il mutato assetto istituzionale, predisporre un *framework*, mediante la diffusione di una licenza d'uso e, quindi, di un contratto, la GNU *General Public License*, che fosse in grado di perpetuare il principio della condivisione del sapere che aveva in precedenza connotato la produzione del software.

L'idea di Stallman è molto ambiziosa. Egli si propone di creare un intero sistema operativo che consenta l'utilizzo di un computer con software interamente libero, caratterizzato, cioè, da un modello distributivo che conferisca, e allo sviluppatore e all'utilizzatore, un insieme minimo di libertà sul sistema stesso, libertà che consentano loro di studiare, modificare, condividere e distribuire, senza ulteriori limiti, il programma in questione. In ultima analisi si tratta di concedere all'utilizzatore del computer la possibilità di modificarne il funzionamento, mediante il conferimento della facoltà di apportare migliorie al software senza il consenso del suo autore, il tutto nel quadro di legalità posto in essere dal contratto di licenza d'uso. Tale licenza, proprio in virtù del mutato assetto giuridico che conferisce all'autore i diritti esclusivi derivanti dal *copyright*, è quindi un atto in grado di porre in essere una relazione giuridica, caratterizzata da una certa reciprocità in quanto a facoltà, obblighi e soggezioni, il cui scopo principale è garantire alle parti in causa un ammontare minimo di libertà irrinunciabili. L'elemento centrale che caratterizza il progetto GNU, l'acronimo ricorsivo (GNU's not Unix) che lo identifica, è quindi, nell'accezione di Stallman, la libertà del fruitore di software.

Il progetto, concepito nei primi anni ’80, reso pubblico nel 1984, è coronato da successo solo nei primi anni ’90: il 1991 vede la nascita di Linux, un kernel utilizzabile nell’ambito del sistema GNU, che ormai comprendeva quasi tutti gli elementi che caratterizzano un sistema operativo, ad eccezione dell’ultimo rappresentato appunto da Linux. Nel 1995 una transazione extragiudiziale pone fine ad una controversia tra la University of California at Berkeley ed AT&T prima, Novel poi. Tale transazione consentirà alla prima la distribuzione di un sistema operativo, anch’esso interamente libero, derivato dal sistema Unix e denominato BSD (acronimo di *Berkeley Software Distribution*), dal quale traggono origine sistemi operativi *Unix-like* come FreeBSD, OpenBSD e NetBSD.

Giunti a metà degli anni ’90, pertanto, la comunità degli sviluppatori che si era radunata attorno al progetto di Stallman, ed ad altri progetti nati in ambito accademico come nel caso di BSD, è in grado di offrire al pubblico degli utilizzatori di software un sistema operativo interamente libero, distribuito, cioè, con licenze che garantiscono al fruitore quel nucleo di libertà cui sopra si accennava.

È sull’onda di questo successo che, nel 1998, nasce la locuzione *software open-source*[2]. Questa nuova etichetta, che starebbe ad indicare ciò che prima si conosceva con il nome di *free software*, viene adottata con l’esplicito scopo di fare del proselitismo, in favore di questa categoria di programmi per elaboratore, nell’ambito del settore commerciale. Ed è nel tentativo di rendere questa tipologia di software appetibile anche al settore commerciale ed industriale che si fa appello ad una presunta superiorità tecnica del software libero, ora *open-source*, su quello proprietario – così vengono chiamati quei programmi la cui distribuzione avvenga

[2] Ad opera di E. Raymond. Si veda E. RAYMOND, *Goodbye, “free software”; hello, “open source”*, http://www.catb.org/~esr/open-source.html, 1998. Si veda anche E. RAYMOND, *The Cathedral and the Bazaar*, http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/2000

mediante il ricorso a licenze che pongano forti limiti alle attività che l'utilizzatore può con essi compiere –, superiorità derivante dalla diversa modalità di sviluppo che caratterizza il primo.

Il software libero/*open-source* è spesso, ma non necessariamente, caratterizzato da un sistema collaborativo decentrato e distribuito di produzione. Inoltre, essendo il codice sorgente liberamente visionabile – questo è un requisito necessario affinché le libertà a cui sopra si accennava siano effettive e non meramente declamate –, esso può essere sottoposto ad una revisione critica da un numero di persone estremamente elevato, a differenza di quanto possa accadere se un programma viene sviluppato nell'ambito di un'organizzazione imprenditoriale chiusa che voglia mantenere su di esso i diritti esclusivi e le prerogative che nascono dal diritto d'autore e dal segreto industriale. I sostenitori del *software open-source* affermano quindi che questo modello di sviluppo ha il vantaggio di rendere il software più robusto e sicuro, attingendo argomenti retorici da discipline quali l'economia, che mostra la superiore efficienza di istituzioni decentralizzate su quelle rigidamente centralizzate e gerarchiche – si pensi al dibattito mercato/pianificazione[3].

Si può incidentalmente notare come, se sul piano teorico simili argomenti esercitino il loro fascino, su quello pratico essi rischino di divenire petizioni di principio. Se è infatti corrispondente al vero che vi sono progetti dotati di elevata visibilità e che attirano un numero molto elevato di ricercatori e programmatori esperti, vero è che ciò rappresenta maggiormente l'eccezione che non la regola. Non mancano infatti, sono invero il numero maggiore, programmi creati da una cerchia estremamente ristretta di individui, i quali prestano la loro opera gratuitamente e, quindi, saltuariamente. Che costoro possano competere con imprese, anche di piccole

[3] Si veda RAYMOND, *The Cathedral and the Bazaar*, cit.

dimensioni, che possono investire nella ricerca e sviluppo risorse certamente maggiori, ci par invero di poterlo dubitare.

2. Software libero come modello di governance

Se si prescinde dal dibattito sul miglior sistema di sviluppo, e se si prescinde anche dalla contrapposizione, dal vago sapore ideologico, tra i sostenitori della superiorità etica e tecnica del software libero e di quello *open-source* su quello proprietario, si può forse analizzare il problema delle relazioni tra software libero e proprietario a partire dalle conseguenze pratiche delle idealità che caratterizzano il primo. In tal caso il software libero si verrebbe caratterizzando come un modello di *governance* delle risorse informatiche, un modello decentralizzato ove all'utente finale è dato pieno potere sulla configurazione del sistema da costui utilizzato.

Una tale impostazione del problema, credo, potrà risultare utile nell'affrontare lo specifico tema della sicurezza informatica e delle modalità con le quali essa debba essere perseguita.

L'appello alla libertà, e non alla superiorità tecnica, si configura infatti come un discorso relativo alla relazione tra l'utilizzatore e la risorsa informatica. Il software libero è volto a fornire a costui pieno accesso, e, quindi, pieno potere sulla singola risorsa. Quello che nelle pagine che seguono si vuole analizzare è, pertanto, come un tale modello possa essere generalizzato per affrontare il problema della *governance* globale delle risorse informatiche, a maggior ragione se connesse in rete. In altri termini, non intendo entrare nel merito del dibattito sulla maggior o minor sicurezza intrinseca del software libero. Voglio invece cercare di comprendere come le questioni relative alla sicurezza entrino nel dibattito sulla *governance* delle risorse informatiche, al fine di analizzare quale contributo il software libero, che, si è detto, rappresenta un sistema di *governance* locale, possa offrire. Una tale

impostazione si fonda sulla constatazione di come la *governance* delle risorse informatiche abbia la capacità di plasmare lo spazio digitale, determinandone lo sviluppo[4].

3. Globale e locale

Introdurrò questo argomento raccontando una vicenda che, un paio di anni fa, destò un certo clamore animando un interessante dibattito sulle relazioni tra le politiche commerciali e quelle di sicurezza. Nel 2004 si era sparsa la voce, sui mezzi di informazione, che Microsoft intendesse cambiare la propria posizione relativamente alla distribuzione degli aggiornamenti ai propri sistemi operativi. Dopo la pubblicazione di Windows XP, il primo grosso pacchetto di aggiornamento, denominato *Service Pack 1*, era stato reso liberamente disponibile ai soli utenti che avessero installato sul proprio computer una copia legittimamente acquistata del noto sistema operativo. Tutti coloro che ne avessero una copia abusivamente duplicata sarebbero stati esclusi. Secondo indiscrezioni di stampa, invece, il *Service Pack 2* sarebbe stato distribuito a chiunque avesse una copia installata di Windows XP, fosse stata questa munita o meno di regolare licenza d'uso[5]. La notizia era però priva di fondamento e, dopo qualche giorno, fu smentita dalla diretta interessata[6].

Le ragioni per le quali Microsoft abbia deciso di non rendere disponibile gli aggiornamenti a chi non fosse titolare di una licenza d'uso sono evidenti e possono essere facilmente catalogate tra le attività di "massimizzazione del profitto" cui un'impresa si deve

[4] Si veda ROSSATO, *Diritto e architettura nello spazio digitale – Il ruolo del software libero*, cit.

[5] Così annunciava C. HIAN HOU, *Security for all*, May 5, 2004, http://computertimes.asia1.com.sg/news/story/0,5104,2292,00.html

[6] Si veda W. CHAI, *Microsoft changes SP2 course on piracy, CNETAsia, ZDNet News*, May 11, 2004.

necessariamente dedicare. Se è pertanto ovvio che essa decida di prendere questo corso di azioni, quel che ci si deve domandare è quali siano le conseguenze di carattere globale di una simile decisione. Per dirla con un noto esperto di sicurezza informatica, «[t]he security of your computer and your network depends on two things: what you do to secure your computer and network, and what everyone else does to secure their computers and networks. It's not enough for you to maintain a secure network. If everybody else doesn't maintain their security, we're all more vulnerable to attack»[7]. Pertanto, negare gli aggiornamenti, in specie quelli legati alla sicurezza, agli utenti di versioni "pirata" di Windows significa aumentare l'insicurezza anche degli utenti legittimi del sistema operativo, per via del fatto che l'ambiente nel quale il loro sistema si trova è meno sicuro.

La decisione di Microsoft, adottata in risposta ad incentivi che agiscono localmente, ha conseguenze di carattere globale. Potremmo definire queste conseguenze una forma di esternalità, ma non intendo soffermarmi troppo, in questa sede, sulla loro natura.

Si potrebbe argomentare, contro le osservazioni or ora fatte, che casi di esternalità di questo genere sono evenienza comune e che, talvolta, in particolar modo nell'eventualità di esternalità negative, il diritto interviene con una qualche forma di regolamentazione. Ma ciò non considera ancora una peculiarità specifica di reti informatiche come Internet.

Si è soliti intendere Internet come "la" rete globale. Una tale definizione è però estremamente forviante nel descrivere e qualificare la natura di Internet. Se volessimo tentare di coglierne l'aspetto più sostanziale, dovremmo dire invece che essa è la globalità delle reti locali interconnesse. Internet, infatti è

[7] Così B. SCHNEIER, *Microsoft and SP2*, Giugno 2004, http://www.schneier.com/crypto-gram-0406.html#4

un'architettura di interconnessione. Ma ciascuna rete interconnessa ha, in verità, un suo proprietario, nel senso che le apparecchiature che la esprimono sono beni sui quali una qualche persona, o ente, vanta un diritto esclusivo di proprietà, e costei avrà la facoltà di decidere come quelle apparecchiature dovranno comportarsi.

Da ciò, per quel che concerne il ragionamento che andavo tessendo, deriva la constatazione di come la *governance* globale di Internet altro non sia che la sommatoria di *governance* locali.

Una tale modalità di governo di un sistema complesso discende ovviamente dalle scelte operate in sede di progettazione del sistema stesso. E, d'altro canto, le scelte operate, nel caso specifico in questione, furono volte proprio a creare quello specifico sistema di *governance*, per ragioni che vale la pena, seppur brevemente, analizzare.

4. End-to-end

Internet si configura come un'architettura di rete aperta, il che sta a significare che la sua struttura è quella di una rete di reti, ciascuna delle quali possa essere progettata, sviluppata ed implementata con tecnologie scelte arbitrariamente. Per la comunicazione tra le varie reti si decise l'adozione di un meta-livello di comunicazione, definibile come un'architettura di interconnessione (*Iternetworking Architeture*), una serie di protocolli che consentissero il transito dei pacchetti dati attraverso le singole reti di cui Internet sarebbe stata formata, mediante interfacce, denominate *gateway*, poste ai loro limiti[8]. Una tale soluzione fu proposta da Vinton Cerf e Robert Kahn in un celebre lavoro del 1974 nel quale si delineavano le modalità di funzionamento di una simile

[8] Si veda B. M. LEINER & V. G. CERF & D. D. CLARK & R. E. KAHN & L. KLEINROCK & D. C. LYNCH & J. POSTEL & L. G. ROBERTS & S. WOLFF, *A Brief History of the Internet, version 3.32*, http://www.isoc.org/internet/history/brief.html

architettura e se ne proponevano gli elementi basilari: il sistema dei *gateway* ed i protocolli necessari[9].

I protocolli che esprimono Internet furono definitivamente codificati nel 1981[10], molto tempo prima che questa divenisse un fenomeno di massa. In essi si faceva applicazione di un principio, poi conosciuto come argomento *end-to-end*[11], in base al quale un sistema informatico deve implementare le funzionalità più complesse ai sui punti terminali, nel nostro caso le singole risorse informatiche, i singoli computer o le singole reti di cui Internet si compone. In tal modo l'architettura di interconnessione, lo spazio che separa i punti terminali, può essere estremamente semplice, svolgendo il minor numero di funzioni possibile, con ovvi vantaggi in sede di implementazione, lasciando, al contempo, impregiudicati tutti gli usi futuri ed eventuali dell'architettura stessa. Detto altrimenti, negli anni settanta non si sapeva come i protocolli da cui era destinata a nascere Internet sarebbero stati utilizzati. Nessuno, molto probabilmente, immaginava che vi sarebbe stata, un giorno, una struttura come la *World Wide Web* fruibile mediante un *browser*, ed in grado di portare nelle nostre case testi, immagini, suoni, ecc. Se invece l'architettura di connessione fosse stata progettata per uno specifico uso, i protocolli sarebbero stati configurabili in modo tale da esser resi estremamente efficienti solo per quel determinato uso, probabilmente a discapito di altri usi possibili.

Si comprende allora come l'argomento *end-to-end*, il mantenere, cioè, le funzionalità più avanzate, anche di sicurezza,

---

[9] V. CERF & R. KAHN, *A Protocol for Packet Network Interconnection*, 22 *IEEE Transactions on Communications*, 1974, 637.

[10] Ad esempio J. POSTEL, *Internet Protocol*, RFC 791 (Standard), 1981, http://www.ietf.org/rfc/rfc791.txt, e J. POSTEL, *Transmission Control Protocol*, RFC 793 (Standard), 1981, http://www.ietf.org/rfc/rfc793.txt

[11] J. H. SALTZER & D. D. CLARK & D. P. REED, *End-to-end Arguments in System Design*, 2 *ACM Transactions in Computer Systems*, 4, 1984, 277.

quanto più possibile nei punti terminali dell'architettura, vicino all'utilizzatore, sia in ultima analisi anche una forma di *governance*, nel senso che a ciascuna rete locale e a ciascuna risorsa sarebbe stata lasciata la facoltà di decidere autonomamente quali funzioni implementare. In secondo luogo, un tale argomento garantiva che non si ponessero discriminazioni tra usi possibili, e che non si operassero distinzione tra usi buoni o cattivi, adeguati o meno, dell'architettura, lasciando che emergessero spontaneamente una pluralità eterogenea di usi possibili.

È stata questa scelta di *design* che ha garantito la possibilità di un'evoluzione inattesa e prolifica di Internet, e che l'ha portata all'attuale livello di popolarità[12].

5. Governance *e sicurezza*

Il problema della *governance*, in riferimento a quello della sicurezza, può quindi essere formulato, in relazione al principio di *design* in base al quale Internet fu progettata, come il problema delle modalità attraverso cui le politiche di sicurezza debbano essere implementate. Più specificamente, è necessario far sì che ciascuna risorsa connessa ad Internet implementi delle politiche, autonome, di sicurezza?

O è forse necessario che tali politiche di sicurezza siano attuate a livello di accesso ad una rete locale, dal momento che i singoli utenti non sono, troppo spesso, consapevoli dei costi connessi alla gestione del rischio? In altri termini, non potendo fare affidamento sulle capacità, e sugli incentivi – mancando delle informazioni rilevanti –, dell'utilizzatore medio di un computer, dobbiamo decidere che esso sia esonerato da una tale responsabilità in favore di soggetti più competenti?

[12] Sul punto si veda M. A. LEMLEY & L. LESSIG, *The End-to-End: Preserving the Architecture of the Internet in the Bradband Era*, 48 *UCLA L. Rev.* 925 (2001).

Ma in tal caso si potrebbe obiettare che la competenza e la diligenza degli amministratori delle singole reti locali non è un dato acquisito, e sarebbe quindi preferibile implementare forme di gestione del rischio già a livello di architettura di interconnessione.

Ovviamente una decisione in merito ha un impatto sulla configurazione dell'architettura di interconnessione. Generalizzando, lo spazio digitale che una rete esprime è connotato anche dalla modalità mediante cui una politica di sicurezza viene implementata. *Firewall*, mascheramenti di rete, controllo degli accessi, attività di *logging*, tutto ciò ha un impatto sulla struttura dello spazio digitale e ne determina, pregiudicandone talune, le linee di sviluppo ed evoluzione possibili. Se è stata la deliberata assenza di scelte centralizzate, incorporate nelle strutture più profonde dello spazio digitale, a connotare la progettazione di Internet, assenza deliberata per via della consapevolezza, propria degli studiosi che diedero vita a quella costruzione intellettuale che oggi si esprime nello spazio digitale, dell'incompletezza delle informazioni al tempo disponibili circa gli sviluppi possibili che avrebbero caratterizzato la loro creatura; se è stata quell'assenza, dicevo, a consentirne la crescita costante sino a renderla ciò che oggi appare ai nostri occhi, si comprende allora come il problema della *governance*, nei termini proposti, debba essere affrontato con la medesima prudenza che meritano quelle decisioni che possono avere un effetto di lungo periodo che molto spesso non viene considerato nel momento in cui vengono adottate.

Ma, ancor più rilevante per un giurista, è il fatto che una tale decisione ha un effetto regolatore del comportamento degli individui che quello spazio si trovino a dover frequentare. Se il primo è infatti un problema di natura tecnica, sebbene con risvolti di scelte pubbliche, per usare un'efficace espressione coniata su di un modello anglosassone, pur tuttavia dobbiamo domandarci se chi tali decisioni

si trovi a dover adottare sia dotato degli incentivi adeguati per operare scelte ottimali. Ottimali in due sensi distinti: adeguate alle circostanze ed in grado di operare quel bilanciamento degli interessi che sempre scelte in tema di sicurezza impongono.

Quel che mi domando, in altri termini, è se, scartata l'idea di incorporare direttamente nei protocolli sistemi di sicurezza, ma permanendo la sfiducia nei confronti dell'utente finale, chi si sente delegato ad operare tali scelte abbia tutte le informazioni rilevanti e sia dotato di un sistema di incentivi tale per cui le proprie scelte siano ottimali non solo localmente, ma anche globalmente.

Nell'esempio del caso Microsoft sopra proposto si comprende facilmente come la risposta debba essere negativa.

Ciò non deve invero stupire. Se si analizza quanto accade nello spazio fisico, allora si deve procedere dalla constatazione che le scelte in tema di sicurezza sono propriamente scelte pubbliche, e che esse sono in gran parte sottratte persino alla volontà del legislatore. Si pensi a quanto del nostro diritto costituzionale è svolto al fine di operare un contemperamento tra esigenze di sicurezza ed esigenze di libertà individuale, contemperamento sottratto al Parlamento in quanto, si ritiene, esso potrebbe agire sulla spinta di interessi e preferenze contingenti che rischierebbero di sconvolgere il delicato rapporto tra sicurezza e liberà che il costituente ha sancito.

Per cercare di chiarire questo punto ritengo utile la metafora del mercato. In esso ciascuno di noi compie scelte locali che hanno conseguenze globali, per quanto ridotta possa essere la loro portata, mediante l'allocazione del proprio reddito. Riferendosi ad un pensatore come Hayek si può ricostruire il sistema dei prezzi come una modalità di computazione del valore delle risorse a partire dalle preferenze di ciascuno, oltre che dalla scarsità relativa delle stesse[13]. Il mercato, allora, è un'istituzione dotata di un insieme di regole per

[13] F. HAYEK, *The Use of Knowledge in Society*, in 35 *AER*, 1945, 519.

la determinazione di quel valore.

Il problema è che il mercato è un'istituzione estremamente efficiente, o comunque più efficiente di altre, per la determinazione del valore dello stagno, o delle carote, in relazione al valore di una moneta, ma diventa inadeguata nella determinazione del valore relativo di altri beni, dalla privacy alla libertà. E ciò, si badi, non per via di una sua intrinseca malvagità, ma per il più semplice fatto che il mercato, come ogni altra istituzione, soffre di limiti propri, che vanno dai costi di transazione, alle esternalità, dall'incompletezza dei contratti all'incompletezza degli stessi mercati. Tanto che, storicamente, vediamo che al mercato si affiancano altre istituzioni per compensarne le deficienze. Si pensi alla ricostruzione dell'impresa fornitaci da Ronald Coase[14]. O si pensi allo Stato per quel che concerne la fornitura di quei beni che il mercato non è in grado di garantire, dai beni pubblici ai diritti individuali.

Tornando allora al contributo che il software libero può offrire al dibattito sulla sicurezza, ritengo che le questioni che esso pone relativamente alle risorse locali si possano generalizzare al problema della gestione globale dello spazio digitale. Non è infatti togliendo facoltà, e responsabilità, all'utente finale che si riuscirà a costruire uno spazio digitale più sicuro ed al contempo strutturato in maniera tale da essere portatore dei medesimi principi di libertà che, nello spazio fisico, ci sono garantiti dalla presenza di una istituzione, come quella statuale, obbligata a contemperare esigenze di sicurezza con esigenze di libertà in base a ciò che riteniamo essere a fondamento della sua stessa legittimità, la Costituzione.

Quel che invece abbiamo visto, particolarmente agli albori dell'era digitale, è stato il fiorire di una letteratura che ha visto nello Stato un nemico da tenere distante dal cyberspazio[15]. Se l'era digitale

[14] R. COASE, *The Nature of the Firm*, in 4 *Economica*, 1937, 386.

[15] Penso ad esempio a J. P. BARLOW, *A Declaration of the Independence of*

rappresenta una sfida per questa istituzione, che talvolta ci appare canuta ed inadeguata all'impresa[16], pur tuttavia dobbiamo considerare che essa è stata, negli ultimi secoli, la principale paladina delle libertà individuali, mediante la predisposizione di norme generali ed astratte, il monopolio della forza, e l'allocazione a sé di tutte quelle scelte di carattere regolamentare che incidono sul comportamento degli individui.

Concludo allora ricordando che il dibattito sulla sicurezza è un dibattito politico e che, accanto a temi squisitamente tecnici, rimane, sullo sfondo, il problema della libertà. Senza quest'ultima, il valore intrinseco della sicurezza è assai ben poca cosa.

Cyberspace, http://homes.eff.org/~barlow/Declaration-Final.html, Febbraio, 1996.

[16] Per una disanima delle sfide che attendono lo Stato ed il diritto nell'era digitale si veda G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2002.

IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E LE MISURE DI SICUREZZA

Giulia M. Lugoboni

1. Introduzione

"Non c'è privacy senza sicurezza"[1]. Questa è sicuramente una delle formule ricorrenti fin dagli albori del dibattito sulla sicurezza dei dati personali apertosi ufficialmente in Italia – ormai più di una decina di anni or sono – con la prima legge nostrana sulla protezione dei dati personali, la celeberrima legge 675/1996.

La formula si presta a rendere sinteticamente l'idea che è alla base di questo mio intervento, e cioè che a nulla serve essere estremamente scrupolosi nella delicata fase iniziale del trattamento dei dati personali, adempiendo correttamente, ad esempio, agli obblighi di informativa e di acquisizione del consenso, se poi non si adottano le dovute precauzioni nelle fasi successive del trattamento, e cioè nell'elaborazione e nella custodia dei dati. La questione della sicurezza non riguarda – come spesso, superficialmente, si è portati a credere – soltanto i dati trattati con mezzi elettronici. Alle

[1] Per approfondimenti in materia di privacy e sicurezza, si vedano da ultimo: M. SALA, M. VINCENTI, *Privacy e misure di sicurezza, alla luce del codice in materia di tutela dei dati personali (d.l.vo 30 giugno 2003, n. 196)*, in *Arch. Civ.*, 2004, 717; L. GIACOPUZZI, *Privacy, Le misure di sicurezza*, reperibile all'URL: http://punto-informatico.it/servizi/ps.asp?i=47252; G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Milano, 2003; ID., *La sicurezza dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, vol. I, 112.

importantissime misure di sicurezza c.d. "logiche", legate all'informatica, si affiancano le più classiche misure di sicurezza c.d. "fisiche" (utilizzo di serrature, lucchetti, casseforti, armadi ignifughi, etc.), ma non deve essere dimenticato un altro aspetto di primaria importanza, quello legato alle misure c.d. "organizzative", il cui fine è quello di fare in modo che nell'intera struttura siano adottati comportamenti conformi ai principi della sicurezza e della protezione dei dati personali. In buona sostanza, è inutile approntare un mastodontico apparato di *password*, profili di autorizzazione, *firewall* e quant'altro, se poi si abbandonano i supporti contenenti i suddetti dati personali su una scrivania, alla mercé di chiunque si trovi ad entrare nel locale.

Il tema delle misure di sicurezza nell'ambito della tutela dei dati personali è stato e rimane assai "caldo"; da ormai più di un anno, infatti, stiamo prendendo atto dei numerosi decreti di proroga che si sono susseguiti nei mesi successivi all'entrata in vigore della legge e che hanno, di fatto, posticipato la data di adozione delle nuove misure di sicurezza previste dal d.lgs. 196 del 2003 – il nostro codice in materia di protezione dei dati personali.

Con il nuovo Codice in materia di protezione dei dati personali (comunemente detto "Codice della privacy"), entrato in vigore in data 1 gennaio 2004[2], il quadro delle misure di sicurezza che devono essere adottate nel trattamento dei dati personali è profondamente cambiato: ferma restando la distinzione tra le misure c.d. "idonee", la cui inosservanza espone alla responsabilità per danni, e le misure c.d. "minime", dalla mancata adozione delle quali conseguono, invece, responsabilità di ordine penale, si rileva che, il d.p.r. 318 del 1999 (che presiedeva all'individuazione proprio delle suddette misure minime) è stato completamente sostituito dal

[2] Il decreto legislativo 30 giugno 2003, n. 196 è pubblicato sul supplemento ordinario n. 123/L alla Gazzetta Ufficiale del 29 luglio 2003, n. 174.

"Disciplinare tecnico in materia di misure minime di sicurezza" (il c.d. Allegato B) che costituisce parte integrante del Codice.

2. Il Codice e le misure di sicurezza

La legge prescrive che gli operatori privati e pubblici, definiti "titolari del trattamento"[3], prima di iniziare qualsiasi operazione di trattamento, debbano obbligatoriamente adottare una serie di misure di sicurezza per custodire e controllare i dati raccolti, al fine di prevenire i rischi di lesione dei diritti dell'interessato.

Le disposizioni che disciplinano l'aspetto della sicurezza nel trattamento dei dati personali sono contenute nella parte I, Titolo V del Codice e nell'allegato B.

Come si diceva poc'anzi, l'impianto normativo della disciplina delle misure di sicurezza prevista dal Codice definisce la protezione dei dati attraverso due livelli:

a) l'art. 31 del codice contempla l'obbligo per il titolare di proteggere i dati adottando misure di sicurezza di livello "idoneo";

b) gli artt. da 33 a 36 configurano invece il livello minimo che le misure di sicurezza devono, in ogni caso, garantire.

Analizziamo qui di seguito, in maggiore dettaglio, i diversi livelli di sicurezza previsti dal nostro Codice.

3. Le misure idonee

L'art. 31 del Codice stabilisce il grado di sicurezza che un titolare del trattamento è tenuto a garantire per proteggere i dati

[3] Ai sensi dell'art. 4, lett. f) del d.lgs. n. 196 del 2003, per "titolare", si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza".

personali[4]. L'obbligo prescritto consiste nel dovere di adottare un standard di sicurezza di alto profilo e di qualità elevata: il titolare non si deve limitare ai soli provvedimenti indicati nel Disciplinare Tecnico (allegato B del Codice), che configurano un livello minimo di sicurezza, ma deve assumere provvedimenti ulteriori maggiormente restrittivi che permettono di alzare il livello di protezione.

Le misure da adottare vanno decise sulla base di un'analisi dei rischi[5], che tenga conto di diversi fattori, quali, ad esempio:

- natura dei dati trattati (comuni, sensibili, giudiziari);

- strumento utilizzato per il trattamento (cartaceo, elettronico, *personal computer* interconnesso o non interconnesso, *server* di rete o semplice terminale);

[4] L'art. 31, rubricato come "obblighi di sicurezza", così dispone: "i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

[5] L'analisi dei rischi è una sorta di fotografia dello stato della sicurezza nella gestione dei dati all'interno di una struttura aziendale o professionale e va effettuata partendo dall'elenco dei trattamenti di dati personali svolti e dagli strumenti utilizzati per il trattamento. Solo avendo un quadro chiaro dei rischi cui è sottoposto il trattamento dei dati si può, infatti, costruire la mappa delle misure di sicurezza necessarie per fronteggiarli. L'analisi dei rischi deve essere formalizzata nei casi in cui il titolare sia tenuto alla redazione del documento programmatico di sicurezza (punto 19.3 dell'Allegato B), tuttavia, anche negli altri casi è comunque opportuno procedere alla stesura dell'analisi dei rischi, alla luce della quale sarà poi possibile valutare l'idoneità dei sistemi di sicurezza già adottati e di quelli di cui si intende procedere all'adozione. In sintesi, l'analisi dei rischi si articola nelle seguenti fasi: 1) individuazione delle tipologie di dati personali trattati e degli strumenti di trattamento; 2) valutazione delle minacce che gravano sui singoli trattamenti di dati personali; 3) valutazione dell'impatto che, per l'organizzazione, ha il verificarsi di eventi negativi, nell'ambito dei singoli trattamenti; 4) identificazione del grado di rischio da coprire, e decisioni conseguenti.

- luogo ove i dati vengono custoditi (archivio fisico, elettronico e relative protezioni);

- personale che ha accesso ai dati (interno o esterno alla struttura; soprattutto con riguardo al personale interno, è assai utile la predisposizione di un mansionario).

Le misure di sicurezza possono ritenersi idonee allorquando si dimostrino efficaci per prevenire i rischi che possono provocare un danno all'interessato in dipendenza di:

- distruzione o perdita dei dati, anche per cause accidentali;

- accesso ai dati da parte di persone non autorizzate a compiere operazioni di trattamento;

- utilizzo improprio di dati per svolgere attività non consentite dalla legge;

- utilizzo improprio di dati per realizzare finalità non contemplate nell'informativa, oppure non pertinenti o comunque eccedenti rispetto alle finalità della raccolta;

- utilizzo improprio di dati al fine di effettuare operazioni che implicano un preventivo accordo dell'interessato, senza aver raccolto il relativo consenso.

Dalla lettura dell'art. 31 si può notare che lo stato di idoneità ivi richiesto fa sì che le misure da adottare non risultino definibili a priori, essendo per loro natura dinamiche, mutevoli e in costante evoluzione.

Il titolare dovrà dunque mantenere vigile l'attenzione sull'evoluzione tecnologica in materia di sicurezza e disporre adeguamenti costanti del sistema di protezione.

La mancata adozione di un livello di sicurezza idoneo espone il titolare ad una possibile condanna per risarcimento del danno in sede civile, ai sensi dell'art. 15 del Codice, che dispone in materia di

danni cagionati per effetto del trattamento[6].

I danni risarcibili possono essere sia di natura patrimoniale che non patrimoniale (come accaduto nella fattispecie, decisa dal Tribunale di Orvieto, con sentenza 22 novembre 2002, in tema di risarcimento dei danni morali sofferti da alcuni clienti di un istituto bancario)[7] e sono dovuti qualora il titolare del trattamento non dimostri, in base al principio dell'inversione dell'onere della prova ex art. 2050 c.c., di aver fatto tutto quanto tecnicamente possibile per evitare il danno cagionato[8].

[6] Il risarcimento dei danni causati ad altri per effetto del trattamento di dati personali è disciplinato dal combinato disposto delle seguenti norme: a) art. 15, comma 1 Codice: "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile"; b) art. 2050 c.c. - responsabilità per l'esercizio di attività pericolose: "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno"; c) art. 2059 c.c. - danni non patrimoniali: "il danno non patrimoniale deve essere risarcito solo nei casi determinati dalla legge"; d) art. 15, comma 2, Codice: "il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 11 (modalità del trattamento e requisiti dei dati personali)".

[7] Trib. Orvieto, sentenza n. 254 del 23 novembre 2002 (mass. 1) "costituisce illecito civile il trattamento di dati relativi alla affidabilità commerciale di persone fisiche da parte dell'istituto di credito cui esse hanno chiesto l'erogazione di un mutuo in autorizzato dei dati personali che configuri anche i reati previsti e puniti dagli artt. 35 e 36 della legge 675/96 comporta il risarcimento del danno non patrimoniale ai sensi sia del combinato disposto degli artt. 9, 18 e 29 c.c. legge 675/96 sia dell'art. 2059 c.c. (nel caso di specie è stato liquidato il danno nella misura, determinata equitativamente, di € 25.000)". Per il testo integrale della sentenza e un commento alla medesima v. G. PASCUZZI, *Lex Aquilia - Giornale didattico e selezione di giurisprudenza sull'illecito extracontrattuale*, Bologna, 2005, n. 4.

[8] In tema di sanzioni e contenzioso nell'ambito della disciplina del Codice si veda G. CAROZZI, *Sanzioni e contenzioso*, in *Dir. e pratica lav*., 2004, 1683.

4. Le misure minime

Gli artt. da 33 a 36 del Codice si occupano, invece, delle misure di sicurezza c.d. "minime". Attraverso tali disposizioni il legislatore ha fissato il principio in base al quale le misure che il titolare ha l'obbligo di adottare non devono comunque essere inferiori ad uno standard minimo pre-configurato[9].

Mentre per le misure di sicurezza c.d. "idonee" (si veda il paragrafo precedente) il legislatore ha disegnato alcune linee guida generali, le misure che compongono lo standard minimo di sicurezza sono individuate dettagliatamente nel Disciplinare tecnico (Allegato B al Codice)[10].

Una definizione generale di misure minime di sicurezza si può ricostruire tramite il testo della relazione al precedente d.p.r. 318/99, secondo cui si tratta di "requisiti minimi di sicurezza, la cui violazione costituisce la sicura esposizione a rischio del bene-privacy protetto dalle norme [...] Violazioni alla presenza delle quali, per la loro assoluta contraddizione con i requisiti minimi ormai generalmente riconosciuti, si deve ritenere che si verifichi un livello non tollerabile di rischio di lesione del diritto alla tutela dei dati personali, e quindi tali da giustificare l'adozione di un apparato sanzionatorio penale".

Le misure di sicurezza di livello minimo devono essere adottate prima di procedere a qualsiasi operazione di trattamento.

[9] Art. 33 - misure minime: "nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali".

[10] Il testo dell'allegato B è riportato integralmente in appendice a questa relazione.

Tali misure si suddividono, secondo l'architettura normativa, in due categorie: a seconda che il trattamento dei dati avvenga "con"[11], o "senza" strumenti elettronici[12].

La mancata adozione delle misure di sicurezza minime espone il titolare, oltre che all'azione di risarcimento del danno *ex* art. 15 del Codice (come nell'ipotesi di omessa adozione delle misure minime idonee), anche ad una possibile sanzione di natura penale. Tale sanzione è stabilita all'art. 169 del Codice, che prevede l'arresto sino a due anni o l'ammenda da 10 mila a 50 mila euro, lasciando però aperta la possibilità di un "ravvedimento operoso" che si verifica adempiendo alle prescrizioni impartite dal Garante, successivamente all'accertamento del reato[13].

[11] Art. 34 - trattamenti con strumenti elettronici - "il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g) tenuta di un aggiornato documento programmatico sulla sicurezza; h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".

[12] Art. 35 - trattamenti senza l'ausilio di strumenti elettronici - "il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati".

[13] Art. 169 - misure di sicurezza - "1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due

È opportuno sottolineare che la fattispecie di cui all'art. 169 del Codice non presenta, in effetti, modifiche di rilevo rispetto alla formulazione del previgente art. 36 della legge 675, come sostituito dall'art. 14 del d.lgs. n. 467 del 2001, fatto salvo l'aumento quantitativo dell'ammenda. Si tratta di un reato di omissione per cui il titolare risulta punibile per il mero fatto di non aver adottato anche una sola delle misure minime elencate nel disciplinare tecnico, indipendentemente dall'aver o meno provocato il danno[14], fatta salva la possibilità, già soprammenzionata, di regolarizzare la propria posizione adottando le misure di sicurezza del caso (c.d. ravvedimento operoso) fissando al contempo un termine, prorogabile fino a sei mesi, entro il quale porle in atto. Inoltre, nel caso di adempimento alle prescrizioni del Garante, entro i sessanta giorni successivi allo scadere del termine, il reo è autorizzato a pagare un'ammenda pari ad un quarto del massimo della

anni o con l'ammenda da diecimila euro a cinquantamila euro. 2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili".

[14] Peraltro, permangono i dubbi di legittimità costituzionale già evidenziati dalla dottrina con riguardo alla precedente normativa (che adottava il medesimo modello di tecnica legislativa) sull'utilizzo del rinvio alla fonte regolamentare operato dalla norma in esame per la determinazione degli elementi dell'illecito. Si veda, in argomento, A. MANNA, *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. e proc*., 2004, 15, nonché P. TRONCONE, *Profili penali del codice della privacy (Commento al d.lg. 30 giugno 2003, n. 196,)*, in *Riv. pen.*, 2004, 1147.

contravvenzione (quindi, euro 12.500) con l'effetto di estinguere il reato.

5. Il Disciplinare tecnico - Allegato B

Il disciplinare tecnico dà corpo alle disposizioni di principio degli artt. 33 e segg. e individua le misure minime di sicurezza che configurano lo standard di protezione dei dati personali[15].

L'allegato B ha, di fatto, abrogato integralmente il precedente "regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali" – d.p.r. 318 del 1999 emanato in attuazione dell'art. 15 della legge 675 del 1996.

È opportuno effettuare una considerazione generale sul contenuto dell'Allegato B: da un lato il Disciplinare conferma talune misure minime già previste dal d.p.r. 318 (tali misure – il cui contenuto è rimasto sostanzialmente invariato – dovevano essere già adottate in passato e dovevano quindi risultare già in essere dal 1 gennaio 2004); dall'altro introduce misure più rigorose (*password* di almeno 8 caratteri) o del tutto inedite (obbligo di *back-up* e di ripartenza entro il termine massimo di 7 gg.) che richiedono al titolare di provvedere ad una completa revisione delle misure di sicurezza adottate sulla base delle disposizioni previgenti.

Come ho già accennato all'inizio di questa relazione, i termini inizialmente previsti dall'art. 180 per le nuove misure minime di sicurezza sono stati oggetto, nel tempo, di 3 successive proroghe: inizialmente, da parte dell'art. 3, del d.l. 24 giugno 2004, n. 158; successivamente, da parte dell'art. 6 del d.l. 9 novembre 2004, n. 266 e, più recentemente, da parte dell'art. 6-*bis* della legge 1° marzo 2005, n. 26, che ha convertito, con modificazioni, il

[15] Il testo dell'allegato B è riportato integralmente in appendice a questa relazione.

d.l. 314 2004. La nuova scadenza entro la quale tutti i soggetti si dovranno adeguare alle disposizioni del disciplinare tecnico è quella del 31 dicembre 2005 (in origine era il 30 giugno 2004!).

È prevista un'ulteriore proroga del termine nel caso in cui si possiedano strumenti elettronici inadeguati; i commi 2 e 3 del novellato art. 180 differiscono ulteriormente al 31 marzo 2006 (in origine era il 31 dicembre 2004) il termine ultimo entro cui le nuove misure minime dovranno essere operative[16].

6. Il Documento Programmatico sulla Sicurezza (DPS)

Una delle misure minime contemplate dal Disciplinare tecnico, forse quella che meglio si presta a riassumere anche tutte le altre (in quanto le "contiene" e le formalizza), consiste nella redazione del c.d. Documento Programmatico sulla Sicurezza (DPS) previsto dal punto 19, all. B.

Non si tratta di una misura inedita, in quanto essa era già contemplata anche nel precedente d.p.r. 318/1999, ove tuttavia il contenuto era diverso sia dal punto di vista soggettivo che oggettivo. Infatti, risulta ampliato il novero dei titolari obbligati alla redazione di detto documento: in base alla disposizione di cui al punto 19 del Disciplinare tecnico, la redazione del DPS risulta obbligatoria – e consente di evitare la sanzione penale di cui all'art. 196 del Codice – nel caso in cui si effettuino trattamenti di dati sensibili e/o giudiziari mediante l'utilizzo di strumenti elettronici, a prescindere dal fatto

[16] Nelle more della pubblicazione degli atti di questo convegno, è intervenuta una ulteriore proroga, disposta dall'art. 10 della legge 23 febbraio 2006, n. 51 che ha convertito con modificazioni l'ennesimo decreto, il d.l. 30 dicembre 2005, n. 273 (in G.U. del 28-02-06). Il termine ultimo per l'adozione delle misure di sicurezza di cui agli articoli da 33 a 35 e all'allegato B è slittato al 31 marzo 2006 (le disposizioni relative sono dunque entrate definitivamente in vigore), mentre per il caso di strumenti elettronici "inadeguati" il nuovo termine previsto è quello del 30 giugno 2006.

che si tratti o meno di elaboratori collegati ad una rete accessibile al pubblico[17].

Il problema interpretativo scaturito dal mancato coordinamento dell'art. 34 del Codice, che alla lettera g) prevede la "tenuta di un aggiornato documento programmatico sulla sicurezza" per tutti i trattamenti di dati effettuati con strumenti elettronici, indipendentemente dalla loro natura (comuni, sensibili e giudiziari), e il punto 19 del Disciplinare tecnico, che prevede tale adempimento per i soli Titolari di trattamenti di dati sensibili e giudiziari effettuati con strumenti elettronici, è stato chiarito dal Garante in quest'ultimo senso[18].

Tuttavia, anche per quanto concerne le realtà aziendali medio-piccole sarebbe opportuno effettuare una riflessione sulle modalità di trattamento dei dati (anche solo comuni-aziendali, ma spesso "strategici" per l'azienda stessa e per i suoi clienti) e sulle misure di sicurezza adottate; e quale occasione migliore della predisposizione ragionata di tale documento, e del suo aggiornamento con cadenza annuale, per la formalizzazione di adeguate procedure aziendali, al fine di prevenire danni e di rendere efficiente la struttura aziendale anche sotto il profilo della *data security*? L'opportunità della riflessione emerge anche alla luce del fatto che tale documento non ha (o non dovrebbe avere) solo una "funzione esterna", in caso di ispezioni, di documentazione dell'adempimento alle prescrizioni legislative in tema di sicurezza nel trattamento dei dati, ma anche (e soprattutto) ha (o dovrebbe

[17] Nella vigenza del d.p.r. 318/1999 venivano espressamente esentati i titolari che utilizzavano elaboratori collegati tra loro attraverso una rete proprietaria (*Local Area Network* interna) o che utilizzavano elaboratori isolati (*stand alone*).

[18] Si vedano il comunicato stampa del 23 marzo 2004 (disponibile all'URL http://www.garanteprivacy.it/garante/doc.jsp?ID=772126) e il parere reso a Confindustria in data 22 marzo 2004 (disponibile all'URL http://www.garante privacy.it/garante/doc.jsp?ID=771307).

avere) una funzione interna di guida all'adozione e al potenziamento delle misure di sicurezza; la tutela della sicurezza nel trattamento dei dati non deve essere considerata un valore antagonista alle esigenze di mercato, bensì un valore aggiunto per la propria organizzazione.

Tornando all'evidenza normativa, all'interno del DPS devono essere regolati anche altri aspetti che non risultavano contemplati dalla legislazione previgente, quali, in sintesi:

Elenco dei trattamenti di dati personali (punto 19.1): la categoria dei dati giudiziari è più estesa rispetto al passato: in base alla definizione di cui all'art. 4 del Codice, risultano compresi anche i provvedimenti giudiziari non definitivi e le informazioni relative alla semplice qualità di indagato o imputato.

Descrizione dei criteri e delle modalità di ripristino dei dati inseguito a distruzione o danneggiamento dei supporti elettronici (19.5).

Previsione di interventi formativi (punto 19.6) per i quali viene richiesta una descrizione molto più dettagliata e puntuale rispetto al passato.

Descrizione dei criteri da adottare per garantire la sicurezza minima in caso di *outsourcing* (punto 19.7).

Obbligo per gli esercenti le professioni sanitarie, di cifrare e separare i dati identificativi dell'interessato da quelli riguardanti lo stato di salute o la vita sessuale (punto 19.8).

Si segnala inoltre che, per espressa previsione (punto 26 del Disciplinare tecnico) il titolare, deve riferire nella relazione accompagnatoria del bilancio di esercizio (ove tenuto) dell'avvenuta redazione e dei successivi aggiornamenti del DPS. Si tratta di una misura inedita, non contemplata nel d.p.r. 318/1999, che dovrebbe servire sostanzialmente a porre all'attenzione del vertice dell'organizzazione del titolare del trattamento le problematiche relative alla sicurezza dei dati e, di conseguenza, a responsabilizzare

i vertici aziendali in merito all'adozione delle misure previste per legge e all'adeguamento della struttura a tali disposizioni, nonché a è, in estrema sintesi, ciò che la legislazione italiana in materia di protezione dei dati personali prevede in tema di misure di sicurezza.

7. Conclusioni

Solitamente, nella prassi, si tende a porre l'accento sulle misure di sicurezza logiche (identificazione e autenticazione degli incaricati, *antivirus*, *back-up*, ecc.) e, in secondo luogo, su quelle fisiche (vigilanza negli accessi alla sede, allarmi, dispositivi anti-incendio e quant'altro), dimenticando l'aspetto forse più importante: mi riferisco alle misure di sicurezza c.d. organizzative, quelle orientate a fare in modo che l'intera struttura adotti comportamenti conformi ai principi generali della sicurezza.

Spessissimo il profilo organizzativo viene valutato dalle aziende soltanto a livello puramente formale e, nella corsa agli adempimenti che si sta verificando ormai ciclicamente allo scadere di ogni proroga, tale aspetto si traduce in mere enunciazioni di principio da inserire nel DPS, ma destinate a non ricevere attuazione pratica (l'esempio più lampante è quello relativo alla formazione degli incaricati).

Eppure, i problemi più evidenti negli incidenti caratterizzati da violazioni della sicurezza dei dati, sono spesso riconducibili ad una carenza organizzativa, come nel caso giudicato dal Tribunale di Orvieto, cui abbiamo precedentemente accennato: una pratica personale di un cliente era stata lasciata incustodita in un luogo visibile e alla portata di tutti e questa "esposizione" aveva cagionato al cliente un grave danno.

Un corretto processo della sicurezza richiede, prima ancora dell'adozione delle concrete misure previste dalla legge, la definizione di una serie di procedure, teleologicamente orientate a

regolamentare gli aspetti organizzativi del processo medesimo. Oltre alla formale definizione di ruoli e responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, appare necessario procedere alla concreta responsabilizzazione di tutti gli incaricati al trattamento e dei loro responsabili, indipendentemente dal fatto che il trattamento avvenga o meno mediante l'utilizzo di strumenti elettronici, sia dal punto di vista della prevenzione degli eventi negativi (accidentali o intenzionali), sia dal punto di vista della limitazione degli effetti causati dall'eventuale verificarsi di eventi negativi.

Appendice alla relazione

Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali – Allegato B. Disciplinare tecnico in materia di misure di sicurezza (Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di

autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si

applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di

dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli

incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono

controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

CONTRIBUTI

PUBBLICA AMMINISTRAZIONE, COMUNICAZIONI ELETTRONICHE E TUTELA DELLA PRIVACY

Nicola Lugaresi

SOMMARIO: *1. Tutela "delle" comunicazioni elettroniche e tutela "dalle" comunicazioni elettroniche. - 2. Le ragioni di un intervento della pubblica amministrazione a tutela di se stessa e del dipendente. - 3. Titolarità, uso e tutela degli indirizzi di posta elettronica. - 4. Aspetti proprietari, segreto epistolare e legittimazione alla tutela. - 5. Filtri* anti-spam *e configurazione degli indirizzi dei dipendenti pubblici.*

1. Tutela "delle" comunicazioni elettroniche e tutela "dalle" comunicazioni elettroniche

Le comunicazioni elettroniche non sollecitate[1], o indesiderate[2], fenomeno comunemente conosciuto come *spam*[3], sono indirizzate a tutti gli utenti di Internet, sia che si tratti di persone fisiche sia che si tratti di persone giuridiche. In particolare, tra le persone giuridiche, sono colpite con particolare frequenza e intensità le pubbliche amministrazioni (e, nel loro ambito, i pubblici dipendenti). Il processo di digitalizzazione cui la pubblica amministrazione è soggetta, l'uso assiduo della posta elettronica da parte della stessa, sia nei rapporti interni che nei rapporti con i cittadini, la diffusione dei siti Web pubblici con la indicazione degli indirizzi *email* dei dipendenti, costituiscono le principali ragioni della vulnerabilità rispetto alle comunicazioni indesiderate.

I problemi che qui si affrontano riguardano la tutela dallo

---

[1] Secondo la rubrica dell'art. 13 della Direttiva 2002/58/CE, nel testo in inglese ("*unsolicited*").

[2] Secondo la rubrica dell'art. 13 della Direttiva 2002/58/CE, nel testo in italiano, e dell'art. 130 del d.lgs. n. 196/2003.

[3] *Spam* è la marca di una carne in scatola venduta negli Stati Uniti; l'associazione del termine con la posta elettronica non sollecitata deriva da una scenetta dei Monty Python.

spam[4], quando si tratti di indirizzi di "proprietà" di una pubblica amministrazione affidati ai dipendenti. In particolare, ci si chiede a chi spetti tale tutela e quali siano gli obiettivi della stessa. In merito al primo profilo, relativo alla legittimazione, si può sostenere che tale tutela sia di competenza dell'amministrazione, in quanto "proprietaria" dell'indirizzo; o del dipendente, cui tale indirizzo è assegnato, in quanto soggetto che riceve, e "tratta" la corrispondenza; o, ancora, di entrambi, in ragione dei rispettivi interessi. In merito al secondo profilo, relativo agli obiettivi, non si tratta solo della protezione della riservatezza dell'individuo, che non deve ricevere posta elettronica indesiderata, ma anche della salvaguardia della funzionalità dell'azione dell'amministrazione, rallentata e ostacolata dalla ricezione di migliaia di messaggi non sollecitati.

Il riferimento normativo principale, nel nostro ordinamento, è costituito dall'art. 130[5] ("Comunicazioni indesiderate") del Codice in materia di protezione dei dati personali (d'ora in poi: Codice), approvato con d.lgs. 30 giugno 2003, n. 196[6]. Tale articolo (con

[4] Per un inquadramento generale delle problematiche relative allo *spamming*, v. N. LUGARESI, *European Union vs. Spam: A Legal Response* in *Spam 2005: Technology, Law and Policy* (Center for Democracy and Technology, Washington D.C., USA, 2005), 45 (disponibile anche all'URL http://www.cdt.org/speech/spam/spam2005/spam2005.pdf), ove si possono trovare altri contributi che affrontano diversi profili; v. anche gli atti della *First Conference on Email and Anti-Spam* (Mountain View, CA, 30-31 luglio 2004) disponibile all'URL http://www.ceas.cc/papers-2004/145.pdf e della *Second Conference on Email and Anti-Spam* (Stanford University, CA, 21-22 luglio 2005) disponibile all'URL http://www.ceas.cc/2005/index.html

[5] L'art. 130 del Codice recepisce l'art. 13 della Direttiva 2002/58/CE, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[6] Sull'art. 130 del Codice, e sulle problematiche relative allo spamming nell'ordinamento italiano, v. A. LEVI, F. ZANICHELLI, *L'utilizzo delle e-mail a fini pubblicitari: dallo "spamming" al "permission marketing"*, in *Riv. Dir. Ind.*, 2001,

riferimento particolare ai primi due commi) consente di inviare comunicazioni elettroniche "per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale" esclusivamente con il consenso preventivo dell'interessato, in applicazione del sistema comunitario di "opt-in"[7], che si distingue dal sistema di "opt-out", proprio ad esempio degli Stati Uniti[8], nel quale è invece possibile mandare posta non sollecitata fino a quando il destinatario non si oppone.

L'impostazione del Codice pone al centro della disciplina, e della tutela, l'individuo, e i suoi dati personali. La nozione di "dato personale", naturalmente alla base dell'intera costruzione del Codice, non riguarda peraltro solo gli individui, essendo riferita a "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione" (art. 4, comma 1, lett. b, Codice), il che lascia la strada aperta per una protezione disgiunta, eventualmente cumulativa. In questo senso, il dato personale costituito dall'indirizzo di posta

198; S. GORINI, S. NIGER, *Privacy e comunicazioni elettroniche*, in J. MONDUCCI, G. SARTOR (a cura di), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 411; A. PRADELLA, *Comunicazioni indesiderate*, in G.P. CIRILLO (a cura di), *Il codice sulla protezione dei dati personali*, Milano 2004, 460; RI. IMPERIALI, RO. IMPERIALI, *Codice della privacy*, Milano, 2004, 577; D. D'AGOSTINI, *A che punto è la lotta allo spam?*, in *Ciberspazio e dir.*, 2004, 215; P. CRUGNOLA, *Disciplina dello spamming*, in *NGCC*, 2004, II, 474; A. STAZI, *La disciplina delle comunicazioni elettroniche non richieste alla luce del d.lgs. n. 70/2003 sul commercio elettronico e del nuovo "codice in materia di protezione dei dati personali"*, in *Dir. Inf.*, 2003, 1101.

[7] Sulla posizione della Comunità europea in materia di *spam*, v. la Comunicazione della Commissione del 22 gennaio 2004, sulle comunicazioni commerciali non sollecitate o "spam"; si vedano anche, del DATA PROTECTION WORKING PARTY, *Working Document, Privacy on the Internet – An Integrated EU Approach to On-line Data Protection* (21 novembre 2000); *Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing* (13 giugno 2003); *Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC* (27 febbraio 2004).

[8] Si fa riferimento al *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, più comunemente conosciuto come *CAN-SPAM Act of 2003*.

elettronica del tipo «nome.cognome@amministrazione.it» è infatti, secondo un'interpretazione letterale, relativa sia al dipendente, persona fisica, del cui nome si tratta, che del datore di lavoro pubblico, amministrazione, del cui dominio si tratta. Ne consegue, considerato che ai sensi del Codice "interessato" è da intendere "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali" (art. 4, comma 1, lett. i, Codice), che tanto dipendente che amministrazione dovrebbero essere considerati quali "interessati".

Il rapporto tra comunicazioni elettroniche[9] (e, nello specifico, posta elettronica)[10] e riservatezza non attiene quindi soltanto al profilo tradizionale relativo alla confidenzialità delle comunicazioni tra due o più soggetti determinati (ed in questo caso interessi del dipendente e dell'amministrazione potrebbero divergere), ma anche al profilo del rispetto della sfera privata dell'individuo (o anche della sfera pubblica dell'amministrazione), che vuole essere lasciato in pace. Si tratta, quindi, dell'essenza stessa della privacy, nella sua accezione più completa[11].

All'avvento delle comunicazioni elettroniche, in riferimento alle problematiche relative al primo profilo (confidenzialità della corrispondenza: tutela "delle" comunicazioni elettroniche), il diritto aveva già in sé le possibili risposte. Giudici e legislatore hanno, anche se non sempre coerentemente, utilizzato lo strumento

[9] Ai sensi dell'art. 4, comma 2, lett. a), del Codice: "ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico".

[10] Ai sensi dell'art. 4, comma 2, lett. a), del Codice: "messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza".

[11] S. WARREN, L.D. BRANDEIS, *The Right to Privacy*, 4 *Harv. L. Rev*. 193 (1890); v. anche la *dissenting opinion* di Brandeis, divenuto giudice della Corte Suprema, nel caso *Olmstead v. United States*, 277 U.S. 438, 478 (1928).

dell'analogia per applicare al tema della riservatezza delle comunicazioni elettroniche una copertura normativa tradizionale e consolidata, anche di livello costituzionale[12], che è stata progressivamente specificata con l'ampliamento espresso del concetto giuridico di corrispondenza[13]. In riferimento al secondo profilo (diritto ad essere lasciati in pace: tutela "dalle" comunicazioni elettroniche), divenuto oggetto di considerazione e di tutela in tempi più recenti, l'applicazione dell'analogia è stata più faticosa, e le norme dedicate hanno seguito un percorso più incerto. In entrambi i casi, i processi interpretativi e normativi non hanno risolto completamente i problemi applicativi, principalmente per le diversità intrinseche, ontologiche, della comunicazione elettronica rispetto a quella tradizionale cartacea.

2. Le ragioni di un intervento della pubblica amministrazione a tutela di se stessa e del dipendente

L'analisi che segue si occupa prevalentemente del profilo di tutela generalmente meno considerato, vale a dire della tutela dell'individuo nei confronti della ricezione di posta (elettronica) non desiderata (tutela "dalle" comunicazioni elettroniche), senza per questo tralasciare il profilo relativo alla confidenzialità delle comunicazioni (elettroniche), specialmente quando questo possa essere funzionale alla ricerca di soluzioni interpretative più corrette e soddisfacenti.

Che anche la pubblica amministrazione possa intervenire nella lotta allo *spamming*, così come gli altri utenti della Rete, non è in discussione. Ma rispetto ai privati cittadini, ed anche alle persone giuridiche private, l'amministrazione ha una posizione differenziata,

[12] Si fa riferimento all'art. 15 Cost., il cui comma primo afferma che "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili".

[13] S. NESPOR, A.L. DE CESARIS, *Internet e la legge*, Milano, 2001, 100.

che pare connotare non solo un diritto, e una facoltà, ma un dovere. Si pensi alle ragioni che portano a combattere il fenomeno dell'invio di comunicazioni elettroniche indesiderate. Alcune di esse riflettono esigenze di carattere individuale, mentre altre fanno riferimento ad interessi più ampi, che si potrebbero connotare quali interessi diffusi (dei cittadini-utenti di Internet), o anche come interessi pubblici (della collettività, nel suo complesso, anche in relazione al "buon andamento" dell'azione amministrativa).

Tra le motivazioni di carattere individuale possiamo pensare in particolare alla tutela di diritti fondamentali, quale il diritto alla riservatezza, nella sua accezione più ampia. Il diritto alla riservatezza ha infatti un contenuto composito, che non si esaurisce nella semplice protezione dei propri dati personali, come una prima lettura del Codice sembrerebbe implicare. La protezione della riservatezza, come diritto fondamentale[14], comporta sì la protezione delle informazioni relative ad una persona (anche giuridica) determinata o determinabile, ma comporta anche, quando non vi siano ragioni di interesse pubblico superiore, la protezione dell'intimità delle comunicazioni, la protezione dell'anonimato, la protezione della sfera privata dell'individuo che vuole essere lasciato in pace, la protezione della possibilità di autonoma formazione della propria personalità[15]. E, con un poco di coraggio, si può sostenere che la protezione della riservatezza comporta anche la protezione non solo della dignità dell'individuo, ma anche del "tempo" delle persone (fisiche, ma anche giuridiche), tempo "personale" che l'invio indiscriminato e sempre più insistente di comunicazioni commerciali viene ad erodere illegittimamente. La pubblica amministrazione,

[14] V. la nuova (e contrastata) Costituzione europea, che tutela sì i dati di carattere personale, all'art. II-68, ma prima ancora, all'art. II-67, la "vita privata e familiare", il domicilio e le comunicazioni.

[15] V. N. LUGARESI, *Internet, privacy e pubblici poteri negli Stati Uniti*, Milano, 2000, 73.

deputata a perseguire l'interesse pubblico in tutte le sue attività, non può chiudere gli occhi di fronte ad un fenomeno che colpisce non solo la stessa amministrazione, ma anche i dipendenti pubblici ed i cittadini.

Nello stesso senso, si consideri che lo *spamming* è strettamente connesso alla diffusione di virus, che possono infestare ogni computer; alla proliferazione di frodi informatiche (ad esempio attraverso il meccanismo, sempre più diffuso, denominato *phishing*)[16], che possono ingannare ogni cittadino; alla circolazione incontrollata di testi e immagini pornografiche (o anche pedopornografiche), che possono avere i minori come destinatari. La pubblica amministrazione non può pertanto disinteressarsi del fenomeno, inteso nel suo complesso, ma deve intervenire per rafforzare la tutela nei confronti dei soggetti deboli presenti in Rete: i bambini, spesso tecnologicamente capaci anche più degli adulti, ma non preparati a rispondere adeguatamente sotto il profilo emotivo e psicologico ad impulsi di carattere sessuale provenienti senza filtro dall'esterno; le persone più ingenue, tenendo conto che la soglia di ingenuità per cadere in alcune delle trappole predisposte in Internet non deve essere necessariamente alta; le persone meno abbienti, che possono avere a disposizione *software* di protezione del proprio computer meno efficace.

Discorsi analoghi si possono ripetere per interessi più ampi, propri della comunità che opera in Internet, e diretti a proteggere "ambiente" e "architettura" della Rete. La diffusione di posta elettronica non sollecitata comporta il rallentamento della Rete, se non in termini globali, almeno in termini di singole porzioni (*servers*, singole connessioni, ad esempio), con possibili sovraccarichi e disagi

[16] Per *phishing* si intende una falsa rappresentazione di indirizzi di posta elettronica o di siti Web finalizzata ad ottenere abusivamente informazioni, quali i dati bancari o il numero di carta di credito, di un soggetto.

nella fruizione. Nel momento in cui il *server* è bloccato, nel momento in cui la connessione è rallentata, la percezione soggettiva dell'utente è che Internet non funzioni. Ne deriva, oltre ad un sentimento di fastidio, una perdita di fiducia nelle possibilità che Internet può dare all'individuo, e pertanto un freno alla presenza in Rete, in senso contrario alle spinte decise verso una progressiva digitalizzazione non solo dell'amministrazione, ma anche dei cittadini, verso quell'obiettivo comunemente sintetizzato, nella normativa e nei documenti ufficiali più recenti, con la locuzione "società dell'informazione". Ne risulta compromessa la possibilità di conseguire l'obiettivo di superare il "divario digitale", con particolare riferimento a quei soggetti che per formazione culturale, età, o altri fattori economici e sociali sono naturalmente più restii ad operare in Internet.

L'inondazione di *spam* comporta inoltre una minore affidabilità delle comunicazioni elettroniche, rendendo più facile la perdita di messaggi "regolari", causata dal particolare funzionamento di filtri *anti-spam* imprecisi e aggressivi adottati, che individuano "falsi positivi" (comunicazioni legittime, ma non considerate tali dal *software*), eliminandoli o comunque inserendoli in caselle dedicate allo *spam*, o, più semplicemente, per la difficoltà di individuare i messaggi desiderati in caselle di posta riempite per la maggior parte da posta non sollecitata. Anche in questo caso, la pubblica amministrazione ha un interesse più forte, di fatto, se non anche giuridicamente, di quello che può avere il singolo individuo, in quanto il suo obiettivo non è limitato a proteggere se stessa, ma è esteso alla protezione dei cittadini e del sistema complessivo delle comunicazioni elettroniche. Nello stesso senso si potrebbe argomentare con riferimento non solo ai cittadini in generale ed ai loro diritti, ma anche più in specifico alle imprese ed ai loro legittimi interessi economici, per quanto concerne la minore attrattiva del

commercio elettronico, riuscendo sempre più difficile distinguere gli operatori seri ed affidabili da chi sfrutta le debolezze del sistema per raggirare consumatori ed utenti.

Il fenomeno dello *spamming*, ed è qui principalmente la ragione del suo successo, comporta del resto un rovesciamento dei costi di *marketing*, che diventano estremamente ridotti per chi spedisce, addossandosi e spalmandosi su chi riceve[17], in termini economici (costi di connessione; adozione di software *anti-spam*; perdita di tempo lavorativo) e sociali (perdita di tempo, anche non lavorativo, per la selezione dei messaggi legittimi; sensazione di fastidio). Per la pubblica amministrazione, rischi, danni e valori sono moltiplicati per fattori altissimi, unendosi la qualità di datore di lavoro con quella di soggetto che deve curare gli interessi della comunità.

La pubblica amministrazione, come le imprese, è del resto tenuta a salvaguardare i propri sistemi informatici dallo *spamming* e dai fenomeni nocivi collegati, dovendo ad esempio esplicitare rischi e misure di protezione nell'ambito del Documento Programmatico della Sicurezza[18]. È tenuta a salvaguardare la propria produttività, cercando di limitare il più possibile il tempo che i dipendenti pubblici sono forzati a dedicare alla "scrematura" dei messaggi in arrivo. È tenuta a salvaguardare la propria credibilità, evitando che messaggi qualificabili come *spam* possano provenire da indirizzi della stessa pubblica amministrazione, per una inadeguata protezione rispetto a programmi che diffondono messaggi non sollecitati

[17] Uno studio commissionato dalla Commissione europea (S. GAUTHRONET, E. DROUARD, *Unsolicited Commercial Communications and Data Protection*, 2001, le cui sintesi possono trovarsi in http://www.privacy.it/aretespamm2001.html, visitato da ultimo il 20 dicembre 2005) stimava, nel 2001, in 10 milioni di Euro il costo complessivo per i destinatari di *spam*.

[18] V. art. 34, comma 1, lett. g), del Codice, nonché il punto 19 dell'allegato B allo stesso.

attraverso indirizzi di altri soggetti. È tenuta a salvaguardare il dipendente, non solo per quanto riguarda, funzionalmente alla prestazione lavorativa, il tempo dello stesso, ma anche per quanto riguarda la riservatezza dello stesso, nel momento in cui gli viene fornito uno strumento di lavoro quale la posta elettronica.

In questo senso, la percezione di maggiore impunità per i messaggi non sollecitati spediti ad indirizzi appartenenti alla pubblica amministrazione dovrebbe essere un'anomalia, da superare, e non una sensazione, da accettare. La pubblica amministrazione dovrebbe intervenire più duramente. Non si tratta infatti di una scelta privata, libera, da non motivare, come può essere quella di un privato. Si tratta invece di una scelta discrezionale, che deve tenere conto sia degli interessi, anche economici (con quello che ne consegue), della pubblica amministrazione intesa come organizzazione, che degli interessi e dei diritti della collettività, delle imprese e dei cittadini. Una scelta che deve tenere conto delle conseguenze, in termini pratici immediati (lotta allo *spamming* più efficace), pratici indiretti (percezione diffusa del disvalore sociale della condotta di chi invia posta non sollecitata) e anche teorici (affermazione netta del rapporto con la riservatezza dell'individuo, e conseguente necessità di tutela).

3. Titolarità, uso e tutela degli indirizzi di posta elettronica

Il problema diventa allora, prima ancora di individuare i meccanismi, normativi, economici, tecnologici, più efficaci di lotta allo *spamming*, quello di superare possibili perplessità interpretative in merito alla "titolarità" delle iniziative che possono (e devono) essere intraprese. Ci si riferisce in particolare, per quanto concerne le caratteristiche della posta elettronica, alla connotazione dell'indirizzo di posta elettronica fornito ai dipendenti delle pubbliche amministrazioni ed alla sua qualificazione giuridica.

La diffusione dell'uso della posta elettronica all'interno della pubblica amministrazione e nei rapporti con i cittadini è un obiettivo fondamentale del processo di digitalizzazione dell'amministrazione e dello sviluppo della società dell'informazione, come confermato recentemente dal d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), il cui art. 3 riconosce a cittadini ed imprese un "diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali"[19]. Ma non è chiaro quale sia la rispettiva posizione di dipendente e pubblica amministrazione nella gestione dell'indirizzo di posta elettronica.

Nelle prime applicazioni giurisprudenziali, relative al settore privato, l'attenzione si è rivolta in particolare ai profili relativi alla riservatezza delle comunicazioni del lavoratore che utilizza l'indirizzo "aziendale". In particolare, in una pronuncia approfondita, ma non convincente in alcune sue parti, il Tribunale di Milano ha affermato la natura di "semplice strumento aziendale" della posta elettronica[20], consentendo il controllo del contenuto della stessa da parte del datore di lavoro (ed escludendo di conseguenza la configurabilità del reato di cui all'art. 616 c.p., rubricato "Violazione, sottrazione e soppressione di corrispondenza", in capo al datore di lavoro che aveva letto la posta elettronica del dipendente durante le ferie di quest'ultimo), indipendentemente dal fatto che il lavoratore fosse stato avvertito di tale possibilità.

Anche se si comprende la *ratio* della pronuncia, che mira ad evitare un uso distorto della posta elettronica aziendale (nella fattispecie, si era accertato un uso non solo privato, ma anche

[19] V. anche, con riferimento più specifico alla posta elettronica Dir. PCM 27 novembre 2003; Dir. PCM 4 gennaio 2005.

[20] Trib. Milano, ordinanza 10 maggio 2002, in *Foro it.*, 2002, II, 385.

concorrenziale rispetto all'attività del datore di lavoro), vi sono alcuni profili che meritano una riflessione più attenta.

Un primo aspetto riguarda la distinzione, individuata dal Tribunale di Milano tra "personalità" dell'indirizzo di posta elettronica e "privatezza" del medesimo. In effetti, sembrano due aspetti di difficile scissione. Se l'indirizzo, costituito nella fattispecie da «nome.cognome@impresa.com», è personale, e contiene, dati personali, o rappresenta comunque un dato personale, come del resto ha riconosciuto espressamente anche il Garante[21], la riservatezza della posta ricevuta a quell'indirizzo dovrebbe essere tutelata, qualora non vi sia un consenso espresso del soggetto cui quella casella è affidata. L'applicazione da parte del Tribunale di Milano di un ragionamento del genere "non poteva non sapere", la cui intrinseca pericolosità è accentuata dal riferirsi a fenomeni tecnologici di cui non tutti possono comprendere il funzionamento e ad elementi giuridici, normativi e giurisprudenziali, non consolidati, non convince. Specialmente se si considera che al datore di lavoro non è richiesto uno sforzo particolare per esplicitare la politica della privacy aziendale, e avvertire il lavoratore che l'indirizzo è sì personale, ma senza esclusività di accesso, e con facoltà di controllo esterno. L'assenza di una tale precisazione può ragionevolmente far pensare al dipendente che un controllo di questo genere non vi sia, o anche che non ve ne sia la possibilità giuridica, in quanto vietato. In questo senso, è preferibile, e più corretto, perseguire finalità di prevenzione che non di repressione successiva[22], attraverso una precisa informazione da fornire al dipendente in merito alla politica della privacy aziendale (o della pubblica amministrazione), con particolare riferimento all'uso degli strumenti elettronici aziendali (o

[21] Garante per la protezione dei dati personali, decisione 25 giugno 2002.

[22] V. DATA PROTECTION WORKING PARTY, *Working document on the surveillance of electronic communications in the workplace*, 29 maggio 2002.

della pubblica amministrazione). E non si entra nella problematica relativa al controllo a distanza dei lavoratori.

Un secondo aspetto riguarda la critica contenuta nell'ordinanza del Tribunale di Milano alla apodittica "assimilazione della posta elettronica alla posta tradizionale", che non abbia considerato "le strutturali diversità dei due strumenti comunicativi". In effetti, la "apodittica assimilazione" non deriva da un'interpretazione ardita, ma, oltre che dall'art. 15 della Costituzione, dalla lettera dell'art. 616 c.p., che al comma 4 equipara espressamente la corrispondenza epistolare con la corrispondenza "informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza". In questo senso, deve essere letta la norma di cui al comma 1 dell'art. 616 c.p., per il quale è punito chiunque "prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta". Non pare di poter dire che la posta elettronica sia una corrispondenza "aperta", anche in assenza di un procedimento di crittografia che ne abbia reso illeggibile il contenuto. Non si tratta di una comunicazione ad un *newsgroup* o ad un forum di discussione, ma di una corrispondenza con un destinatario determinato. La corrispondenza in entrata è diretta al dipendente, non al datore di lavoro. E se si volesse sostenere una destinazione congiunta di parte della posta, vi sarebbe comunque il problema dell'accertamento di tale circostanza, che presupporrebbe la lettura di tutta la posta. La corrispondenza in uscita è diretta ad un soggetto terzo rispetto a dipendente e datore di lavoro, e pertanto la confidenzialità della stessa deve essere tutelata con anche maggiore attenzione, coinvolgendo soggetti che "possono non sapere" e che sono estranei all'organizzazione del datore di lavoro.

In questo senso, la posta elettronica dovrebbe ricevere la stessa tutela della corrispondenza "epistolare", cartacea, indirizzata al lavoratore. Se non sono consentiti, in riferimento alla posta

tradizionale, l'apertura della posta in entrata o il controllo della posta in uscita del dipendente, non si vede perché, di fronte al dato costituzionale e normativo esistente, possa essere "aperta" e letta la posta del dipendente, all'insaputa dello stesso, in assenza di un mandato[23].

4. Aspetti proprietari, segreto epistolare e legittimazione alla tutela

Senza entrare in aspetti ancora più specifici della pronuncia del Tribunale di Milano, si può peraltro rilevare che, sulla base della normativa esistente, il soggetto del cui indirizzo si tratta (indirizzo che normalmente riporta almeno il cognome dello stesso) non dovrebbe essere spogliato della capacità di "gestire" il medesimo indirizzo. Si può discutere sulle modalità (e sui presupposti, primo tra tutti quello "informativo") attraverso cui il datore di lavoro può aprire la posta elettronica e leggere i messaggi in entrata e in uscita, ma questo può, tutt'al più, comportare una "cogestione" della casella di posta elettronica, conformemente a quanto si diceva in merito alla posizione condivisa di "interessato". Aspetto questo che si riprenderà in seguito, a proposito della titolarità delle iniziative di reazione alla ricezione di posta elettronica non sollecitata.

Il problema principale è quello di conciliare aspetti proprietari, relativi allo "strumento aziendale" e aspetti relativi alla protezione della riservatezza delle comunicazioni, relativi al contenuto della corrispondenza elettronica[24]. A volte, come dimostrano esempi proprio in materia di *spamming*, la tutela degli aspetti proprietari può combinarsi con la tutela dei diritti

[23] Per il secondo comma dell'art. 15 Cost., la limitazione di libertà e segretezza della corrispondenza "può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge".

[24] S. NESPOR, A.L. DE CESARIS, *Internet*, cit., 105.

individuali[25].

Anni fa, in uno dei primi casi di "cyberlaw", Compuserve, fornitore di servizi Internet statunitense, citò in giudizio, dopo preventiva diffida, Cyberpromotions, azienda che si occupava di *direct marketing*, per l'invio di ondate di posta non sollecitata ai suoi sottoscrittori, circostanza che aveva determinato le proteste degli stessi e la perdita di vari abbonamenti. Compuserve sosteneva, e il giudice le diede ragione, che vi fosse un'ipotesi di "trespass to chattels" nei confronti di apparecchiature e infrastrutture[26], difendendo indirettamente la privacy degli utenti (negli Stati Uniti, una legge federale *anti-spam*, il CAN-SPAM Act, fu approvata solo nel 2003 facendo seguito ad una serie di iniziative legislative a livello statale)[27]. In tempi più recenti, AmericaOnLine e Microsoft hanno citato un commerciante di articoli sportivi francese per l'invio di posta elettronica non sollecitata, sostenendo violazioni proprietarie e danni di immagine, ed ottenendo risarcimenti e spese legali[28].

Non ci si deve necessariamente scandalizzare se la protezione di un diritto fondamentale (e particolarmente intimo) quale la riservatezza dell'individuo passa attraverso strumenti di tutela della proprietà e di interessi economici di altri soggetti. Se questo aumenta il livello di protezione, è anzi auspicabile. Nel momento in cui questo approccio comporta l'indebolimento del profilo relativo alla riservatezza delle comunicazioni, e della privacy dell'individuo, nascono invece i problemi. Ed è quanto può accadere

---

[25] J. KELMAN, *E-Nuisance: Unsolicited Bulk E-Mail at the Boundaries of Common law Property Rights*, 78 *S. Cal. L. Rev.* 363 (2004).

[26] Il caso, *Compuserve, Inc. v. CyberPromotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997), viene citato come la prima applicazione del *trespass to chattels* alla posta elettronica non sollecitata.

[27] V. A. BEPKO, *A State-by-State Comparison of Spam Laws*, 13 *Media L. & Pol'y* 20 (2004).

[28] Tribunal de Commerce de Paris, 5 maggio 2004 disponibile all'URL http://www.legalis.net/jurisprudence-decision.php3?id_article=1203

in materia di comunicazioni elettroniche non sollecitate, in particolare quando l'indirizzo di posta elettronica sia quello fornito da una pubblica amministrazione (o da altro datore di lavoro).

Se infatti si assume che l'indirizzo fornito sia uno strumento "aziendale", di proprietà della pubblica amministrazione, si potrebbe dubitare che il dipendente, cui la casella di posta elettronica sia assegnata per esigenze di servizio, possa attivarsi nei confronti dello *spammer*, ed in particolare che possa ricorrere al Garante o al Giudice ordinario, ai sensi, rispettivamente, degli artt. 141 e seguenti e dell'art. 152 del Codice. Se un'interpretazione proprietaria fosse portata alle sue conseguenze estreme, il dipendente non potrebbe far altro che segnalare la vicenda alla pubblica amministrazione, che potrebbe poi decidere autonomamente come reagire. Questo significa anche che, di fronte ad una raccolta di indirizzi di posta elettronica, ad esempio sul sito di una determinata pubblica amministrazione, e di un conseguente invio di una *email* indesiderata a tutti i dipendenti della stessa da parte dello *spammer*, lo stesso potrebbe sostenere che si tratti di una sola violazione della normativa, e non di un numero di violazioni pari alle *email* inviate. Ne deriverebbe un rischio particolarmente limitato per lo *spammer*, riducendosi sensibilmente la capacità deterrente degli strumenti posti a tutela della privacy dell'individuo, che deve essere tutelata anche nell'esercizio della propria attività lavorativa.

Il pericolo è reale, come dimostra un semplice esempio di origine personale. Recentemente ho ricevuto due messaggi commerciali non sollecitati, da parte della medesima azienda, indirizzati alla casella di posta elettronica dell'università. Alla fine del primo messaggio commerciale, l'avvertimento relativo all'applicazione della normativa sulla protezione dei dati riportava, tra l'altro: "La informiamo che gli indirizzi *email* presenti nel nostro archivio provengono da elenchi e servizi di pubblico dominio

pubblicati anche via Web o per autorizzazione dei possessori". Nessuna autorizzazione era stata data dal sottoscritto. La pubblicazione sul Web, come ha affermato esplicitamente il Garante, non comporta peraltro che gli indirizzi possano essere utilizzati liberamente[29], ma solo per l'uso istituzionale[30]. La *mail* era quindi qualificabile come *spam*.

Nel secondo messaggio, qualche settimana più tardi, l'avvertimento finale cambia, e recita, tra l'altro: "La informiamo che gli indirizzi *email* presenti nel nostro archivio non provengono da elenchi e servizi di pubblico dominio. Gli indirizzi di questa lista sono di proprietà di Atenei già nostri Clienti, o sono presenti per autorizzazione dei possessori con iscrizione diretta nella *home page* del nostro sito". Chi invia posta commerciale ha compreso il vantaggio che può derivargli dal riconoscimento della proprietà dell'indirizzo da parte della pubblica amministrazione, e lo afferma esplicitamente. Non solo. L'avvertimento continua: "La rimozione dalle nostre liste, qualora si tratti di indirizzi di proprietà di Atenei, dovrebbe essere richiesta dal legittimo proprietario, quindi esclusivamente dall'Ateneo in questione, richiesta da effettuarsi per singolo indirizzo e non per «gruppi» di indirizzi".

Lo *spammer* non si limita, presentando la propria interpretazione come norma cogente, ad inibire il dipendente (sia pure con un curioso uso del condizionale, che lascia trasparire almeno qualche dubbio, mascherato da gentile concessione) ad intraprendere eventuali azioni sulla base del Codice, ma, con una certa incoerenza, sostiene che qualora l'amministrazione chieda la cancellazione degli indirizzi dalla *mailing list* dello *spammer*, questo

[29] Garante per la protezione dei dati personali, parere 29 maggio 2003, Garante per la protezione dei dati personali, decisione 20 marzo 2002.

[30] Garante per la protezione dei dati personali, decisione 28 maggio 2002; si veda anche, in senso parzialmente contrario, Giud. Pace Padova, 3 febbraio 2004, n. 233, in *Dir. Regione*, 2004, 799.

possa essere fatto solo per indirizzi singoli. Mentre questa ultima affermazione è più facilmente confutabile (se gli indirizzi sono di proprietà dell'amministrazione, la stessa può decidere che siano cancellati anche tutti insieme, ed in questo senso l'interpretazione proposta potrebbe ritorcersi contro lo *spammer*), la questione sulla proprietà è più sottile. Ma è comunque l'interpretazione opposta, secondo la quale è l'individuo che deve avere (eventualmente anche non in via esclusiva) la legittimazione ad agire davanti al Garante o davanti al Giudice ordinario, a convincere maggiormente, e non solo per i motivi "pratici" evidenziati.

L'indirizzo di posta elettronica assegnato ad un dipendente, specie se riporta nell'indirizzo dati personali (il cognome, eventualmente anche il nome), fa riferimento ad un soggetto determinato, che sopporta in via immediata e principale gli abusi compiuti da altri. Quando una *mail* non sollecitata è spedita ad un indirizzo di posta elettronica assegnata ad un soggetto determinato si tratta, in definitiva, di una violazione della riservatezza di tale soggetto, e di un indebito trattamento dei dati personali dello stesso soggetto. Lo *spamming* comporta infatti una duplice violazione della privacy dell'individuo, e una duplice violazione del Codice. Si ha infatti, una violazione dell'art. 23 del Codice, configurandosi un trattamento illecito di dati personali (l'indirizzo di posta elettronica), effettuato senza consenso preventivo, ed una violazione dell'art. 130 del Codice, dedicato in modo specifico alle comunicazioni indesiderate, configurandosi l'invasione della sfera di riservatezza del destinatario[31].

Vi è poi un ulteriore motivo pratico. Se il dipendente non potesse lamentarsi direttamente, dovrebbe rivolgersi ogni volta alla pubblica amministrazione, che si potrebbe trovare soggetta ad un sovraccarico di richieste, a meno di sostenere che il dipendente non

[31] Cfr. Giud. Pace Napoli, 10 giugno 2004, in *Foro it.*, 2004, I, 2908.

abbia nemmeno questa facoltà, trattandosi di uno strumento aziendale in relazione al quale ogni tipo di tutela è riservata all'amministrazione. Non solo questa interpretazione si presenta come particolarmente rigida e non rispettosa della riservatezza dell'individuo, ma essa potrebbe poi esporre la pubblica amministrazione a responsabilità, quanto meno per mancato controllo, qualora al dipendente arrivassero *mail* dal contenuto osceno, o violento, o comunque idoneo a turbare il destinatario ed a creare una ambiente di lavoro ostile.

La soluzione più ragionevole sembra pertanto quella di consentire una doppia tutela nei confronti dello *spamming*, che deriva dalla qualifica di "interessato" riconoscibile sia al dipendente che alla pubblica amministrazione. Da un lato, la pubblica amministrazione deve avere la facoltà di difendere il proprio strumento "aziendale" non solo da abusi del dipendente (con i limiti e con le garanzie che legge e Costituzione prevedono), ma anche da abusi di terzi che colpiscono il dipendente ed espongono a rischi altri strumenti aziendali. Dall'altro, il dipendente deve avere la facoltà di difendere la propria casella di posta elettronica da messaggi non sollecitati e potenzialmente lesivi della propria riservatezza, intesa in senso ampio e del proprio tempo.

Si ha, in sostanza, una cogestione, disgiunta, dell'indirizzo, funzionale alla maggiore tutela possibile. Se problemi possono sorgere nel rapporto tra dipendente e pubblica amministrazione in relazione alla confidenzialità della posta elettronica, non ne dovrebbero invece sorgere in merito al rapporto con gli *spammers*, in quanto amministrazione e dipendente condividono l'interesse a non ricevere posta indesiderata. Ma anche l'interesse di uno solo dei due deve consentire di intraprendere le iniziative di tutela individuate dall'ordinamento.

Che lo schema esclusivamente proprietario non possa funzionare è confermato da ulteriori considerazioni, relative alla portata del "segreto epistolare". Si prendano tre esempi "offline".

La Pretura di Verona, con pronuncia in sede cautelare del 6 novembre 1990 inibisce la pubblicazione della corrispondenza di Elio Vittorini da parte di un settimanale, in assenza del consenso degli eredi dello stesso[32]. Di fronte alla vendita delle lettere, a fini di sfruttamento commerciale, non prevale né l'aspetto proprietario riferito alla lettera nella sua materialità, né la tutela del diritto d'autore, ma la necessaria tutela del carattere confidenziale della corrispondenza. In sede di merito, il Tribunale di Milano, con pronuncia del 30 giugno 1994[33], ribadisce, in riferimento all'art. 93 della l. 22 aprile 1941, n. 633 (legge sul diritto d'autore) "il diritto soggettivo assoluto alla riservatezza epistolare e la sua prevalenza sul diritto di proprietà materiale sulla corrispondenza (come anche sull'eventuale diritto d'autore)".

Nello stesso senso, il Tribunale di Milano, con pronuncia del 5 marzo 1998[34], afferma che costituisce violazione del diritto alla riservatezza la pubblicazione di corrispondenza a carattere confidenziale di Federico Fellini, in assenza del consenso dei parenti o congiunti, ed indipendentemente dal consenso del destinatario delle lettere.

Infine, il Tribunale di Milano, con ordinanza del 9 settembre 2004[35], ha ritenuto una corrispondenza epistolare confidenziale, e quindi non pubblicabile senza il consenso degli aventi diritto, sulla base dell'aspettativa di riserbo e discrezione del destinatario.

In tutti e tre i casi, si è valutato come preponderante il segreto epistolare, espressione di un diritto personalissimo e

[32] Pret. Verona, 30 ottobre 1990, in *Dir. Inf.*, 1991, 71.
[33] Trib. Milano, 30 giugno 1994, in *Foro it.*, 1995, I, 1667.
[34] Trib. Milano, 5 marzo 1998, in *Dir. Inf.*, 1999, 410.
[35] Trib. Milano, 9 settembre 2004, in *Foro it.*, 2005, I, 1, 249.

fondamentale, sugli aspetti proprietari, espressioni di interessi economici. In tutti e tre i casi le lettere, materialmente, erano di proprietà dei destinatari. La presenza, e la necessaria tutela, del segreto epistolare hanno costituito peraltro un limite alla facoltà di godimento di quel "bene", con riferimento particolare al contenuto dello stesso. La tutela della riservatezza del mittente, nel momento in cui sono scritte cose personali, che si può supporre che lo stesso non avrebbe voluto che fossero diffuse, comporta una intrasferibilità delle lettere, e a maggior ragione una non pubblicabilità delle stesse.

Ancora più importante è rilevare che il sacrificio delle facoltà di godimento relative al diritto di proprietà (delle lettere) non è avvenuto per la presenza di un altro diritto economico, il diritto di autore in capo agli eredi, ma per la presenza di un diritto dell'individuo, indipendentemente dalla sua fama o dal valore "artistico" o "storico" di ciò che è scritto. Il che significa che si tratta di una protezione che può, o meglio che deve, essere garantita a tutti.

Ferme restando le difficoltà interpretative e applicative, resta il fatto che la proprietà, incontestata, delle lettere, è destinata a soccombere, nel momento in cui si vuole disporre delle stesse, di fronte alla tutela dell'aspettativa di riservatezza di ciò che si scrive in una corrispondenza "chiusa" ad un altro soggetto.

Pur nella diversità delle situazioni e delle fattispecie, non sorprende pertanto che la "proprietà" dell'indirizzo di posta elettronica da parte del datore di lavoro, pubblico o privato, non implichi necessariamente che lo stesso possa aprire la corrispondenza del dipendente. Il datore di lavoro non può aprire la posta cartacea del dipendente, anche se indirizzata presso il luogo di lavoro. Perché questo dovrebbe essere consentito nei confronti della posta elettronica? Si potrebbe sostenere che la differenza è data dal fatto che la posta tradizionale è consegnata dal servizio pubblico, mentre la posta elettronica del dipendente si avvale del sistema approntato

dal datore di lavoro. Ma questo proverebbe troppo, in quanto non ci sarebbe più alcuna garanzia di riservatezza nel luogo di lavoro (locali di proprietà del datore di lavoro) od in riferimento al contenuto delle telefonate (telefoni di proprietà del datore di lavoro), e così via. Il fatto è che la proprietà dei sistemi non implica il venir meno della segretezza delle comunicazioni e della corrispondenza[36].

Sempre in via analogica, si possono proporre altri argomenti interpretativi. Si pensi all'ipotesi di locazione. Può il proprietario aprire la cassetta delle lettere relativa all'appartamento locato, nella quale l'affittuario ha posto un'etichetta con il proprio nome? Può il proprietario aprire la corrispondenza contenuta in quella buca delle lettere? No, il proprietario non può. E allora, perché tutto questo dovrebbe essere consentito in riferimento alla posta elettronica?

5. Filtri anti-spam *e configurazione degli indirizzi dei dipendenti pubblici*

La lotta allo *spamming* si avvale non solo di strumenti giuridici, ma anche di mezzi tecnologici[37], quali i filtri *anti-spam*. Fino a qualche anno fa si pensava che, combinati con meccanismi di *self-regulation*, tali filtri potessero essere sufficienti a risolvere il problema. Purtroppo, non è così. A volte essi non filtrano tutti i messaggi non desiderati, riproponendo pertanto, anche se in misura minore, i fastidi sopra evidenziati. A volte essi filtrano messaggi legittimi ritenendoli erroneamente *spam* (c.d. "falsi positivi"), determinando pertanto la possibile perdita di messaggi legittimi. Tra l'altro, qualora l'indirizzo *email* sia utilizzabile anche per motivi personali, in via consuetudinaria, senza espressi divieti da parte del

[36] V. DATA PROTECTION WORKING PARTY, *Working document on the surveillance*, cit., p.to 4.1.

[37] D. SORKIN, *Technical and Legal Approaches to Unsolicited Electronic Mail*, *U.S.F.L. Rev.* 325 (2001).

datore di lavoro, questo potrebbe porre problemi di responsabilità qualora fossero filtrati, e scartati, messaggi personali[38].

In questo senso, l'utilizzo di filtri *anti-spam* da parte della pubblica amministrazione deve tenere conto non solo della politica, espressa o meno, di utilizzazione della posta elettronica, ma anche di considerazioni relative all'efficacia, all'aggressività ed al funzionamento degli stessi. La pubblica amministrazione che decide di utilizzare un filtro *anti-spam*, si trova di fronte a più opzioni. Può impostare il filtro in modo da apporre una "etichetta" alle *mail* sospette, con ciò allertando il dipendente, ma esponendolo alla stessa quantità di *spam* (o raddoppiandolo addirittura, qualora ogni messaggio sospetto fosse accompagnato da un messaggio preventivo di avvertimento). Oppure deviando le *mail* sospette in una cartella specifica dedicata ("*Spam*", o, meglio, "*Probabile Spam*"), che il dipendente avrebbe poi l'onere di controllare periodicamente per verificare l'assenza di falsi positivi. Questa soluzione renderebbe più facile la consultazione della posta non sospetta nella casella "personale" (che potrebbe comunque contenere messaggi sfuggiti al filtro), ma rischia comunque di perdere, nella massa dei messaggi di *spam*, i "falsi positivi". Oppure ancora direttamente distraendo i messaggi sospetti, senza che questi arrivino nella casella di posta elettronica del dipendente. Nel momento in cui l'indirizzo non è ritenuto utilizzabile per motivi personali, il rischio di falsi positivi verrebbe assunto direttamente dalla pubblica amministrazione (e dal cittadino, e da chi comunque corrisponde con essa).

Ma, a questo punto, un altro aspetto deve essere chiarito, e riguarda la configurazione dell'indirizzo assegnato al dipendente. Si possono ipotizzare tre soluzioni principali, per quanto riguarda la

[38] Si pensi, sia pure in ambito diverso, alla *class action* recentemente portata avanti negli Stati Uniti dai clienti di Verizon, che aveva bloccato, per combattere lo spam, una grande quantità di messaggi, legittimi, provenienti dall'estero.

parte dell'indirizzo alla sinistra del segno @: un riferimento diretto alla persona cui è assegnato, con l'inserimento del cognome, eventualmente accompagnata da nome o iniziale; una sigla alfanumerica (ad esempio nl147), che non consente l'immediata identificazione della persona partendo dall'indirizzo (ma indirettamente sì, con quanto ne consegue in termini di applicazione del Codice, ai sensi della definizione di "dato personale" di cui all'art. 4, comma 1, lett. b, trattandosi comunque di identificabilità); un riferimento non alla persona, ma all'ufficio.

Nel primo caso, l'aspettativa di "personalità" dell'individuo è più alta sia per quanto riguarda gli aspetti relativi ad un possibile controllo che per quanto riguarda la tutela da *spamming*. Inoltre, è più alta anche per quanto concerne il corrispondente, esterno all'amministrazione, del dipendente, a cui più difficilmente può applicarsi il criterio del "non può non sapere", peraltro criticabile anche in relazione al dipendente. Nel terzo caso, la natura di strumento aziendale è più evidente, con una maggiore apertura per la pubblica amministrazione. Nel secondo caso, siamo di fronte ad una situazione intermedia.

Sotto una diversa prospettiva, peraltro, la configurazione degli indirizzi di posta elettronica dei dipendenti delle pubbliche amministrazioni deve tenere conto delle esigenze di organizzazione delle stesse e delle aspettative di trasparenza dei cittadini. L'indirizzario elettronico di una pubblica amministrazione deve avere come finalità principale la fruibilità da parte dei cittadini, che non devono trovarsi di fronte ai problemi che spesso incontrano quando cercano di contattare telefonicamente soggetti all'interno dell'amministrazione. Il problema è quindi quello di conciliare esigenze che possono apparire, per certi versi, opposte.

A parte la costruzione formale degli indirizzi, si tratta poi di definire una politica dell'uso degli strumenti informatici, anche in

analogia, quando possibile e razionale, con le soluzioni adottate per altri mezzi di comunicazione personale. Sostenere che l'uso della posta elettronica nel luogo di lavoro, con indirizzi non aziendali, del tipo *webmail*[39], comporta la conseguenza di una distrazione del tempo lavorativo per fini non lavorativi può essere vero. Ma allora non si dovrebbe consentire l'uso del cellulare nell'orario di lavoro, trattandosi comunque di possibili comunicazioni private.

In questo senso, si dovrebbe fare riferimento a criteri di ragionevolezza, che però non sempre sono così evidenti e condivisi nella coscienza sociale. Certamente, il primo criterio di ragionevolezza, in assenza di una disciplina specifica, dovrebbe essere quello della trasparenza dei comportamenti e delle regole[40]. Qualsiasi soluzione l'amministrazione (così come ogni datore di lavoro) dovesse adottare, essa dovrebbe esplicitare le proprie scelte attraverso una chiara politica della privacy relativa alle comunicazioni elettroniche sul posto di lavoro, tanto con riferimento agli aspetti di riservatezza e confidenzialità delle comunicazioni, quanto a quelli di tutela dalle comunicazioni non sollecitate.

[39] V., sulle problematiche di un uso di indirizzi *webmail* sul luogo di lavoro, DATA PROTECTION WORKING PARTY, *Working document on the surveillance*, cit., p.to 4.4.

[40] V. DATA PROTECTION WORKING PARTY, *Working document on the surveillance*, cit., p.to 3.1.3.

ALLA RICERCA DELLA SICUREZZA: SOCIETÀ, REGOLE E TECNOLOGIE DIGITALI

Paolo Guarda

1. Premessa

Il tema sicurezza rappresenta un ambito di ricerca unico ed appassionante, ma definirne i contenuti è impresa ardua. Numerose sono le implicazioni sociali ed economiche che ne alterano le componenti e ne sbiadiscono i confini[1].

Quando si parla di Internet vengono spesso utilizzate espressioni roboanti ed evocative quali "rete delle reti" e "rete globale", che sembrano voler avvolgere il mondo digitale di un velo di misticismo che ne scolorisce i tratti e ne rende evanescenti i contenuti.

A causa delle sue innegabili implicazioni sociali, Internet suscita in molti preoccupazione: si pensa, infatti, che essa possa rappresentare uno strumento nelle mani di criminali e terroristi. A-territoriale ed a-nazionale per sua intrinseca qualità, Internet spaventa i governi perché i contenuti che in esso viaggiano sono

[1] Per uno studio del rapporto tra sicurezza e libertà nel mondo digitale v. da ultimo N.W. PALMIERI, *Sicurezza o libertà? Introduzione al diritto di Internet*, Bologna, 2005; v. anche K.A. TAIPALE, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 9 *Int'l J. Comm. L. & Pol'y* 8 (2005).

difficilmente controllabili[2].

I tragici eventi dell'11 settembre e le inevitabili ripercussioni che ne sono derivate hanno rafforzato una tendenza già in atto, modificando il modo in cui le persone concepiscono le responsabilità dello Stato e riconsiderando il suo tradizionale ruolo di custode della sicurezza.

È ormai largamente condivisa l'idea secondo la quale la tecnologia non è priva di valori[3]. La struttura di un software, l'architettura dell'ambiente digitale, o semplicemente, il codice binario riflettono e formano allo stesso tempo i valori del sistema. Esiste un rapporto complesso tra la storia delle idee ed il mutamento tecnologico tale da poter provocare cambiamenti economici, oltre che trasformazioni nelle istituzioni sociali. Ma, la relazione tra tecnologia ed idee agisce anche in senso opposto, potendo i cambiamenti sociali e culturali modificare i contesti digitali. Lo stato di guerra, nonché la fiducia o la diffidenza nei confronti del nuovo "mondo globalizzato" creano un nuovo ambiente telematico.

La sicurezza informatica non è materia da riservare soltanto ai tecnici perché è probabile che non si otterrebbe un corretto bilanciamento tra accessibilità e segretezza nel contesto digitale. Si corrono, poi, dei rischi nel lasciare la decisione ai soli esperti di sicurezza operanti nelle organizzazioni governative: sussistono,

[2] V. M.D. BIRNHACK, N. ELKIN-KOREN, *The Invisibile Handshake: The Reemergence for the State in the Digital Environment*, *Virginia Journal of Law & Technology*, 2003 reperibile sul sito Web http://ssrn.com; P. BONETTI, *In nome della sicurezza internazionale si possono limitare i diritti di difesa, di giusto processo e di proprietà di potenziali finanziatori del terrorismo?*, in *Quaderni Cost*., 2006, 144. Per un'analisi del rapporto tra privacy e sicurezza dopo l'attacco alle "Torri gemelle", v. P. GUARDA, *Agenti software e sicurezza*, in G. PASCUZZI (a cura di), *Diritto e tecnologie evolute del commercio elettronico*, Padova, 2004, 315.

[3] Cfr. L. LESSIG, *Open Code and Open Societies: Values of Internet Governance*, 74 *Chi.-Kent L. Rev* 1045 (1999); ID., *Free culture. How big media uses technology and the law to lock down culture and control creativity*, New York, 2004; ID., *Code and other laws of cyberspace*, New York, 1999.

infatti, fortissimi "incentivi perversi" e stimoli che inducono a nascondere le informazioni sulla sicurezza informatica.

Il tema della trasparenza o della segretezza è stato centrale in molti dei dibattiti dedicati ad Internet ed alle problematiche ad essa connesse: utilizzazione libera contro forti *copyright*; vasta diffusione delle informazioni personali contro la protezione della privacy; *free software* contro software proprietari. Internet è un grande motore per la produzione di "sapere libero", perché consente di condividere a basso costo informazioni tra un numero enorme di persone. Determinare un corretto livello di accessibilità ed apertura nella procedura di sicurezza informatica è di cruciale importanza, per evitare che l'incomparabile utilità di Internet venga gravemente compromessa. Comunque, per mantenere i vantaggi derivanti dallo strumento in parola per l'educazione, il commercio, la democrazia, e tutte le altre sue possibili applicazioni, è necessario mettere a punto tecnologie, leggi e istituzioni in grado di realizzare la giusta combinazione tra *openness* ed *hiddenness* nella sicurezza informatica. Questa, invero, assume una rilevanza importantissima soprattutto per stabilire cosa debba essere tenuto nascosto e cosa invece debba essere reso accessibile, in un mondo che fa della facilità di comunicazione e della libertà nell'accesso e scambio dei dati i principi che regolano la "comunità telematica"[4].

Nel secondo paragrafo di questo saggio si analizzerà il concetto di "sicurezza"; nel paragrafo terzo si prenderà in esame l'esperienza statunitense sia per quanto riguarda l'opera del legislatore volta a rafforzare l'attività di *intelligence* e prevenzione, sia per le numerose tecnologie di sorveglianza che nel paese

[4] In N. NEGROPONTE, *Essere digitali*, Milano, 1995, 241, si legge: "la facilità di accesso alle informazioni, la mobilità e la possibilità di indurre cambiamenti è ciò che renderà il futuro tanto diverso dal presente".

americano vengono impiegate per contrastare il terrorismo[5]; nel quarto paragrafo si descriverà l'attuale situazione italiana dopo l'emanazione del c.d. "pacchetto sicurezza" con riferimento alla discussione in atto in ambito comunitario in tema di *data retention*; nell'ultimo paragrafo si svolgeranno alcune considerazioni conclusive.

2. Definizione del concetto di sicurezza e sue implicazioni in ambito informatico

Con l'espressione sicurezza si può intendere una situazione di affidabilità che induce un soggetto a sentirsi protetto rispetto all'ambiente esterno e difeso in situazioni di pericolo e di aggressioni che possano compromettere la sua sfera d'azione.

L'analisi di questo concetto può svolgersi su diversi piani: sociale, economico e giuridico[6].

Da un punto di vista sociale, osserviamo l'interazione tra due modalità di comportamento: da un lato abbiamo gli scambi a livello orizzontale che si stabilizzano sul buon funzionamento tra le conseguenze dell'azione ed il positivo giudizio che ad esso si dà; dall'altro l'integrazione che si concretizza attraverso l'intesa tra soggetti, norme condivise dalla comunità e valori comuni. La definizione del termine "sicurezza" deve coinvolgere l'analisi della sua percezione su entrambi questi livelli[7].

---

[5] Per uno studio sulle diversità d'approccio tra Unione europea e Stati Uniti d'America ai problemi relativi alla globalizzazione di Internet, v. J.S. BAUCHNER, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, 26 *Brook. J. Int'l L.* 689 (2000).

[6] Cfr. G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 2.

[7] J. HABERMAS, *La costellazione postnazionale, Mercato globale, nazioni e democrazia*, Milano, 1999, 61; CORASANITI, *Esperienza giuridica e sicurezza informatica*, cit., 2. Abbiamo un'ottima analisi sociologica sul tema in W. SOFSKY, *Rischio e sicurezza*, Torino, 2005.

Su un piano economico, si possono dare al concetto di sicurezza due differenti letture: si può parlare di un semplice stato di fatto, o si possono considerare determinate condizioni ottimali per la propria attività tali da ridurre i pericoli e i rischi. La sicurezza intesa quale insieme di condizioni che limitano il rischio fino a ridurlo in prossimità dello zero va considerata come un costo nell'attività economica. Si tratta di un valore aggiunto solo per chi opera per la riduzione del rischio (assicurazioni, polizia, etc.).

La situazione che noi definiamo "sicurezza" si basa su un equilibrio tra fiducia nel mondo esterno e rischio accettabile[8]. La stessa espressione "rischio" trova storicamente la sua origine nell'ambito della navigazione nei secoli XVI e XVII, quando indicava il navigare in acque ignote, non segnalate nelle carte[9]. Questo rischio trasposto in chiave moderna diviene "dinamismo che muove una società legata allo scambio, che intende determinare il proprio futuro anziché lasciarlo alla religione, alla tradizione o ai capricci della natura"[10].

Allorché a livello sociale si avverte il problema "sicurezza", s'impone, in prima battuta, un intervento pubblico di regolazione e garanzia[11]: ciò comporta una continua opera di vigilanza, verifica, promozione e dialettica tra le posizioni coinvolte, con un'attività di costante adeguamento dei parametri e standard di sicurezza alle

[8] Funzionale al tema della sicurezza è il concetto di "rischio" il quale non rappresenta solo una condizione individuale ma in determinati contesti e scenari diviene di interesse globale.

[9] È curioso, inoltre, notare come altri termini, come "pirata" e "navigare", usualmente riferiti ad Internet siano ripresi dal gergo marinaro.

[10] CORASANITI, *Esperienza giuridica e sicurezza informatica*, cit., 4.

[11] Il problema e la discussione della sicurezza dei sistemi si afferma gradualmente. Inizialmente si registra la tendenza a privilegiare gli interventi diretti a prevenire accessi fisici al sistema e ai dati con la previsione di condotte incriminatici, per sviluppare poi una corretta analisi delle possibili ipotesi di intervento.

condizioni che variano in rapporto alle conoscenze tecnologiche o che derivano da fattori esterni o interni di rilevante importanza[12].

Le tecnologie digitali, oltre a contribuire alla diffusione di rischi, offrono anche possibili rimedi contro di essi: "se è vero che i ritrovati tecnologici possono essere all'origine di intrusioni nella vita delle persone, è altrettanto vero che un uso accorto della tecnologia può scongiurare (o quanto meno depotenziare) i rischi più inquietanti"[13].

L'insicurezza del sistema informatico è stata valutata talvolta come una caratteristica innata originata da una complessità di fattori in continua evoluzione e quindi priva di una possibile soluzione. Da ciò lo slogan ripetutamente affermato negli ultimi anni: "la sicurezza non è un risultato, bensì un processo". Questa affermazione, nonostante l'apparente semplicità, non deve però essere intesa in senso assoluto e far passare l'idea che l'insicurezza sia intrinsecamente ed inevitabilmente connessa allo sviluppo delle tecnologie digitali. Bisogna invece persuadersi della necessità di "costruire progressivamente una metodologia nella quale oltre agli aspetti tecnologici oggi prevalenti, convivano elementi di carattere giuridico (definizione e interpretazione delle regole legislative, amministrative, di autodisciplina volontaria delle categorie, contrattuali), di carattere tecnico-scientifico (definizione di standard e rimedi), di carattere organizzativo (istituzione di *task force* dedicate o di articolazioni organizzative specializzate negli interventi possibili) ed infine di carattere economico (analisi dei costi-benefici

[12] Per approfondimenti sugli standard e sulle norme tecniche di sicurezza, v. B. SIEFF, *Responsabilità civile e standard di sicurezza. Analisi di un rapporto sul paradigma dell'attività di produzione e rigenerazione di dispositivi medici*, tesi di dottorato. Per un'analisi degli standard di sicurezza nello specifico tema dei pagamenti *on-line*, v. P. GUARDA, *Sicurezza dei pagamenti e privacy nell'e-commerce*, in *Diritto dell'Internet*, 2005, 91.

[13] G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002, 63.

delle situazioni concrete, individuazione delle risorse utilizzabili, ammortizzazione pianificata dei costi derivanti dall'esposizione a rischio)"[14].

Sul piano giuridico, sia civile che penale, si assiste ad un approccio frammentato caratterizzato dall'estensione di categorie e regole "vecchie" a nuovi fenomeni che spesso poco hanno in comune con l'esperienza precedente. Il che conduce ad interpretazioni sostanzialmente lesive del principio di eguaglianza[15].

Internet allo stesso tempo collega e mette in crisi, offre opportunità prima impensabili e presenta rischi non ancora pienamente compresi, facilita la comunicazione e rende sempre più insicuri. È necessario allora uno studio che tenga conto di tutti i piani sui quali il problema si presenta, quello giuridico, quello sociale e quello economico, trattandosi di ambiti che convivono e sono parimenti fondamentali nei diversi settori di regolamentazione, sia a livello nazionale che internazionale, nel settore pubblico come in quello privato.

3. Tecnologie per la sorveglianza v. *principi costituzionali: l'esperienza degli Stati Uniti d'America*

L'attacco terroristico alle Torri Gemelle dell'11 settembre, messo a segno da un'organizzazione occultamente insediata ed efficacemente ramificata nel tessuto della società americana, ha costretto le autorità statunitensi a potenziare, sui piani normativo ed operativo, l'intero apparato dei servizi di sicurezza. Conseguentemente la stessa opinione pubblica è stata obbligata ad interrogarsi sul corretto bilanciamento tra la sfera dei diritti ed il bisogno di sicurezza che ha portato all'incremento dei poteri di

[14] CORASANITI, *Esperienza giuridica e sicurezza informatica*, cit., 15-16.

[15] Per approfondimenti v. N. IRTI, *L'età della decodificazione*, IV ed., Milano, 1999; CORASANITI, *Esperienza giuridica e sicurezza informatica*, cit., 19.

sorveglianza in capo agli organi esecutivi dello Stato[16].

Il 16 ottobre 2001 il Congresso americano approvava a tempo di record, e con una maggioranza schiacciante che trovava riscontro su un elevatissimo consenso popolare, una nuova legge chiamata *Usa Patriot Act* (acronimo di *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, d'ora in avanti USAPA)[17], la quale garantiva ulteriori poteri di intercettazione e sorveglianza alle autorità federali, rimuoveva le barriere tra gli organi preposti all'applicazione della legge e quelli dell'intelligence, aumentava le possibilità di accedere ad informazioni riservate nel campo finanziario per contrastare i finanziamenti ai terroristi e consentiva all'*Attorney General* di incarcerare o di espellere gli stranieri sospettati di legami con il terrorismo[18].

Seguirono numerose prese di posizione e critiche da parte di vari settori ed organizzazioni della società civile che disapprovavano la decisione delle autorità americane, ai loro occhi troppo lesiva delle libertà e dei diritti dei cittadini, e non basata sul necessario *check and balance* che precedentemente conferiva alle corti l'opportunità di

[16] V. da ultimo G. FROSIO, *Cosa resta della privacy? – diritto alla riservatezza dell'"uomo medio" dopo l'11 settembre*, in *Ciberspazio e dir*., 2005, 173; R. WARNER, *Surveillance and The Self: Privacy, Idendity, and Techonology*, 54 *DePaul L. Rev*. 847 (2005); C.S. FISHMAN, *The Future of Internet Surveillance: a Symposium to Discuss Internet Surveillance, Privacy & the Usa Patriot Act: Surveillance, Records & Computers: Technologies and the Internet: The Impeding Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 *Geo. Wash. L. Rev*. 1503 (2004); L. NELSON, *Public Administration and Civil Liberties - Protecting the Common Good: Technology, Objectivity, and Privacy*, 62 *P. A. R. Suppl*. 1 (2002); J.B. GOULD, *Playing with Fire: The Civil Liberties Implications of September 11th*, 62 *P. A. R. Suppl*. 1, 74 (2002); M.W. SPICER, *The War on Terrorism and the Administration of the American State*, *ibidem*, 63.

[17] Pub. L. No. 107-56, 115 *Stat.* 272 (2001).

[18] V. J.C. TING, *Unobjectionable But Insufficient-Federal Initiatives in Response to the September 11 Terrorist Attacks*, 34 *Conn. L. Rev*. 1145 (2002).

verificare che non avvenissero abusi nella gestione ed applicazione dei poteri di sorveglianza conferiti alle autorità statali.

Circa un anno dopo (25 novembre 2002) veniva emanato, l'*Homeland Security Act*[19], che si inseriva sul solco scavato dall'USAPA ed istituiva un nuovo *Department of Homeland Security*, cui doveva essere devoluto il compito di prevenzione e protezione contro gli atti terroristici.

Crescente importanza hanno, così, assunto gli studi dedicati all'impatto sulla società e sul tradizionale *right to privacy* delle nuove tecnologie applicate nell'ambito delle intercettazioni telefoniche e telematiche ed, in generale, nell'attività investigativa di intelligence. La possibilità di utilizzare sistemi di intercettazione telematica (si veda tra tutti il software *Carnivore* approntato dal FBI) nella lotta contro il terrorismo internazionale, infatti, se da un lato presenta notevoli ed evidenti vantaggi quanto ad efficacia ed efficienza, dall'altro presta il fianco a legittime critiche da parte di quanti denunciano l'eccessivo carattere intrusivo di questi strumenti e i possibili abusi che la loro realizzazione comporta.

Occorre chiedersi se si debba inevitabilmente affrontare il problema dal punto di vista di una necessaria e difficilmente superabile contrapposizione tra il concetto di sicurezza e il principio di privacy, o se è possibile trovare una via che porti non solo e non tanto ad un bilanciamento tra questi, ma che faccia apparire quanto la realizzazione del primo si concretizzi inevitabilmente nell'attuazione del secondo.

La sicurezza informatica è stata profondamente segnata dall'implementazione, da parte delle autorità americane, di nuovi strumenti di investigazione telematica che pongono però notevoli problemi in quanto anch'essi invasivi delle libertà e della riservatezza dei cittadini. Daremo di seguito una rapida descrizione

[19] Pub. L. No 107-296, 116 *Stat.* 2135 (2002).

di alcuni di questi strumenti tecnologici implementati dai servizi di intelligence americana. Alcuni di essi sono ancora in uso, altri sono stati, almeno ufficialmente, abbandonati.

Nel luglio del 2000 l'FBI presentava *Carnivore*[20]: si trattava di un software in grado di "catturare" messaggi *e-mail* di persone sospette o di "tracciare" messaggi spediti verso e da il loro indirizzo di posta elettronica. "Carnivore" era dotato di un filtro che poteva essere impostato per "passare in rassegna" diversi "pacchetti digitali" per specifiche stringhe di testo o con ben definiti *target* di messaggi provenienti da un computer o da un indirizzo *e-mail*. Il programma poteva lavorare secondo due differenti impostazioni: *pen* o *full*. In *pen mode*, intercettava solo le informazioni relative agli indirizzi, includenti l'indirizzo *e-mail* del mittente e del destinatario e l'oggetto del messaggio[21]: tale impostazione risultava utile per le autorità, anche se il contenuto del messaggio non poteva essere letto per la presenza di un sistema di criptazione. In *full mode*, invece, intercettava l'intero contenuto del messaggio. Una volta che i "pacchetti" desiderati erano stati raccolti, l'FBI doveva ricostruirli per successive analisi[22].

---

[20] V. i contributi di P.P. SWIRE, *What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory*, reperibile all'URL: http://www.arxiv.org/abs/cs.CY/0109089, 50-51; A. ETZIONI, *Implications of Select New Technolgies for Individual Rights and Public Safety*, 15 *Harv. J. of L. & Tech.* (2002); C.D.H. SCHULTZ, *Unrestricted Federal Agent "Carnivore" and the Need to Revise the Pen Register Statute*, 76 *Notr. L. Rev.* 1215 (2001); T.C. HASS, *Carnivore and the Fourth Amendment*, 34 *Conn. L. Rev.* 261 (2001).

[21] Un'autorevole voce dubita della reale utilità delle informazioni così raccolte: v. S. RODOTÀ, *Dei diritti e delle garanzie nella guerra contro Al Quaeda*, reperibile sul sito Web http://www.repubblica.it

[22] Tale procedura richiedeva due altri programmi: il *Packteer* e il *Coolminer*. Il *Packteer* ricostruiva la sessione TCP (*Transmission Control Protocol*) dagli IP dei "pacchetti", di seguito salvati in maniera tale da poter essere letti da *Coolimier*. Questo era un programma di lettura che permetteva all'FBI di visualizzare la sessione TCP nuovamente ricostruita. In aggiunta, tale ultimo programma, tramite

Nonostante l'implementazione di "Carnivore", il governo americano era stato notevolmente ostacolato nel suo compito dall'impossibilità di decifrare un numero di messaggi sempre crescente a causa della diffusione della c.d. "criptazione forte"[23]. Occorre per inciso precisare che la crittografia informatica è una scienza che utilizza algoritmi per criptare e decriptare dei dati, al fine di immagazzinare informazioni o trasmetterle in maniera sicura attraverso reti per loro stessa natura insicure, quali Internet. Un algoritmo crittografico è una funzione matematica che lavora in combinazione con una chiave (una parola, un numero o una frase) per criptare il testo. La sicurezza dei dati criptati dipende da due fattori: la forza dell'algoritmo crittografico e la segretezza della chiave[24].

Per ovviare a tale inconveniente, l'FBI ha sviluppato da tempo dei software detti *Key Logger System* (KLS), che, una volta installati fisicamente sul computer del sospettato, usano un dispositivo di *keystroke capture* per registrare le chiavi di accesso nel momento in cui sono digitate sul computer[25]. Non sono, però, in grado di ricercare o registrare dati salvati sul computer e nemmeno di registrare le *keystroke* mentre il modem è in azione.

---

una specifica impostazione, offriva la possibilità di selezionare e ridurre i dati che si intendeva visualizzare. Poiché Carnivore era predisposto per registrare le sole informazioni raccolte attraverso il filtro, l'ordine del giudice doveva determinare il "settaggio" di questo per meglio adattarlo alle circostanze del caso e alle esigenze normative.

[23] Con terminologia anglosassone si parla di *strong encryption*: v. SWIRE, *What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory*, cit., 11-13; M. TAMMINGA, *Cryptic secrets of public keys*, 27 *Law Practice Management* 18 (2001); J. CRIMMINS, *Wiretap report: encryption doesn't foil U.S. intercepts*, 147 *Chicago Daily L. Bulletin* 3 (2001).

[24] I software che usano la c.d. "criptazione forte" sono facilmente disponibili sul mercato a basso costo.

[25] ETZIONI, *Implications of Select New Technolgies for Individual Rights and Public Safety*, cit., 19-20.

Nel novembre del 2001, l'FBI fece sapere di aver sviluppato un tipo di tecnologia digitale meno invasiva, da un punto di vista fisico, in quanto permette di introdurre il software su di un computer senza installare fisicamente alcun dispositivo su di esso. Tale software è il c.d. *Magic Lantern*[26], un tipico *trojan*, cioè un programma che consente l'accesso al computer altrui, mediante due file, uno *client* ed uno *server*. Il file *server* è un programma eseguibile, che una volta lanciato in esecuzione si installa in maniera nascosta sul computer ed apre le porte a chiunque possegga un *client* equivalente al *server*; viene spedito attraverso Internet, per esempio via *e-mail*, e si auto-installa nel computer da sorvegliare, cominciando a registrare le chiavi digitate per poi spedire le informazioni raccolte all'FBI. Tutto ciò mentre l'ignaro utente è connesso ad Internet[27].

Sulla strada dell'implementazione di nuovi tipi di tecnologie per la sorveglianza globale, tra il 2002 ed il 2003 il DARPA (*Defense Advanced Research Projects Agency*) era stato incaricato di sviluppare un software, chiamato "*Total Information Awareness*" (TIA) in grado di offrire alle agenzie di investigazione impegnate nella lotta al terrorismo la possibilità di comparare ed esaminare praticamente la totalità dei database[28]. Lo strumento in parola non

[26] Si v. C. WOO, M. SO, *The Case for Magic Lantern: September 11 highlights the need for increased surveillance*, 15 *Harv. J.L. & Tech.* 497, 521 (2002); N. HARTZOG, *The "magic lantern" revealed: a report of the FBI's new "key logging" Trojan and analysis of its possible treatment in a dynamic legal landscape*, 20 *J. Marshall J. Computer & Info. L.* 287 (2002).

[27] Il tipo di informazioni che un tale programma è in grado di raccogliere lo distingue dagli altri tipi di sorveglianza: i *keystroke logger*, registrando le chiavi d'accesso non appena digitate sul computer, sono un ottimo strumento per le agenzie di investigazione governative per decriptare i sistemi di "criptazione forte" utilizzati dai criminali e dai terroristi per nascondere le loro informazioni.

[28] J. MARCKOFF, *Surveillance capability now widely dispersed: experts. (Defense Advanced Research Projects Agency's Infomation Awareness Office's Total Information Awareness project)*, 149 *Chi. Daily Law Bulletin* 1 (2003); *Total*

sarebbe stato dotato di un suo specifico archivio, bensì strutturato in maniera tale da riconoscere i formati di tutti i database delle agenzie governative e di tradurre le ricerche grazie ad una interfaccia software. Pochi strumenti come il *Total Information Awaraness*, poi ribattezzato "*Terrorism Information Awareness*", hanno suscitato tante polemiche. Il TIA, infatti, era un progetto pensato per far parlare tra loro database spionistici, militari, amministrativi e commerciali al fine di poter ottenere un'informazione il più possibile dettagliata e completa. Una legge di spesa approvata dalla Camera dei Rappresentanti di Washington ha negato, però, ogni forma di finanziamento al TIA, decretando così l'impossibilità per la creatura dell'ammiraglio John Pointdexter di muovere anche solo i primi passi[29].

Per non parlare poi di *Echelon*[30]. Progettato e amministrato dalla *National Security Agency* (NSA), il sistema *Echelon* è utilizzato per intercettare normali *e-mail*, fax, telex e telefonate che viaggiano nella rete di telecomunicazione mondiale. Diversamente dalla maggior parte dei sistemi di spionaggio sviluppati durante la "guerra fredda", la tecnologia in questione è progettata principalmente per

---

"Terrorism" Information Awareness (TIA), reperibile sul sito Web http://www.epic.org

[29] In Olanda è di imminente creazione un archivio informatico che conterrà informazioni relative ai nascituri i quali, a partire dal 2007, riceveranno un identificativo numerico e rimarranno schedati per tutta la loro vita con costanti aggiornamenti. Cfr. *Olanda, i neonati in un database*, reperibile sul sito Web http://punto-informatico.it

[30] Cfr. A. ROSSATO, *Diritto e architettura nello spazio digitale. Il ruolo del software libero*, Padova, 2006, 56-58; E.L. BROW, *ECHELON: the National Security Agency's compliance with applicable legal guidelines in light of the need for tighter national security*, 11 *CommLaw Conspectus* 185 (2003); K.J. LAWNER, *Post-Sept. 11th international surveillance activity - a failure of intelligence: the Echelon interception system & the fundamental right to privacy in Europe*, 14 *Pace Int. L. Rev.* 435 (2002); M.L. HANIES, *The secret life of Echelon (national security spy system)*, 160 *New Jersey L. J.* 27 (2000).

obiettivi non militari (governi, organizzazioni, aziende, gruppi, ed individui praticamente in ogni parte del mondo). Potenzialmente sono sottoposte a sorveglianza tutte le comunicazioni tra le persone, tra uno Stato e l'altro (ma anche all'interno dello stesso Stato), ovunque nel mondo. Non è certo una novità che le agenzie di intelligence sorveglino le *e-mail* e gli altri mezzi di comunicazione. *Echelon* non è stato realizzato per spiare una particolare *e-mail* o una specifica utenza fax. Al contrario il sistema lavora indiscriminatamente intercettando grandissime quantità di comunicazioni per estrarne i messaggi di potenziale interesse. Al fine di monitorare la rete di telecomunicazione globale è stata organizzata una catena di strutture di intercettazione che attraversano l'intero globo. Alcune di queste controllano i satelliti di comunicazione, altre i *network* a terra ed altre le comunicazioni radio. *Echelon* lega insieme tutte queste strutture a beneficio degli Stati Uniti e di alcuni suoi alleati. Computer posti in ogni stazione del sistema *Echelon* cercano, tra i milioni di messaggi intercettati, quelli contenenti le *keyword*, le parole chiave, precedentemente inserite. Le *keyword* includono tutti i nomi, le località, i soggetti contenuti nei messaggi "interessanti". Ogni parola dei messaggi intercettati viene scansionata automaticamente sia che il telefono, la *e-mail* o il fax siano nella lista di quelli "da controllare", sia che provengano da qualsiasi altra utenza. Le migliaia di messaggi vengono letti simultaneamente nel momento in cui giungono alle stazioni.

Da ultimo il c.d. *Face Recognition system*, basato sulla possibilità di collocare una serie di *smart camera* aventi la capacità di confrontare "in tempo reale" le immagini delle persone riprese in ambienti pubblici o privati con database di immagini facciali pre-registrate[31].

[31] L'implementazione di questo sistema di sorveglianza potrebbe vedere utilizzato in un prossimo futuro un agente software magari in stretto contatto ed

Si intende, ora, valutare l'interazione tra l'utilizzazione di questi software nella sicurezza informatica e il contesto giuridico americano.

Preliminare è l'analisi del IV Emendamento della Costituzione americana: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probabile cause…"[32]. Fin dall'invenzione del telefono, la giurisprudenza e la dottrina hanno sempre cercato di determinare l'esatta interpretazione di un documento adottato originariamente con riferimento agli strumenti di investigazione propri del diciottesimo secolo. Per molti anni la Corte Suprema degli Stati Uniti ha utilizzato la citata disposizione costituzionale per decidere con quali modalità gli strumenti governativi potessero essere impiegati per contrastare la criminalità o semplicemente per far applicare la legge in maniera più efficace. Anche se la *ratio* potrebbe apparire a prima vista ispirata alla tutela della privacy, il IV Emendamento trova la sua motivazione principalmente nella tutela del potere: esso è meglio compreso se considerato come uno strumento per

---

interconnessione con altri sistemi di intercettazione telematica ed ambientale; tutto ciò richiama la possibilità di realizzare un c.d. *Active Enviroment*, cioè l'interconnessione di strumenti elettronici presenti in un determinato luogo attraverso programmi ad agenti software, capaci di interagire tra loro scambiandosi informazioni e di condizionare, tramite un *composer*, il contesto reale. Per approfondimenti su questa nuova tecnologia, v. M. ROTENMBERG, *Privacy and Security After September 11*, 77 *Minn. L. Rev.* 1115, 1121-1122 (2002); R.J. O'HARROW, *Facial Recognition System Considered for U.S. Airports*, *Wash. Post*, Sept. 23, 2001, A14; K. ALEXANDER, *Airport to Get Facial Recognition Technology Oakland*, *Los Angeles. Times*, Oct. 29, 2001, B1; *The Many Faces of Viisage*, in http://www.notbored.org/viisage.html; P.E. AGRE, *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*, reperibile sul sito Web http://dlis.gseis.ucla.edu/people/pagre/bar-code.html

[32] Cfr. O.S. KERR, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 *Mich. L. Rev.* 801 (2004).

preservare la potestà del popolo sul governo e garantire alla sovranità popolare la possibilità di determinare come il governo possa introdursi nella vita dei cittadini ed influenzarne il comportamento. Il IV Emendamento finisce così col garantire una protezione più vasta rispetto alla semplice riservatezza: esso assicura che le intrusioni nella sfera personale dei singoli siano basate su regole stabilite dai cittadini, che devono essere rispettate per effettua legittimamente l'attività di sorveglianza.

Nel decidere quando sia applicabile il IV Emendamento, la Corte Suprema richiede che si stabilisca preliminarmente se l'attività del governo sia da considerarsi un "search" secondo la Costituzione. Per lo più, questa ricerca è volta a determinare se l'atto posto in essere dall'autorità governativa sia equivalente al tipo di indagini che i padri fondatori della nazione avevano considerato foriero di problemi. Se l'attività è ritenuta similare è considerata un "search" e la Costituzione ne limiterebbe il potere imponendo una autorizzazione supportata da una "probable cause". Se l'attività, invece, non è ritenuta essere similare gli agenti governativi saranno liberi di intraprendere la loro attività di investigazione senza dover sottostare ad alcun vincolo. Con riferimento alle nuove tecnologie di intercettazione telematica ed ambientale, questa interpretazione consente che il loro utilizzo non sia disciplinato dalle previsioni costituzionali in quanto, secondo un'interpretazione rigidamente letterale, la Corte non le considera "search" ai sensi del IV Emendamento[33].

[33] M. GUTTERMAN, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 *Syracuse L. Rev.* 647 (1988), dove l'autore sostiene che "this approach fails to protect privacy rights, and permits their gradual decay with each improved technological advance"; v. anche D.E. STEINBERG, *Making Sense of Sense-Enhanced Searches*, 74 *Minn. L. Rev.* 563 (1990).

In un recente caso, *Kyllo v. United States*[34], la Corte Suprema ha compiuto un primo passo verso un'interpretazione non basata sulla riservatezza. Nel decidere che l'utilizzo da parte degli agenti governativi di apparecchiature per il rilevamento termico senza una specifica autorizzazione sono da considerarsi illegali, il giudice Scalia ha concluso affermando che se una tecnologia è da considerarsi "not in general public use", la Corte dovrebbe "assure preservation of the degree of privacy against government that existed when the Fourth Amendment was adopted"[35]. In altre parole, piuttosto che chiedersi se i primi estensori della Carta costituzionale avessero considerato l'azione in questione un "search", la Corte dovrebbe verificare se essi avrebbero approvato tale livello di intrusività ai fini di garantire la sicurezza. La decisione in oggetto ha le potenzialità di far ritornare il Quarto Emendamento al suo ruolo originario, in modo da assoggettare tutte le attività investigative effettuate con l'ausilio delle nuove tecnologie alle limitazioni che esso prevede[36].

4. "Pacchetto sicurezza" Pisanu, diritti civili e data retention

Il c.d. "pacchetto sicurezza" del Ministro dell'Interno Pisanu, emanato sull'onda emotiva dell'attentato terroristico alla

[34] 533 U.S. 27 (2001).

[35] 533 U.S. 34 (2001).

[36] Il caso Kyllo suggerisce che l'utilizzo da parte delle agenzie governative delle nuove tecnologie dovrebbe sempre essere soggetto al necessario e preventivo ottenimento di una autorizzazione anche se si trattasse di strumenti di pubblico utilizzo. Una tale interpretazione significherebbe muoversi verso la riconciliazione del IV Emendamento con la dottrina della separazione dei poteri onde riconoscere nuovamente nel popolo l'autorità sovrana nel compito di fare le leggi, al di là dell'appropriato livello di riservatezza e sicurezza. Cfr. C. SLOBOGIN, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance*, 86 *Minn. L. Rev.* 1393 (2002); S. BANDES, *Power, Privacy and Thermal Imaging*, 86 *Minn. L. Rev.* 1384 (2002). Per approfondimenti si rimanda a GUARDA, *Agenti software e sicurezza informatica*, cit., 327-334.

metropolitana di Londra, si compone di due interventi normativi: il decreto legge 27 luglio 2005, n. 144 (modificato con la legge di conversione 31 luglio 2005, n. 155) ed il decreto del Ministro dell'Interno 16 agosto 2005 (come precisato dalla circolare del Ministero dell'interno n. 557/2005)[37].

La disciplina ruota attorno a due punti fondamentali: da un lato, l'imposizione dell'obbligo di conservazione dei dati di traffico "circostanziali" e, dall'altro, l'estensione di obblighi e controlli di "polizia amministrativa" anche alle associazioni e ai comitati – fenomeni associativi impropriamente definiti "circoli privati" – in modo da rendere praticamente applicabile l'obbligo di licenza anche ai singoli cittadini.

Partendo da quest'ulto punto, l'art. 7, comma 1, del d.l. in parola, così come convertito dalla legge n. 155 del 2005, si applica in maniera inequivocabile agli esercenti attività commerciali nel settore delle telecomunicazioni (vedi: Internet *point*, *call center*, Internet caffé): questi soggetti sono da intendersi destinatari dell'obbligo di conservazione e di messa a disposizione dei dati di traffico.

I problemi sorgono con l'estensione degli obblighi ai "circoli privati di qualsiasi specie". Il codice civile individua agli articoli da 36 a 42 le associazioni non riconosciute e comitati, che pur non avendo personalità giuridica sono comunque, seppur con limitazioni, soggetti di diritto. Dove il decreto Pisanu si riferisce ai "circoli privati" si dovrebbe intendere, più correttamente, "associazioni non riconosciute" o "comitati". Tale lettura, però, è portatrice di infauste conseguenze. Un'associazione non riconosciuta nasce senza bisogno di particolari formalità, per il solo fatto che due o più persone decidono di operare per il raggiungimento di un obiettivo comune.

[37] Cfr. M. CAMMARATA, *Libertà e sicurezza: un binomio impossibile?*, reperibile sul sito Web http://www.interlex.it; ID., *Anti-terrorismo: troppi problemi per norme confuse e inutili*, *ibidem*.

Ne deriva che qualsiasi tipo di associazione non riconosciuta – anche quelle parrocchiali o sportive – che, per qualsiasi ragione, consentissero ai propri aderenti l'uso di un computer collegato ad Internet, dovrebbero chiedere la licenza al questore e permettere che, anche senza mandato del magistrato, l'accesso della polizia al domicilio privato adibito a "sede", per eseguire "controlli amministrativi".

Siamo evidentemente di fronte ad una grave limitazione della libertà di associazione, che non rispetta il principio della inviolabilità del domicilio. Il decreto Pisanu non collega la licenza di polizia – come nel caso della licenza amministrativa per la somministrazione di alimenti e bevande nei "circoli privati" – al particolare scopo associativo ed alla modalità con le quali esso viene perseguito, ma limita indiscriminatamente la libertà di qualsiasi cittadino associato che si collega ad Internet, tanto da porre in essere un'attività di controllo della società civile particolarmente invasiva e pericolosa.

Veniamo ora alla questione *data retention*. Anche qui le norme lasciano spazio a interpretazioni differenti rispetto alla tipologia dei dati da conservare e ai servizi di cui si dovrebbero conservare le attività.

Innanzitutto occorre sottolineare che la *data retention* rappresenta una soluzione poco efficiente per le indagini, in quanto trasmette agli investigatori una falsa sensazione di sicurezza e non consente di rintracciare proprio quei soggetti criminali più pericolosi, particolarmente motivati e tecnicamente preparati.

Nonostante si sostenga che l'obbligo di conservazione dei dati si applichi estensivamente a qualsiasi "servizio di comunicazione elettronica", in realtà questo non accade. È infatti possibile affermare che i "dati circostanziali" da conservare obbligatoriamente sono soltanto quelli relativi ai servizi di comunicazione (*e-mail*, *chat*, *instant messaging*), mentre restano

fuori dalla *retention* quelli relativi alla consultazione passiva di risorse (navigazione e lettura di newsgroup) o di pubblicazione di contenuti (ftp).

Si giunge a questa conclusione considerando che l'art. 6 del d.l. n. 144/2005 impone la *data retention* per i "dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi". Questa interpretazione è confermata dal successivo decreto ministeriale 16 agosto 2005, il cui art. 1 afferma chiaramente che gli obblighi valgono per "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". Ribadisce il concetto l'art. 2 del decreto (monitoraggio delle attività), che fa nuovamente riferimento alla "comunicazione" come oggetto degli obblighi di *retention*. Si legge infatti nella norma: "I soggetti di cui all'art. 1 adottano le misure necessarie a memorizzare e mantenere i dati relativi alla data ed ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato dall'utente, esclusi comunque i contenuti delle comunicazioni". Lo stesso articolo, poi, recepisce la necessità di conservare i dati garantendone la non alterabilità e la non accessibilità a terzi non autorizzati. Ben difficilmente, quindi, i dati circostanziali di traffico potranno avere valore probatorio se non saranno conservati seguendo almeno le minime indicazioni del decreto ministeriale.

Anche in ambito comunitario la questione *data retention* ha incontrato notevole interesse. La Commissione europea ha infatti più volte cercato di far passare una proposta di direttiva in cui si prevedeva la conservazione fino a sei mesi dei dati relativi al traffico

e fino ad un anno per quelli pubblici[38].

Dopo lunghi ed accesi dibattiti sul tema, il Consiglio dei Ministri europei della Giustizia decise di dare finalmente il via ad una direttiva che, negli intenti dei promotori, fosse condivisa ed accettata e la sottopose all'approvazione del Parlamento europeo, il quale da sempre aveva manifestato contrarietà soprattutto sulla possibilità di conservare i dati per più di un anno. La direttiva del Parlamento europeo e del Consiglio 2006/24/CE del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, è stata, così, approvata in prima lettura. Essa prevede l'obbligo per gli operatori telefonici e gli Internet *provider* di conservare i dati di ogni comunicazione telefonica e collegamento *on-line* per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione. Le informazioni da conservare sono quelle necessarie per rintracciare ed identificare la fonte e la destinazione di una comunicazione, per determinare la data, l'ora e la durata di una comunicazione, nonché il tipo e le attrezzature di comunicazione utilizzate dagli utenti, per rintracciare infine l'ubicazione delle apparecchiature di comunicazione mobile. È, comunque, assolutamente vietata la conservazione dei contenuti delle comunicazioni.

Molteplici sono gli aspetti di criticità che la nuova direttiva presenta. Innanzitutto, i costi dell'operazione ricadono interamente sugli operatori telefonici ed Internet (e, quindi, di rimando sugli utenti): non è, infatti, prevista alcuna forma di rimborso per le spese

[38] Al contrario di quanto accaduto in alcuni paesi europei dove simili misure sono state adottate, la proposta prevedeva anche una forma di compensazione per operatori e *provider* che devono sobbarcarsi gli oneri della conservazione dei dati. Cfr. *La Commissione UE adotta la Data Retention*, disponibile sul sito Web http//www.punto-informatico.it

sostenute per la *data retention*. Inoltre, dubbi vengono sollevati anche sulle finalità per le quali sarà possibile consultare i dati conservati: inizialmente pensata per contrastare il terrorismo internazionale e la criminalità organizzata, la direttiva è stata poi, invece, estesa a tutti i tipi di reati che si possono commettere. Tutto questo, a detta dei contestatori della nuova normativa, potrebbe avere come unico effetto quello di mettere a rischio i diritti individuali e la privacy degli utenti-cittadini, risultando sostanzialmente inutile ai fini di sicurezza[39].

La direttiva trova chiaramente origine nel clima di incertezza successivo agli attentati di Londra ed in essa hanno prevalso le ragioni di "sicurezza ad ogni costo". La questione non appare però chiusa in quanto lo scetticismo dei Garanti della privacy ed i molti comitati "anti-data retention" sorti potrebbero indurre a modificare la normativa appena adottata. In Italia, in attesa del recepimento della direttiva, si continua ad applicare la citata legge Pisanu, la quale già impone la conservazione dei dati telefonici e di connessione ad Internet fino al 31 dicembre 2007, con modalità assai più stringenti, ed a tratti meno chiare, di quelle proposte in sede europea.

5. Conclusioni: società, regole giuridiche e tecnologia

L'attenzione dei governi mondiali sul tema della sicurezza informatica è in costante crescita, con la conseguenza che è notizia ormai di ogni giorno l'adozione di leggi nuove e sempre più invasive per la privacy degli individui.

Il cittadino si sente sempre più controllato e la sua insicurezza cresce all'interno di un mondo, reale e digitale, nel quale le insidie si moltiplicano in modo esponenziale.

[39] Gli stessi Garanti della Privacy europei hanno più volte ribadito che la *data retention* andrebbe equiparata all'intercettazione vera e propria e quindi adottata solo in misure eccezionali.

La Rete stessa cresce e si evolve continuamente. Le nostre abitudini, il nostro sistema di vita, le nostre stesse esistenze sono costantemente modificate e, spesso, "alterate". Nella Rete si proiettano e si amplificano tutte le paure, tutti i problemi, tutte le insicurezze individuali e sociali. Il fatto però che questi stati d'animo siano condivisi da un numero indefinito di persone rende la percezione dell'insicurezza un fenomeno globale. Questa globalizzazione può rappresentare al tempo stesso una soluzione al problema. Diviene sempre più centrale la "comunità" che coinvolge sia soggetti istituzionali ed economici che milioni di utenti, connessi ad Internet dai più disparati angoli del mondo. Una rete ed una comunità globali non inducono all'omologazione, bensì alla ricerca di soluzioni diverse: nuove sono le opportunità di conoscenza e di sviluppo relazionale in ogni ambito del vivere umano.

L'individuo assume un ruolo fondamentale all'interno di questa comunità[40]. È lui il protagonista: l'implementazione di nuove tecnologie per l'autodifesa, come la criptazione, i filtri anti-spam che utilizzano sistemi di filtraggio a base statistica (cioè i filtri c.d. bayesiani)[41], le piattaforme digitali che consentono un efficace controllo dei propri dati personali – *Platform for Privacy Preferences* (P3P)[42] –, spostano l'attenzione sui singoli utenti della rete che non devono perdere la consapevolezza di essere essi stessi fautori e

[40] In tale ambito diventa fondamentale il ruolo dei c.d. codici di condotta i quali costituiscono un momento di aggregazione della categoria interessata e di confronto con le altre categorie, con la previsione di risposte pragmatiche ai rischi ed alla insicurezza che questi codici determinano; v. PASCUZZI, *Il diritto dell'era digitale*, cit., 57-60.

[41] Cfr. D. MCCULLAGH, *Technology and Security*, 25 *Harv. J. Law & Pub. Pol'y* 129 (2001).

[42] Cfr. W. MCGEVERAN, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 *N.Y.U.L.Rev.* 1812 (2001).

creatori del mondo digitale[43].

In un'epoca caratterizzata dall'insicurezza ed a tratti dalla sfiducia, è necessario continuare a credere nel valore più importante della nostra civiltà, la libertà. "La libertà ha bisogno di sicurezza. La libertà è sempre libertà da qualcosa. Libertà significa assenza di asservimento, di coazione e di tutela, di paura e di violenza. La si difende avversando le prepotenze, ponendo limiti alle intromissioni altrui e proteggendosi dai pericoli"[44].

[43] Forse verrà un giorno in cui "non ci sarà più bisogno di computer "giganteschi" e di "linee" telefoniche. I dispositivi di elaborazione saranno inseriti nel corpo umano, controllati da chiavi e codici biometrici, l'accesso all'informazione sarà diretto e immediato, continuo, senza necessità di "copia", perché copia sarà onnipresente nella mente, quando la si evoca. Chi scrive musica lo farà come fecero gli antenati, per le sale di teatro; e così faranno i produttori di film. Se cercano notorietà senza compenso metteranno le loro opere […] in pubblico dominio […]. Tutti potranno attingere senza diventare pirati. Perché il pensiero che raccoglie e fruisce informazione non può mai essere pirata": in PALMIERI, *Sicurezza o libertà? Introduzione al diritto di Internet*, cit., 289.

[44] SOFSKY, *Rischio e sicurezza*, cit., 147. Troviamo un'altra significativa riflessione in PALMIERI, *Sicurezza o libertà? Introduzione al diritto di Internet*, cit., 279-280: "la libertà ha sempre avuto i suoi nemici – e continuamente ne acquista di nuovi. Questi, anche se sono in talune aree sulla difensiva, sono agguerriti e ben lontani dalla resa. È dovere di tutti coloro che dei benefici della libertà godono, da sempre o da poco, di fare quanto è pacificamente possibile perché siano ridotti e progressivamente eliminati gli ostacoli al suo pieno godimento. Questo vale per Internet allo stesso modo come per qualunque altra area dell'informazione e della comunicazione. La Rete deve essere difesa dall'attentato alla sua libertà. Occorre difendere la libertà ad ogni costo. Non è una difesa che possa essere delegata: tutti sono responsabili e coinvolti, come individui e come collettività".

QUADERNI PUBBLICATI NELLA COLLANA DEL DIPARTIMENTO DI SCIENZE GIURIDICHE

1. *Legal Scholarship in Africa* - MARCO GUADAGNI (1989)

2. *L'insegnamento della religione nel Trentino-Alto Adige* - ERMINIA CAMASSA AUREA (1990)

3. *Il nuovo processo penale. Seminari* - MARTA BARGIS (1990)

4. *Proprietà-garanzia e contratto. Formule e regole nel leasing finanziario* - MAURO BUSSANI (1992)

5. *Fonti e modelli nel diritto dell'Europa orientale* - GIANMARIA AJANI (1993)

6. *Il giudizio di "congruità" del rapporto di cambio nella fusione* - LUIGI ARTURO BIANCHI (1993)

7. *Interessi pubblici e situazioni soggettive nella disciplina della concorrenza del mercato* - FRANCO PELLIZZER (1993)

8. *La legge controllata. Contributo allo studio del procedimento di controllo preventivo delle leggi regionali* - EMANUELE ROSSI (1993)

9. *L'oggetto del giudizio sui conflitti di attribuzione tra i poteri dello Stato. Fonti normative. Strumenti e tecniche di giudizio della Corte Costituzionale* - DAMIANO FLORENZANO (1994)

10. *Dall'organizzazione allo sviluppo* - SILVIO GOGLIO (1994)

11. *Diritto alla riservatezza e trattamenti sanitari obbligatori: un'indagine comparata* - CARLO CASONATO (1995)

12. *Lezioni di diritto del lavoro tedesco* - ULRICH ZACHERT (1995)

13. *Diritti nell'interesse altrui. Undisclosed agency e trust nell'esperienza giuridica inglese* - MICHELE GRAZIADEI (1995)

14. *La struttura istituzionale del nuovo diritto comune europeo: competizione e circolazione dei modelli giuridici* - LUISA ANTONIOLLI DEFLORIAN (1996)

15. *L'eccezione di illegittimità del provvedimento amministrativo. Un'indagine comparata* - BARBARA MARCHETTI (1996)

16. *Le pari opportunità nella rappresentanza politica e nell'accesso al lavoro. I sistemi di "quote" al vaglio di legittimità* - (a cura di) STEFANIA SCARPONI (1997)

17. *I requisiti delle società abilitate alla revisione legale* - EMANUELE CUSA (1997)

18. *Germania ed Austria: modelli federali e bicamerali a confronto* - FRANCESCO PALERMO (1997)

19. *Minoranze etniche e rappresentanza politica: i modelli statunitense e canadese* - CARLO CASONATO (1998)

20. *Scritti inediti di procedura penale* - NOVELLA GALANTINI e FRANCESCA RUGGIERI (1998)

21. *Il dovere di informazione. Saggio di diritto comparato* - ALBERTO M. MUSY (1999)

22. *L'*Anti-Rousseau *di Filippo Maria Renazzi (1745-1808)* - BEATRICE MASCHIETTO (1999)

23. *Rethinking Water Law. The Italian Case for a Water Code* - NICOLA LUGARESI (2000)

24. *Making European Law. Essays on the 'Common Core' Project* - MAURO BUSSANI e UGO MATTEI (2000)

25. *Considerazioni in tema di tutela cautelare in materia tributaria* - ALESSANDRA MAGLIARO (2000)

26. *Rudolf B. Schlesinger – Memories* - UGO MATTEI e ANDREA PRADI (2000)

27. *Ordinamento processuale amministrativo tedesco (VwGO)* – Versione italiana con testo a fronte - GIANDOMENICO FALCON e CRISTINA FRAENKEL (cur.) (2000)

28. *La responsabilità civile. Percorsi giurisprudenziali* (Opera ipertestuale. Libro + Cd-Rom) - GIOVANNI PASCUZZI (2001)

29. *La tutela dell'interesse al provvedimento* - GIANDOMENICO FALCON (2001)

30. *L'accesso amministrativo e la tutela della riservatezza* - ANNA SIMONATI (2002)

31. *La pianificazione urbanistica di attuazione: dal piano particolareggiato ai piani operativi* - (a cura di) DARIA DE PRETIS (2002)

32. *Storia, istituzione e diritto in Carlo Antonio de Martini (1726-1800). 2° Colloquio europeo Martini, Trento 18-19 ottobre 2000, Università degli Studi di Trento* - (a cura di) HEINZ BARTA, GÜNTHER PALLAVER, GIOVANNI ROSSI, GIAMPAOLO ZUCCHINI (2002)

33. *Giustino D'Orazio. Antologia di saggi. Contiene l'inedito "Poteri prorogati delle camere e stato di guerra"* - (a cura di) DAMIANO FLORENZANO e ROBERTO D'ORAZIO (2002)

34. *Il principio dell'apparenza giuridica* - ELEONORA RAJNERI (2002)

35. *La testimonianza* de relato *nel processo penale. Un'indagine comparata* - GABRIELLA DI PAOLO (2002)

36. *Funzione della pena e terzietà del giudice nel confronto fra teoria e prassi. Atti della Giornata di studio - Trento, 22 giugno 2000* - (a cura di) MAURIZIO MANZIN (2002)

37. *Ricordi Politici. Le «Proposizioni civili» di Cesare Speciano e il pensiero politico del XVI secolo* - PAOLO CARTA (2003)

38. *Giustizia civile e diritto di cronaca. Atti del seminario di studio tenuto presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento, 7 marzo 2003* - (a cura di) GIOVANNI PASCUZZI (2003)

39. *La glossa ordinaria al Decreto di Graziano e la glossa di Accursio al Codice di Giustiniano: una ricerca sullo* status *giuridico degli eretici* - RUGGERO MACERATINI (2003)

40. *La disciplina amministrativa e penale degli interventi edilizi. Un bilancio della normativa trentina alla luce del nuovo testo unico sull'edilizia. Atti del Convegno tenuto nella Facoltà di*

Giurisprudenza di Trento l'8 maggio 2003 - (a cura di) DARIA DE PRETIS e ALESSANDRO MELCHIONDA (2003)

41. *The Protection of Fundamental Rights in Europe: Lessons from Canada* - CARLO CASONATO (ED.) (2004)

42. *Un diritto* per *la scuola. Atti del Convegno* "Questioni giuridiche ed organizzative per la riforma della scuola". Giornata di Studio in onore di Umberto Pototschnig (Trento, 14 maggio 2003). *In appendice: U. Pototschnig, SCRITTI VARI (1967-1991)* - (a cura di) DONATA BORGONOVO RE e FULVIO CORTESE (2004)

43. *Giurisdizione sul silenzio e discrezionalità amministrativa. Germania - Austria - Italia* - CRISTINA FRAENKEL-HAEBERLE (2004)

44. *Il processo di costituzionalizzazione dell'Unione europea. Saggi su valori e prescrittività dell'integrazione costituzionale sovranazionale* - (a cura di) ROBERTO TONIATTI e FRANCESCO PALERMO (2004)

45. *Nuovi poteri del giudice amministrativo e rimedi alternativi al processo. L'esperienza francese* - ANNA SIMONATI (2004)

46. *Profitto illecito e risarcimento del danno* - PAOLO PARDOLESI (2005)

47. *La procreazione medicalmente assistita: ombre e luci* - (a cura di) ERMINIA CAMASSA e CARLO CASONATO (2005)

48. *La clausola generale dell'art. 100 c.p.c. Origini, metamorfosi e nuovi ruoli* - MARINO MARINELLI (2005)

49. *Diritto di cronaca e tutela dell'onore. La riforma della disciplina sulla diffamazione a mezzo stampa. Atti del convegno tenuto presso la Facoltà di Giurisprudenza dell'Università di Trento il 18 marzo 2005* - (a cura di) ALESSANDRO MELCHIONDA e GIOVANNI PASCUZZI (2005)

50. *L'Italia al Palazzo di Vetro. Aspetti dell'azione diplomatica e della presenza italiana all'ONU* - (a cura di) STEFANO BALDI e GIUSEPPE NESI (2005)

51. *Appalti pubblici e servizi di interesse generale. Atti dei seminari tenuti presso la Facoltà di Giurisprudenza di Trento. Novembre - Dicembre 2004* - (a cura di) GIAN ANTONIO BENACCHIO e DARIA DE PRETIS (2005)

52. *Il termalismo terapeutico nell'Unione europea tra servizi sanitari nazionali e politiche del turismo* - ALCESTE SANTUARI (2006)

53. *La gestione delle farmacie comunali: modelli e problemi giuridici* - (a cura di) DARIA DE PRETIS (2006)

54. *Guida alla ricerca ed alla lettura delle decisioni delle corti statunitensi* - (a cura di) ROBERTO CASO (2006)

55. *Dialoghi sul danno alla persona.* Saggi raccolti nell'ambito della seconda edizione dei "Dialoghi di diritto civile" tenutisi presso il Dipartimento di Scienze Giuridiche dell'Università di Trento (a.a. 2004-2005) - (a cura di) UMBERTO IZZO (2006)

56. *Il diritto degli OGM tra possibilità e scelta.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento. 26 novembre 2004 - (a cura di) CARLO CASONATO e MARCO BERTI (2006)

57. *Introduzione al biodiritto. La bioetica nel diritto costituzionale comparato* - CARLO CASONATO (2006)

58. *La famiglia senza frontiere.* Atti del convegno tenuto presso la Facoltà di Giurisprudenza dell'Università di Trento il 1° ottobre 2005 - (a cura di) GIOVANNI PASCUZZI (2006)

59. *Sicurezza informatica: regole e prassi.* Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005 - (a cura di) ROBERTO CASO (2006)

COUPON D'ORDINE COLLANA "QUADERNI DEL DIPARTIMENTO DI SCIENZE GIURIDICHE DELL'UNIVERSITÀ DI TRENTO"

Compilare ed inviare al Dipartimento di Scienze Giuridiche, Università degli Studi di Trento, via posta (Via Verdi 53 – 38100 Trento – Italia) o via fax (+ 39 0461 881874).

Dati per la spedizione:

Cognome e nome
o Ragione sociale .....

Indirizzo .....

Città e C.A.P. .....

Telefono .....

E-mail .....

Barrare la casella qui a fianco se si desidera ricevere la fattura. ☐

Codice fiscale / Partita IVA .....

N. copie	Titolo	Autore

Accetto la forma di pagamento a mezzo contrassegno postale con l'addebito delle spese di spedizione correnti per ordini di importo inferiore a euro 25,00.

Informativa resa ai sensi dell'art. 13 del d.lgs. n. 196/2003
- Codice in materia di protezione dei dati personali -

Il trattamento dei dati personali viene svolto nell'ambito del Dipartimento di Scienze Giuridiche dell'Università degli Studi di Trento, nel rispetto di quanto stabilito dal d.lgs. 30 giugno 2003, n. 196 e dalle norme regolamentari della medesima Università. Il "titolare" del loro trattamento è l'Università di Trento. I dati personali sono trattati esclusivamente per fini istituzionali, con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003). Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento. Le richieste vanno rivolte al Dipartimento di Scienze Giuridiche. Nessun dato personale viene comunicato o diffuso. Il presente modulo integra una richiesta di invio di materiale informativo. I dati personali forniti mediante il medesimo modulo sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia a tal fine necessario.

Data: ..... Firma leggibile: .....