PROFILI GIURIDICI DELLA SICUREZZA INFORMATICA

di Paolo Guarda

L'importanza che la protezione dei dati personali ha acquisito nell'ambito della società dell'informazione porta alla necessità di garantire la sicurezza del contesto digitale all'interno del quale tali dati vengono trattati. Da questa prospettiva la sicurezza informatica costituisce l'ultimo approdo del cammino percorso dalla tutela della *privacy* nell'arco di più di un secolo, e ne rappresenta un elemento fondamentale: si pensi alla complessa disciplina delle misure di sicurezza contenuta nel Codice sulla protezione dei dati personali ed alla regolamentazione dei relativi standard. Il termine sicurezza si connota di diverse accezioni dai significati ambigui e non sempre sovrapponibili. Non è neppure spesso così chiaro a giovamento di chi tale sicurezza venga perseguita e quale sia il giusto approccio per raggiungerla, se mediante un controllo ed un'applicazione preventiva o tramite un sistema di verifica e soluzione *ex post*. Il contributo cercherà di fornire indicazioni utili a risolvere questi interrogativi.

The gain in importance of personal data protection in the Information Society leads to the need to ensure the security of the digital environment in which these data are processed. From this point of view, security is the last step of privacy evolution over more than a century, and represents a key element: a paradigmatic example of that is the complex discipline of the security measures contained in the Italian Data Protection Code and the regulation of relating standards. The term security is characterized by different, ambiguous, and not always overlapping, meanings. It is not even clear those for which security is pursued and what is the right approach to reach it, whether through monitoring and preventive enforcement or through a system of ex post verification and resolution. The paper will try to provide guidance to solve these questions.

———

1. PREMESSA: SICUREZZA E SUOI SIGNIFICATI

L'importanza che la protezione dei dati personali ha acquisito nell'ambito della società dell'informazione porta alla necessità di garantire la sicurezza del contesto digitale all'interno del quale tali dati vengono trattati. La capillare diffusione dei personal computer nel tessuto sociale e la creazione di banche dati sempre più efficienti nell'attività di aggregazione di informazioni e della loro elaborazio-

ne hanno determinato un bisogno di sicurezza che talvolta trascende in veri e propri stati d'*ansia* [1]. Il mutamento tecnologico provoca cambiamenti economici e trasformazioni nelle istituzioni sociali. Allo stesso tempo, i cambiamenti sociali e culturali modificano i contesti digitali: la fiducia o la diffidenza nei confronti del nuovo mondo globalizzato sono in grado di condizionare l'evoluzione dell'ambiente telematico [2].

Con il termine *sicurezza* si può, in prima battuta, 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 essere affrontata su diversi piani: quello sociale, economico, informatico e giuridico [3].

Da un punto di vista sociale, osserviamo l'interazione tra due livelli di comportamento: su un primo livello, troviamo gli scambi che si realizzano tra le conseguenze positive che una specifica azione determina e il favorevole giudizio che a esse si associa; su un secondo livello, invece, abbiamo l'integrazione tra soggetti, norme condivise dalla comunità e valori comuni. La definizione del termine *sicurezza* deve coinvolgere l'analisi della sua percezione a entrambi questi livelli [4]. Allorché si avverte il problema *sicurezza*, s'impone subito l'esigenza di un intervento pubblico di regolazione e

[1] Cfr. G. Pascuzzi, *Il diritto dell'era digitale*, Il Mulino, Bologna 20103, pp. 59-65.

[2] In N. Negroponte, *Essere digitali*, Sperling & Kupfer, Milano 1995, p. 241 si legge: *La facilità di accesso alle informazioni, la modalità e la possibilità di indurre cambiamenti è ciò che renderà il futuro tanto diverso dal presente*. Per uno studio sulle diversità d'approccio tra Unione Europea e Stati Uniti d'America ai problemi relativi alla globalizzazione di Internet, J.S. Bauchner, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate*, in «Brooklyn journal of international law» 26 (2000/01).

[3] Per uno studio del rapporto tra sicurezza e libertà nel mondo digitale, da ultimo N.W. Palmieri, *Sicurezza o libertà? Introduzione al diritto di Internet*, Pitagora, Bologna 2005; anche K.A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, in «International Journal of Communications Law & Policy» 8 (2005).

[4] Cfr. G. Corasaniti, *Esperienze giuridica e sicurezza informatica*, Giuffrè, Milano 2003, p. 2.

garanzia [5]. Ciò comporta una continua opera di vigilanza, verifica, promozione e dialettica tra le posizioni coinvolte, con un'attività di costante adeguamento di parametri e standard di sicurezza alle condizioni che variano in rapporto alle conoscenze tecnologiche o che derivano da fattori esterni o interni di rilevante importanza [6].

Su un piano, invece, prettamente economico, si possono dare al concetto di sicurezza due differenti letture, potendosi parlare di un semplice stato di fatto, da un lato, oppure di determinate condizioni ottimali per la propria attività tali da ridurre i pericoli e i rischi, dall'altro. La sicurezza, intesa quale insieme di condizioni che mitigano 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, imprese che offrono servizi di sicurezza, ecc.) [7].

La situazione che noi definiamo *sicurezza* si basa su un equilibrio tra fiducia nel contesto in cui ogni individuo si trova a operare e tolleranza al rischio [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. 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 tra-

[5] Il problema e la discussione circa la 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, per sviluppare poi una corretta analisi delle possibili ipotesi di intervento.

[6] Per un'analisi degli standard di sicurezza nello specifico tema dei pagamenti on-line, P. Guarda, *Sicurezza dei pagamenti e privacy nell'e-commerce*, in «Diritto dell'Internet» 2005, p. 91.

[7] W. Sofsky, *Rischio e sicurezza*, Einaudi, Torino 2005, p. 65: *Nonostante la loro efficienza, i mercati sono tutt'altro che sicuri. L'economia è un affare rischioso. I fattori sono troppi e vari perché le scelte possano dirsi al riparo dall'incertezza … Nuove tecnologie imprimono a volte scosse tali da far tremare tutta l'economia.*

[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.

dizione o ai capricci della natura [9].

In ambito informatico, si registra come lo sviluppo delle tecnologie digitali e la diffusione della società dei computer abbia reso sempre più evidente la necessità di programmare e implementare strumenti via via più evoluti, volti a proteggere i file e le informazioni raccolte nelle banche dati (si parla appunto di *computer security*). La Rete ha poi colorato di nuove sfumature questo settore di studio. L'affermarsi di sistemi cosiddetti *distributed* e il diffondersi di reti di comunicazione tra i diversi terminali, infatti, ha sollevato un nuovo problema: la tutela dell'integrità dei dati durante la loro trasmissione. Il termine *network security* individua, appunto, questa sottocategoria della sicurezza informatica, la quale focalizza la propria attenzione sugli strumenti che consentono le comunicazioni intercorrenti tra i vari punti e nodi di una rete. Posto che Internet è definita come la rete delle reti, si parla anche di *Internet security* [10]. La scienza informatica nel campo della *computer security* si basa su alcuni principi che, sulla scorta dei principi giuridici, caratterizzano e condizionano l'analisi dei diversi contesti in cui essa poi si estrinseca. La loro definizione è oggetto di dibattiti e approfondimenti da parte della dottrina scientifica [11]. L'insicurezza di un sistema infor-

[9] G. Corasaniti, *Esperienza giuridica e sicurezza informatica* … cit., p. 4.

[10] Il tema delle architetture informatiche è oggetto di analisi anche nella psicologia, in quanto dipende da un modo di sentire che non si basa sulla probabilità e sui calcoli matematici ma sulle reazioni psicologiche che abbiamo di fronte ai rischi e alle misure di protezione. Da qui l'acquisita consapevolezza che la protezione dei dati personali rappresenti una sorta di *trade-off*, di bilanciamento nelle scelte tra i guadagni rispetto a un certo obiettivo e le contemporanee perdite riguardo a un altro. Vedi gli ottimi approfondimenti di quello che viene considerato un *guru* della *computer security*, B. Schneier, reperibili sul suo *blog*, *Schneier on Security*, http://www.schneier.com/blog/. Tra gli altri si segnalano: B. Schneier, *The Psychology of Security*, Gennaio 2008, reperibile all'URL: http://www.schneier.com/essay-155.html; ID., *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*, Springer, Berlin 2006. L'autore individua cinque aspetti specifici del *trade-off* di sicurezza su cui un individuo può essere portato a sbagliare: a) il grado di rischio, b) la probabilità del rischio, c) il valore dei costi, d) l'efficacia della misura di protezione nel mitigare il rischio, e) il *trade-off* stesso.

[11] Per approfondimenti sul tema della sicurezza informatica, R. Anderson, *Security Engineering. A Guide to Building Dependable Distributed Systems*, Wiley, New

matico è stata valutata talvolta come una caratteristica 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 non va fatta passare l'idea che l'insicurezza sia intrinsecamente e 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, di carattere contrattuale specifico), di carattere tecnico-scientifico (definizione di standard), di carattere organizzativo (istituzione di* task force *dedicate o di articolazioni organizzative specializzate negli interventi possibili) e infine di carattere economico (analisi dei costi-benefici delle situazioni concrete, individuazione delle risorse utilizzabili, ammortizzazione pianificata dei costi derivanti dall'esposizione a rischio).* [12]

Se il problema che qui ci impegna viene, infine, approcciato avendo presente l'inscindibile rapporto che lega la sicurezza alla *privacy*, occorre sgomberare il campo da possibili fraintendimenti dovuti all'ambiguità del termine *sicurezza* stesso. Da un lato con esso, infatti, intendiamo la protezione del singolo e quindi dei sistemi informatici posti sotto il suo controllo: da questa prospettiva la sicurezza informatica non rappresenta altro che la naturale evoluzione della protezione dei dati personali. Dall'altro, però, talvolta si fa riferimento a un concetto sostanzialmente diverso, quello della sicurezza pubblica o nazionale: è questo il caso della normativa emergenziale con finalità di contrasto al terrorismo; in tale contesto *sicurezza* si-

---

York 2001, pp. 3 ss. reperibile all'URL: http://www.cl. cam. ac.uk/%7Erja14/book.html; D. Gollman, *Computer Security*, Wiley and Sons, Chichester 2006², pp. 17 ss.; W. Stallings, *Network Security Essentials: Applications and Standards*, Pearson Prentice Hall, Upper Saddle River, N. J. 2007³, pp. 11 ss.

[12] G. Corasaniti, *Esperienza giuridica e sicurezza informatica* … cit., pp. 15-16.

gnifica riduzione del livello di protezione della *privacy* e dei dati personali dei cittadini, venendo così ad assumere una connotazione opposta a quella appena descritta. È importante avere chiara tale distinzione soprattutto quando si cerca di declinare nel contesto informatico principi e regole che contraddistinguono l'ambito giuridico.

Nello scenario informatico poi, e più precisamente all'interno della Rete, la tematica si distingue per peculiari caratteristiche. Nel corso della navigazione su Internet l'utente lascia, spesso a sua insaputa, numerose tracce. Lo fa sin dall'inizio quando si connette a essa tramite il suo *Internet Service Provider* (ISP); o quando si collega ai vari siti Web; oppure quando scrive o legge la sua posta elettronica. Tutte queste tracce si trovano in diversi luoghi: nei file di *log* dell'ISP, nei file di *log* del proprio computer, nei *cookie* automaticamente scaricatisi sulla macchina dell'utente, e così via. Occorre porre sempre più l'attenzione su questo aspetto.

Esistono, infatti, diversi soggetti potenzialmente interessati a queste informazioni. Ma chi ci spia e perché? Anzitutto lo fa lo Stato. Paradigmatico è il caso statunitense nel quale, dopo l'attacco alle Torri Gemelle, le agenzie investigative hanno visto aumentare il loro potere e la loro capacità di penetrazione nella vita privata dei cittadini, in virtù di una nuova legislazione specificamente mirata a contrastare il pericolo terrorismo: il famigerato *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) ne è un ottimo esempio. L'approccio al problema terrorismo che traspare da questi interventi normativi si ricollega a quel concetto di sicurezza pubblica che permette al legislatore di giustificare un abbassamento del livello di protezione della *privacy* dei propri cittadini. Non è peregrino, però, ipotizzare che l'attività di controllo da parte dello Stato si possa caratterizzare anche per azione di poteri deviati interessati a monitorare e controllare la vita di soggetti di evidenza pubblica. Spiano, poi, anche le imprese commerciali. Lo fanno tracciando la navigazione degli utenti e profilandone gli interessi e i gusti commerciali. Scopo di questa forma di controllo è mettere in opera forme di *marketing* sempre più mirate

ed efficaci. L'utente sarà così *bersagliato* da mail con contenuto similare ai suoi interessi e la sua navigazione sarà scandita da numerosi *banner* pubblicitari giustapposti ai siti Web visitati con l'offerta di prodotti per i quali è già stato dimostrato gradimento. Nuova frontiera è il monitoraggio al fine di auto-tutela dei propri interessi [13]. Infine, a spiare possono essere anche dei soggetti privati con lo scopo di porre in essere attacchi diretti al sistema informatico della vittima, o per *voyeurismo* o semplice curiosità.

Il presente contributo cercherà di fornire indicazioni utili a chiarire il concetto di sicurezza informatica declinato all'interno del contesto giuridico. Per fare ciò si approfondiranno gli ambiti applicativi dei due significati di sicurezza, quello personale e quello pubblico, che sono stati sopra individuati. Nel secondo paragrafo si descriverà, pertanto, la disciplina della sicurezza dei dati contenuta all'interno della normativa italiana in tema di trattamento dei dati personali. Il terzo paragrafo tratterà, invece, seppur per cenni, del rapporto tra la protezione delle informazioni e la sicurezza dello

[13] Nel famoso caso Peppermint si palesa il conflitto tra *copyright* e *privacy*. Il fatto è il seguente: un'impresa tedesca, la Peppermint, titolare di diritti d'autore su repertori di opere musicali, si serve di un'impresa svizzera, la Logistep, la quale fornisce, mediante l'utilizzo di appositi software, servizi di monitoraggio delle reti P2P, al fine di individuare e memorizzare elementi che comprovino le violazioni dei propri diritti e l'individuazione dei responsabili di tali violazioni. Il trattamento dei dati da parte della Peppermint è avvenuto in due fasi: in un primo momento si è provveduto alla raccolta ed elaborazione automatizzata di svariate informazioni di carattere personale ottenute, come detto, tramite reti di *peer-to-peer* grazie a un software utilizzato dalla Logistep; in un secondo momento, si è cercato il modo di ottenere dall'autorità giudiziaria in sede civile la comunicazione dei dati posseduti dagli ISP al fine di riuscire a collegare gli indirizzi IP raccolti ai nominativi degli intestatari delle utenze telefoniche. Ottenuti tali dati, il legale della Peppermint inviava, infine, diverse centinaia di lettere a persone individuate come intestatari delle linee di collegamento a Internet, contestando la violazione dei diritti derivanti dalla produzione di fonogrammi e proponendo una soluzione bonaria, alternativa alla denuncia in sede penale, basata sul rispetto di alcune condizioni che comprendevano un versamento di una somma di denaro. Per approfondimenti, R. Caso, *Il conflitto tra copyright e privacy nelle reti peer to peer: in margine al caso Peppermint. Profili di diritto comparato*, in «Diritto dell'Internet» 2007, p. 471 (reperibile anche in formato digitale all'URL: http://www.jus.unitn.it/users/caso/DRM/Libro/peppermint/home.asp).

Stato, fornendo utili approfondimenti con riferimento al ruolo e alle strategie che i governi dei diversi Paesi stanno assumendo all'interno della Rete. Infine, si svolgeranno delle considerazioni di sintesi volte a tracciare i possibili scenari futuri della sicurezza informatica.

2. La sicurezza nel trattamento dei dati personali

La disciplina della sicurezza del trattamento dei dati personali si ritrova nell'ordinamento giuridico italiano all'interno del d. lgs. 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali* (d'ora in avanti: *Codice Privacy*) [14]. In esso viene riservato un apposito Titolo V, Parte I, alla regolamentazione della *Sicurezza dei dati e dei sistemi*, dedicando il Capo I agli obblighi di sicurezza in generale e il Capo II alle misure minime di sicurezza [15]. La nuova discipli-

[14] Per quanto riguarda la disciplina della protezione dei dati personali, si veda, in prima battuta, N. Lugaresi, *Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario*, in «Giustizia amministrativa» 2004, p. 289; R. Pardolesi, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. Pardolesi (a cura), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano 2003, pp. 1-57; L.A. Bygrave, *Data Protection Law. Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague – London – New York 2002; P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, Milano 2002; P. Guarda, *Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in «Ciberspazio e diritto», 2008, p. 65 (reperibile all'URL: http://eprints. biblio. unitn.it/archive/00001524/); M. Martines, *La protezione degli individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione europea*, in «Rivista italiana di diritto pubblico comunitario» 2000, p. 719; J. Morton, *Data Protection and Privacy*, in «European Intellectual Property Review» 18 (1996), p. 558.

[15] Sul tema delle misure di sicurezza in materia di *privacy*, C. Rabazzi, P. Perri, G. Ziccardi, *La sicurezza informatica e la privacy*, in G. Ziccardi (a cura), *Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto*, Giuffrè, Milano 2005, pp. 516 ss.; P. Perri, *Le misure di sicurezza*, in J. Monducci, G. Sartor (a cura), *Il codice in materia di protezione dei dati personali*, CEDAM, Padova 2004, p. 137; A. Biasiotti, *Codice della privacy e misure minime di sicurezza: D. Lgs. 196/2003*, Epc, Roma, 2004[2]; G. Corasaniti, *La sicurezza dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno-

na è contenuta negli articoli 31 e seguenti del *Codice Privacy*, nel suo *Disciplinare Tecnico in materia di misure minime di sicurezza* (allegato B). Infine, come criterio a carattere generale si pone, inoltre, quello sancito all'art. 3, il quale riconosce e definisce il principio di necessità nel trattamento dei dati [16].

La disciplina della sicurezza dei dati personali deriva dall'obbligo sancito a livello europeo dall'art. 17 della direttiva 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, che al primo comma così recita:

> *Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche e organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno*

Zencovich (a cura), *Il codice dei dati personali*, Giuffrè, Milano 2004, pp. 112-163; ID., *Esperienza giuridica e sicurezza informatica* … cit., pp. 153-257; F. Berghella, *Guida pratica alle nuove misure di sicurezza per la privacy*, Maggioli, Roma 2003, p. 141; M. Maglio, *Le misure di sicurezza nei sistemi informativi: il punto di vista di un giurista alla luce della legge sulla tutela informatica*, in «Contratto e impresa» 2000, p. 1; P. Perri, *Introduzione alla sicurezza informatica e giuridica*, in E. Pattaro (a cura), *Manuale di diritto dell'informatica e delle nuove tecnologie*, CLUEB, Bologna 2002, p. 306; G. Elli, *Privacy e sicurezza dei dati*, Milano, 2001; A. Sessa, *Le misure minime di sicurezza per il trattamento dei dati personali (d. p. r. 28 luglio 1999, n. 318)*, in «Rassegna forense» 2000, p. 81; P. Veneziani, *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali: prime osservazioni*, in «Rivista trimestrale di diritto penale dell'economia» 1997, p. 135.

[16] L'art. 36 del *Codice Privacy* stabilisce che il *Disciplinare Tecnico* venga periodicamente aggiornato con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie in relazione all'evoluzione tecnica e all'esperienza maturata nel settore. Il fatto che si preveda la necessità di un aggiornamento costante risponde alle nuove logiche normative in settori in cui la tecnologia gioca un ruolo di rilevante importanza. Si hanno così regolamentazioni a due livelli: un primo livello che stabilisce le regole generali e i principi di base relativi all'attività che si deve svolgere, un secondo che determina più nel dettaglio gli specifici standard da adottare, i quali, vista la costante evoluzione tecnologica, sono soggetti a un necessario, periodico aggiornamento.

> *di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.*

2.1. Obblighi di sicurezza

All'art. 4, co. 3, del *Codice Privacy* troviamo la definizione di *misure minime*:

> *il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.*

Nel descrivere le misure di sicurezza, il *Codice* fa riferimento a fattori ed eventi di rischio di diversa importanza e causalità, che dipendono da varie condizioni interne ed esterne, nei confronti delle quali assume estrema importanza il complesso degli strumenti e dei metodi adottati in via preventiva nel contesto delle operazioni di trattamento. Maggiore sarà il rischio che può derivare da intromissioni esterne o da possibili interventi sui dati personali, tanto più sarà da ritenersi vincolante l'adozione di strumenti e metodologie volte alla sua prevenzione o riduzione.

L'art. 31 prescrive che:

> *I dati personali oggetto di trattamento [siano] 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.* [17]

[17] L'articolo riproduce alla lettera il primo comma dell'art. 15 della l. 675/1996, affrontando il tema delle misure di sicurezza idonee e preventive, da tenere ben distinte dalle misure minime di sicurezza.

L'ambito soggettivo della disciplina comprende sia i soggetti pubblici che quelli privati.

La regolamentazione di apposite misure di sicurezza preventive nel trattamento dei dati personali nasce dalla necessità di contrastare fenomeni di illiceità informatica sempre più diffusi che possono determinarsi dall'interno come dall'esterno del sistema informatico.

Le misure *idonee e preventive* non vengono tipizzate per condivisibile scelta normativa, in quanto il riferimento a specifiche soluzioni tecniche non sarebbe risultato praticabile dato il loro continuo mutare al variare delle tecnologie a disposizione. Tali misure vanno rapportate a tre criteri di riferimento: 1) il progresso tecnico; 2) la natura dei dati; 3) la specifica caratteristica del trattamento. Si noti come manchi qualsiasi riferimento ai costi dell'implementazione, che invece la direttiva 95/46/CE prevedeva all'art. 17. Questa scelta rende l'impianto delle misure di sicurezza nel contesto nazionale maggiormente restrittivo rispetto a quello europeo, non prevedendo la possibilità di una maggiore modularità di implementazione delle misure stesse. Ciò avrebbe probabilmente garantito alla regolamentazione una maggiore efficacia applicativa, specialmente con riferimento a strutture organizzative di differente dimensione ed entità [18].

In attuazione della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, l'art. 32 individua, poi, particolari obblighi riguardanti i fornitori di un servizio di comunicazione elettronica accessibile al pubblico, i quali sono tenuti ad adottare idonee misure tecniche e organizzative *adeguate al rischio esistente*, ai sensi dell'art. 31, al fine di salvaguardare la sicurezza dei servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comu-

[18] G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, Milano 1997, pp. 330 ss. Per un'analisi dei costi di implementazione delle regole stabilite dal *Codice Privacy* all'interno delle relazioni aziendali nei primi anni di sua applicazione, A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, Milano 2007, in particolare pp. 203-315.

nicazioni elettroniche rispetto a ogni forma di utilizzazione o cognizione non consentita. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente. Infine, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati nel caso in cui sussista

> *un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare …, tutti i possibili rimedi e i relativi costi presumibili.*

Uguale informativa è inviata al Garante per la protezione dei dati personali (d'ora in avanti: *Garante Privacy*) e all'Autorità per le garanzie nelle comunicazioni.

Ricorre, infine, la responsabilità civile, quindi l'obbligo risarcitorio, nel caso in cui le misure adottate non siano idonee a evitare il danno. Ciò ai sensi dell'art. 15 del *Codice Privacy*, il quale, facendo esplicito rimando all'art. 2050 c. c. (relativo allo svolgimento di attività pericolose), determina un'inversione dell'onere della prova che incombe, così, sul titolare del trattamento, il quale, per non incorrere in responsabilità, dovrà dimostrare l'adozione di tutte le misure logiche, fisiche e procedurali atte a impedire il verificarsi del danno.

2.2. Misure minime di sicurezza

Il Capo II del *Codice Privacy* all'art. 33 provvede a fornire una concreta definizione delle misure *minime* di sicurezza che i titolari del trattamento, nel quadro dei più generali obblighi di sicurezza previsti all'art. 31 o in speciali disposizioni, sono tenuti ad adottare per

assicurare un livello minimo di protezione dei dati personali [19].

Qualsivoglia soggetto che si dedichi al trattamento dei dati personali è, di conseguenza, obbligato sia all'osservanza di un generico obbligo di protezione, che all'implementazione di ulteriori misure che di *minimo* risultano avere solo l'aggettivo, in quanto incidono considerevolmente sull'organizzazione e sui metodi di trattamento dei dati stessi, introducendo prescrizioni direttamente vincolanti e la cui inosservanza è, pure, penalmente sanzionata.

Nel *Codice* è rimasta inalterata la distinzione tra trattamenti effettuati con gli strumenti elettronici e senza l'ausilio di essi (come ad esempio quelli su supporto cartaceo); mentre all'interno dei *trattamenti effettuati con strumenti elettronici* non si fa più la distinzione, di cui al d. p. r. 28 luglio 1999, n. 99, fra quelli attuati mediante elaboratori non accessibili da altri elaboratori (cosiddetti *stand alone*) e quelli, invece, posti in essere attraverso elaboratori accessibili in rete.

Con riferimento ai trattamenti con strumenti elettronici, l'art. 34 specifica che il trattamento dei dati personali è consentito solo nel caso in cui vengano adottate, nei modi previsti dal *Disciplinare Tecnico in materia di misure minime di sicurezza* (Allegato B del *Codice*), le seguenti misure *minime* [20]:

- *autenticazione informatica*: l'insieme di tutti gli strumenti elet-

[19] Manca una prescrizione articolata in grado di predefinire in un chiaro ambito di adeguatezza il carattere dei dati da proteggere e l'ambito entro il quale la disposizione dovrebbe applicarsi (ciò sarebbe risultato anche maggiormente coerente con la direttiva 95/46/CE).

[20] In pratica si tratta di un sintetico quadro direttamente ispirato al d.p.r. 318/1999 emanato sulla base della previgente disciplina e il cui contenuto è puntualmente esplicato nel *Disciplinare Tecnico*. Le previsioni di tale disciplinare si basano sullo standard ISO/IEC 17799: 2005 (*Code for practice for information security management*). Il Garante per la protezione dei dati personali ha ultimamente provveduto a semplificare alcune misure minime richieste dal *Codice Privacy* e dall'allegato tecnico a favore di talune categorie di soggetti: cfr. Provv. del 19 giugno 2008: *Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili* e il Provv. del 27 novembre 2008: *Semplificazioni delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali*; cfr. anche quanto sancito dall'art. 29 del d. l. 25 giugno 2008, n. 112, che prevede in specifici casi l'esonero dell'adozione del DPS.

tronici e di tutte le procedure per la verifica, anche indiretta, dell'identità dell'utente;

- *adozione di procedure di gestione delle credenziali di autenticazione*: queste sono costituite dall'insieme dei dati e dei dispositivi, in possesso di una persona, da questa conosciuti e a essa univocamente correlati, necessari affinché si abbia l'autenticazione informatica (vedi ad esempio il riconoscimento biometrico, lo *user id*, la *password*, l'impronta digitale, le *smart card*, ecc.);
- *utilizzazione di un sistema di autorizzazione*: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, sulla base del profilo di autorizzazione stabilito dai responsabili a favore del richiedente, già precedentemente autenticato al sistema [21];
- *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici*: il titolare del trattamento è tenuto a un aggiornamento periodico, o quantomeno con cadenza annuale, dei profili di autorizzazione al fine di verificare la permanenza delle condizioni necessarie per lo svolgimento del trattamento in capo al singolo incaricato [22];
- *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici*: i mezzi da adottare per garantire la protezione degli strumenti e dei dati non sono stati specificatamente previsti con la consapevolezza che il continuo progresso tecnologico degli strumenti tecnici finalizzati a tale scopo avrebbe condannato a una rapida quanto inesorabile obsolescenza qualsiasi altra più specifica previsione;

[21] Sul punto il *Disciplinare Tecnico* fornisce le istruzioni relative alla gestione del sistema di autenticazione informatica. Possiamo, quindi, individuare una prima fase relativa alla autenticazione, in cui il sistema informatico provvede a individuare in modo certo l'identità dell'utente mediante l'impiego di specifici sistemi di riconoscimento, e una seconda fase relativa alla autorizzazione, nella quale all'utente è consentito di accedere alle specifiche risorse individuate nel profilo di autorizzazione, come ad esempio a determinati database, file specifici, programmi sul sistema, ecc.

[22] Cfr. *Disciplinare Tecnico* al punto 14.

- *adozione di procedure per la custodia di copie di sicurezza (cosiddette copie di* back-up*) e per il ripristino della disponibilità dei dati e dei sistemi*: si prevede la predisposizione da parte del titolare di procedure relative alla memorizzazione e alla custodia di copie di sicurezza volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità e il ripristino dei dati o degli strumenti elettronici in caso si verifichi un problema che abbia determinato la perdita o l'alterazione dei dati stessi;
- *tenuta di un aggiornato documento programmatico sulla sicurezza* (DPS): esso consiste in un documento organico pensato al fine di tenere in considerazione i sistemi informativi presenti in una particolare struttura e rappresenta lo strumento organizzativo più importante e innovativo, costituendo la base uniforme per il controllo delle strategie di sicurezza in concreto adottate [23]. Lo scopo principale è quello di fornire un quadro completo della struttura organizzativa facente capo al titolare del trattamento da un punto di vista logistico, informatico e di allocazione delle risorse umane [24];

[23] Il DPS è stato introdotto nel nostro ordinamento per la prima volta dall'art. 6 del d.p.r. 318/1999, poi ribadito come visto nell'art. 34, lett. g, *Codice Privacy*. Per approfondimenti cfr. P. Perri, *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano 2007, pp. 252-262; F. Tommasi, *La sicurezza dei sistemi informativi ed il documento programmatico sulla sicurezza*, in G. Cassano (a cura), *Diritto delle nuove tecnologie informatiche e dell'Internet*, Ipsoa, Milano 2002, p. 853; S. Sutti, *La sicurezza dei sistemi informativi aziendali. Norme protettive, oneri e misure*, ivi, p. 837.

[24] L'art. 34, lett. g, *Codice Privacy* inserisce il DPS tra le misure minime di sicurezza, ma è il punto n. 19 dell'Allegato B – *Disciplinare Tecnico in materia di misure minime di sicurezza* – a esporne il contenuto, così articolato: a) l'elenco dei trattamenti di dati personali; b) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati; c) l'analisi dei rischi che incombono sui dati; d) 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; e) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (cosiddetto *data restore*); f) la previsione di interventi formativi; g) 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; h) per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da a-

- *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*: le tecniche di cifratura o i codici identificativi devono rendere i dati inintelligibili momentaneamente anche all'incaricato autorizzato ad accedervi e non devono permettere l'identificazione dell'interessato se non in caso di necessità [25].

Ancora qualche considerazione in tema di conseguenze connesse all'omessa adozione di misure di sicurezza. L'art. 169 *Codice Privacy* prevede che chiunque, essendovi tenuto, ometta di adottare le misure minime previste dall'articolo 33 sia punito con *l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro*. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione che fissa 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 (a titolo di oblazione) una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato [26].

---

dottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato (v. punto 24, Allegato B).

[25] Cfr. art. 22 del *Codice* dove sono sanciti i principi applicabili al trattamento dei dati sensibili e giudiziari.

[26] Si noti che si prevede una sanzione penale e subito dopo si concede la possibilità al trasgressore di adeguarsi alle prescrizioni del Garante con l'estinzione del reato a seguito del pagamento di una somma di denaro, a titolo di oblazione: questo può assumere un effetto di deterrenza in caso di realtà piccole, ma presenta un impatto notevolmente inferiore nei confronti di grosse e più complesse strutture organizzative.

2.3. Il principio di necessità nel trattamento dei dati

Il principio di necessità rappresenta uno tra gli aspetti più innovativi del *Codice Privacy*. Esso è sancito all'art. 3:

> *i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.* [27]

La particolare rilevanza attribuita a questa previsione attraverso la sua collocazione *topografica* all'interno del *Codice* tra i principi generali si può far derivare dall'opportunità, avvertita con considerevole urgenza dal nostro legislatore, di predisporre idonee forme di tutela per limitare al massimo la circolazione di dati personali connessa all'informatizzazione della società moderna, con specifico riferimento all'esponenziale diffusione dell'utilizzo della Rete.

L'ambito d'applicazione dell'articolo in oggetto è da rinvenirsi in riferimento al trattamento di dati effettuato attraverso l'impiego di *sistemi informativi* e *programmi informatici*. Nel linguaggio corrente l'espressione *sistema informativo* richiama un complesso di risorse (sia di tipo hardware che di tipo software) finalizzato al trattamento automatizzato delle informazioni, mentre con quella di *programmi informatici* si è semplicemente fornita una traduzione concettuale, anche se non prettamente letterale, del termine inglese software.

Il principio di necessità rappresenta, in un certo senso, una sorta di anticipazione degli adempimenti previsti dal Titolo V e impo-

[27] Sul principio di necessità in dottrina, R. D'Orazio, *Il principio di necessità nel trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura), *Il codice del trattamento dei dati personali*, Giappichelli, Torino 2007, pp. 20-27; G. Resta, *Il diritto alla protezione dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura), *Il codice dei dati personali …* cit., pp. 45 ss.; cfr. anche A. Palmieri, R. Pardolesi, *Il codice in materia di protezione dei dati personali e l'intangibilità della* privacy *comunitaria*. Nota a sent. Corte di Giustizia delle Comunità Europee 6 novembre 2003, n. causa C-101/01, in «Foro italiano» 2004/4, p. 59.

ne al titolare del trattamento di adottare delle misure organizzative informatiche idonee a escludere per quanto possibile l'utilizzo di dati personali e identificativi.

Questo risultato potrà essere perseguito utilizzando o dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità. Nel primo caso, ci troviamo di fronte a una specificazione del principio generale sancito all'art. 11, comma 1, lett. d, laddove si stabilisce, tra l'altro, che i dati trattati devono essere *non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*. Quando le finalità per cui i dati sono sottoposti a trattamento possono essere conseguite anche attraverso il trattamento di dati non associabili a un soggetto identificato, allora il titolare non sarà legittimato a elaborare dati eccedenti, tra cui sicuramente vanno fatti rientrare quelli relativi all'identificazione dell'interessato [28]. Nel caso, invece, dell'utilizzazione di modalità che permettano di identificare l'interessato solo in caso di necessità, occorre intendere tale previsione come un esplicito riconoscimento di favore legislativo per i trattamenti effettuati attraverso pseudonimi, ovvero scorporando le informazioni trattate in modo tale che l'incaricato non abbia alcuna possibilità di identificare l'interessato cui i dati si riferiscono.

Sul piano dell'implementazione, questa disposizione richiede qualcosa di nuovo e alquanto oneroso, soprattutto in riferimento alla situazione in cui si trova a operare. Essa presuppone cospicui investimenti, tanto sotto il profilo delle risorse informatiche (risultando chiaramente necessario un ripensamento dei sistemi), quanto sotto quello delle risorse umane [29].

La dottrina ha, finora, proposto una lettura riduttiva della disposizione in oggetto individuando in essa unicamente un criterio di organizzazione tecnica degli archivi informatici, finalizzato a in-

[28] Merita di ricordare che il trattamento di dati anonimi non è soggetto alle previsioni normative del *Codice* le quali trovano applicazione solamente in relazione al trattamento di dati personali.

[29] Cfr. A. Palmieri, R. Pardolesi, *Il codice in materia di protezione dei dati personali* … cit.

centivare l'adozione di *privacy enhancing technology* (PET) [30].

Il principio di necessità sancito all'art. 3 del *Codice* fornisce un generale criterio di indirizzo e di conformazione dell'azione tecnologica. Da parte di alcuni è stato sostenuto che esso sembra imporre una prescrizione eccessiva e certamente volta a disciplinare in via preventiva l'utilizzazione di risorse informative da parte di soggetti pubblici e privati, con evidenti problemi di incostituzionalità in rapporto alla libertà individuale e d'impresa [31]. In realtà, il principio in oggetto, sebbene possa apparire astruso nella sua genericità, trova la sua ragion d'essere nel fatto che alcuni rischi per la sicurezza di un sistema informativo possono essere evitati solo se a monte, al momento della programmazione della struttura informatica, ci si pone il problema di implementare le previsioni normative sulla protezione dei dati personali. La *privacy* dei dati può essere raggiunta solamente se il sistema è costruito in maniera tale da consentire la sua difesa [32].

---

[30] Cfr. R. Acciai, S. Melchionna, *Le regole generali per il trattamento dei dati personali*, in R. Acciai (a cura), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini 2004, p. 71; S. Niger, *Il diritto alla protezione dei dati personali*, in J. Monducci, G. Sartor (a cura), *Il codice in materia di protezione dei dati personali* … cit., pp. 12-13 ss. In particolare sulle PET, cfr. G. Pascuzzi, *Il diritto dell'era digitale* … cit., pp. 77-81; D. Martin, A. Serjantov (a cura), *Privacy Enhancing Technologies*, Atti del 4° workshop internazionale PET 2004 Toronto, Sperling, Berlino 2005.

[31] Cfr. G. Corasaniti, *La sicurezza dei dati personali* … cit., p. 142.

[32] Un nuovo ed emergente filone di ricerche interdisciplinari si dedica, appunto, allo studio dell'incorporazione di valori giuridici all'interno delle architetture digitali, seguendo un approccio interdisciplinare e giovandosi, così, dell'apporto di numerose e diverse scienze, l'economia, il diritto, la sociologia, l'informatica. Ci si riferisce al c.d. *value-sentitive design* o *value-centered design.* Per approfondimenti, cfr. S. Bechtold, *Value-centered Design of Digital Rights Management*, 2004, reperibile sul sito Web: http://www.indicare.org/tikiread_article. php? articleId = 39; B. Friedman, D.C. Howe, E. Felten, *Informed Consent in the Mozilla Browser: Implementing Value-sensitive Design*, in *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002.

3. La sicurezza dello Stato

Il termine *sicurezza* assume un significato particolare quando viene declinato in ambito pubblico e/o nazionale.

L'analisi del ruolo dello Stato nel contesto digitale, soprattutto con riferimento al suo compito di controllore delle attività che in esso vengono poste in essere, non può prescindere dai tragici eventi successi l'11 settembre 2001: l'attacco terroristico alle Torri Gemelle, 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 e operativo, l'intero apparato dei servizi di sicurezza [33]. La stessa opinione pubblica è stata, così, obbligata a interrogarsi sul corretto bilanciamento tra la sfera dei diritti e il bisogno di sicurezza che ha portato all'incremento dei poteri di sorveglianza in capo agli organi esecutivi dello Stato [34].

Il 16 ottobre 2001 il Congresso statunitense 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* (USAPA) [35] – cui abbiamo già fatto cenno sopra – 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 a informazioni riservate nel campo finanziario per contrastare i finanziamenti ai terroristi e consentiva all'*Attorney Ge-*

[33] Per un'analisi del rapporto tra *privacy* e sicurezza dopo l'attacco alle Torri gemelle, cfr. P. Guarda, *Agenti software e sicurezza*, in G. Pascuzzi (a cura), *Diritto e tecnologie evolute del commercio elettronico*, Cedam, Padova 2004, p. 315.

[34] Cfr. da ultimo G. Frosio, *Cosa resta della privacy? – diritto alla riservatezza dell'*uomo medio *dopo l'11 settembre*, in «Ciberspazio e diritto» 2005, p. 173; L. Nelson, *Public Administration and Civil Liberties – Protecting the Common Good: Technology, Objectivity, and Privacy*, in «Public Administration Review» 62 (2002) Issue Supplement s1; J.B. Gould, *Playing with Fire: The Civil Liberties Implications of September 11th*, ivi, p. 74; M.W. Spicer, *The War on Terrorism and the Administration of the American State*, ivi, p. 63.

[35] «Public Law» 107-56, 26 (2001), 115 Stat. 271.

neral di incarcerare o di espellere gli stranieri sospettati di legami con il terrorismo [36]. Esso di fatto non introduceva forme nuove di controllo e intercettazione rispetto a quelle già in uso nel contesto giuridico statunitense, bensì andava a facilitarne l'utilizzo riducendo sensibilmente i limiti e le garanzie che vigilavano sul rispetto dei diritti fondamentali dei cittadini [37].

Seguirono numerose prese di posizione e critiche da parte di vari settori e 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 sistema di *checks and balances* che precedentemente conferiva alle Corti l'opportunità di verificare che non avvenissero abusi nella gestione e applicazione dei poteri di sorveglianza conferiti alle autorità statali.

Circa un anno dopo (25 novembre 2002) veniva emanato l'*Homeland Security Act* [38], che si inseriva sul solco tracciato dall'USAPA e 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 all'ambito delle intercettazioni telefoniche e telematiche, e, 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 a 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 il loro utilizzo comporta.

---

[36] V.J.C. Ting, *Unobjectionable but Insufficient-Federal Initiatives in Response to the September 11 Terrorist Attacks*, in «Connecticut Law Review» 34 (2002), p. 1145.

[37] Per approfondimenti cfr. A. De Pretis, *L'approccio giurisprudenziale alla tutela della privacy informatica: capacità innovativa e tradizione costituzionalistica*, in «Diritto informazione e informatica» 2008, p. 911; ID., *Il Patriot Act e le libertà digitali*, ivi, 2007, p. 599.

[38] «Public Law» 107-296, 27 (2002), 116 Stat. 2135.

Il fenomeno della legislazione emergenziale anti-terrorismo non ha interessato evidentemente solo l'ordinamento statunitense ma ha riguardato numerosi altri Stati, andando così ad assumere i connotati di un fenomeno globale [39].

3.1. Internet e terrorismo

Occorre trattare, seppur brevemente, di un aspetto peculiare della società dell'informazione che sta via via crescendo in termini di importanza e diffusione: l'utilizzo delle informazioni come arma volta a degradare o manipolare il patrimonio informativo di un determinato obiettivo prescelto. Ci si riferisce a quel fenomeno che prende il nome di *Information warfare* [40]. Ciò può avvenire in diversi contesti. Quello più dichiaratamente militare, dove l'attacco informatico serve spesso per anticipare e preparare un conseguente attacco tradizionale ed è volto a danneggiare i sistemi informativi del nemico riducendo così fortemente la sua capacità di reazione all'aggressione [41]. Quello, invece, industriale e commerciale, nell'ambito del quale gli ingenti investimenti tesi a contrastare strategie di spionaggio aziendale dimostrano l'esistenza di un'esigenza sempre più avvertita in un contesto che, per certi aspetti, rappresenta una sorta di nuovo *campo di battaglia* per i tradizionali conflitti armati. Abbiamo,

[39] Ad esempio in Inghilterra si possono ricordare il *Terrorism Act* del 2000, l'*Anti-terrorism, Crime and Security Act* del 2001 (ATCSA), il *Prevention of Terrorism Act* del 2005, il *Terrorism Act* del 2006, ecc.; in Germania il *Terrorismusbekaempfungegesetz* del 9 gennaio 2002 e la *Luftsicherheitsgesetz* del 14 gennaio 2005; in Italia, infine, si ricorda la l. 1 agosto 2005, n. 155: *Conversione in legge, con modificazioni, del decreto legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale*.

[40] Cfr. G. Ziccardi, *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Tomo II, Giuffrè, Milano 2008, pp. 236-245. Per uno studio del fenomeno all'interno del diritto internazionale cfr. S.J. Shackelford, *From Nuclear War to Net Ware: Analogizing Cyber Attacks in International Law*, in «Berkeley Journal of International Law» 27 (2009), p. 192.

[41] Questa tecnica è molto usata nella moderna guerra tecnologica. Talvolta la si utilizza anche solo per rallentare l'attività ritenuta pericolosa: si pensi agli attacchi informatici di cui sono frequentemente vittima le centrarli nucleari iraniane.

infine, l'utilizzo della guerra delle informazioni in uno scenario più prettamente sociale, quando non direttamente personale o *domestico*: gruppi di pressione, *lobbies*, singoli cittadini si servono sempre più della Rete per porre in essere attacchi mirati a siti istituzionali o *blog* privati, così spostando nel contesto digitale il loro attivismo politico.

È oramai chiaro e assodato che il terrorismo internazionale si serve con sempre più frequenza e perizia della Rete e delle tecnologie digitali in generale per porre in essere la propria attività eversiva. L'utilizzo di Internet da parte dei terroristi è volto a perseguire diverse finalità [42]: innanzitutto si cerca di porre in essere una sorta di *psychological warfare*, tentando, così, di fiaccare la resistenza emotiva dell'opinione pubblica del Paese che si intende attaccare diffondendo notizie e filmati che hanno il dichiarato intento di colpire la sensibilità dei singoli cittadini [43]; inoltre, la Rete è un insostituibile strumento pubblicitario e propagandistico, che aumenta esponenzialmente le possibilità di reclutamento di nuovi adepti e di raccolta fondi; Internet è, poi, sicuramente utilizzata per la ricerca di informazioni con riferimento ai futuri, possibili bersagli (cosiddetto *data mining*); infine, le reti telematiche vengono impiegate per condividere le informazioni e per programmare e coordinare l'attività dei vari gruppi sparsi a livello globale.

Questo fenomeno, in evidente tendenza espansiva, richiede un intervento diretto e chiaro da parte delle autorità statali che si trovano a doversi contrapporre anche nel contesto digitale alla minaccia terroristica.

[42] Cfr. G. Ziccardi, *Informatica giuridica* … cit., pp. 245-248.

[43] Si veda ad esempio l'uso che Al Jazeera fa dei video di prigionieri occidentali nelle mani dei terroristi che talvolta vengono resi disponibili sulla Rete.

3.2. *Gli strumenti utilizzati dai governi per contrastare il terrorismo in Rete*

Dopo l'11 settembre lo Stato comincia a rivendicare un ruolo diretto nella gestione delle attività che vengono poste in essere nella Rete e a garantire la sicurezza propria e dei propri cittadini attraverso un'opera di controllo e regolamentazione dell'intero fenomeno. I governi dei vari Paesi hanno così iniziato a elaborare nuove strategie volte a contrastare le attività criminali e, più in particolare, terroristiche che trovano in Internet una potentissima cassa di risonanza. Passiamole di seguito in rassegna [44].

Anzitutto, si assiste all'aumentare dell'importanza di alleanze strategiche nel contesto telematico con soggetti terzi e più in particolare con gli *Internet Service Provider* (ISP). Si parla sempre più spesso di una sorta di *invisible handshake* che porrebbe in relazione, secondo modalità e percorsi non sempre trasparenti, le autorità statali e i vari nodi della Rete (siano essi ISP, appunto, o più semplicemente *content provider*, quali Google, Facebook e i vari *social network*) [45]. L'attività che viene di fatto delegata è quella di sorveglianza, intercettazione, blocco e chiusura dei siti attraverso un fenomeno che sempre più assume le vesti di una sorta di privatizzazione della censura. Questa tendenza è comune a tutti gli Stati, siano essi basati su diritti costituzionalmente garantiti o su regimi più o meno dittatoriali (gli esempi estremi sono evidentemente la Repubblica Popolare Cinese, la Repubblica Islamica dell'Iran, la Repubblica Socialista del Vietnam). L'autonomia degli ISP nei vari ordinamenti statali è direttamente proporzionale alla libertà di cui gode la Rete nei Paesi di riferimento: avremo così in alcuni un controllo esercitato attraverso la previsione di regole di responsabilità che impongono agli ISP soprattutto obblighi di collaborazione *ex post* con le forze del-

[44] Cfr. M. Bettoni, *Terrorismo e Internet: alcune considerazioni giuridiche, politiche e tecnologiche*, in «Ciberspazio e diritto», 2010, p. 231, in particolare pp. 239-246.

[45] Cfr. M.D. Birnhack, N. Elkin-Koren, *The Invisible Handshake: The Reemergence for the State in the Digital Environment*, in «Virginia Journal of Law and Technology» 8 (2003), p. 6.

l'ordine; in altri casi, invece, la pressione sarà più stringente anche perché in tali contesti i nodi della Rete risultano spesso statali o fortemente controllati dalle autorità governative. Il diffondersi di questa strategia sta via via portando a una sorta di delega a soggetti privati del controllo nella Rete di diritti costituzionalmente garantiti e protetti (vedi ad esempio la libertà e la segretezza della corrispondenza, la libertà di manifestazione del pensiero, la libertà di stampa, ecc.).

Una seconda strategia perseguita dalle autorità statali è quella di porre in essere direttamente l'attività di controllo e sorveglianza dei contenuti della Rete. Anche questo tipo di approccio al problema è comune a tutti i Paesi del mondo con intensità, modalità e conseguenze che variano negli ordinamenti giuridici a seconda, come visto sopra, del grado di libertà che in essi è riconosciuto ai consociati. Di qui la tendenza a dotarsi di corpi di polizia specializzati (in Italia la Polizia postale) che cercano di contrastare nel contesto digitale le attività criminali utilizzando gli strumenti che le tecnologie di sorveglianza offrono loro. In questa prospettiva si registra una pericolosa riduzione dello spazio personale del singolo che porta a comprimere fortemente la sua *privacy*.

Altro approccio è, poi, quello caratterizzato dal blocco dell'accesso e dalla censura dei contenuti presenti sulla Rete. Queste sono misure adottate dalle autorità statali al fine di limitare l'accesso a materiale ritenuto illegale. Si persegue la prima (il blocco dell'accesso) allorquando il sito Web sospetto si trovi su un *server* situato all'esterno del territorio nazionale; si impone invece la censura allorquando, invece, la pagina sia posta su un *server* all'interno del territorio nazionale e, di conseguenza, direttamente sanzionabile con l'oscuramento delle informazioni in essa contenuto [46].

Infine, la strategia più comune e socialmente invasiva, perpe-

[46] L'etichetta di *terrorista internazionale* viene quindi associata in maniera più o meno elastica ed estendibile a diverse organizzazioni nazionali e internazionali. Ciò talvolta è utilizzato in maniera strumentale per poter considerare *fuori legge* gruppi che sono, invece, semplicemente in contrasto con la linea governativa (si pensi all'approccio russo con riferimento alle regioni indipendentiste e alla Gran Bretagna con riferimento alle organizzazioni dell'Irlanda del Nord).

trata dalle autorità statali, è quella delle intercettazioni delle comunicazioni private. Essa è stata fortemente potenziata dalla legislazione antiterroristica. Su tale tema si è già detto sopra e non è questo il luogo per dilungarsi troppo. Basti qui ricordare che in realtà si tratta di un fenomeno sicuramente non nuovo ma che, a causa della rivoluzione informatica, ha cominciato a presentare peculiari criticità: la digitalizzazione e la sempre più capillare diffusione di Internet hanno, infatti, determinato una semplificazione tecnologica dell'attività di intercettazione, diminuendone di conseguenza i costi. Ciò ha portato a un aumento sia dei soggetti in grado di svolgere l'attività suddetta che dei *bersagli* dell'intercettazione stessa. All'aumento delle ipotesi e delle modalità di intercettazione e archiviazione si è accompagnato un allentamento dei limiti imposti dai vari ordinamenti a garanzia dei singoli [47].

3.3. Dati relativi al traffico e 'data retention'

In tale ambito merita un approfondimento la tematica relativa alla ritenzione dei dati relativi al traffico per finalità di contrasto alla criminalità e al terrorismo: la cosiddetta *data retention* [48].

Cominciamo con alcune definizioni: l'art. 4, co. 2, lett h, *Codice Privacy* afferma che i dati relativi al traffico sono quelli sottoposti *a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione*. Si tratta, quindi, dei dati relativi alla fonte e alla destinazione, alla data, all'ora, alla durata della connessione e a quelli concernenti la relativa fatturazione. L'art. 123 del *Codice* prevede la regola relativa alla loro *riten-*

[47] Cfr. M. Bettoni, *Terrorismo e Internet* … cit., p. 244.

[48] Per approfondimenti cfr. S. Aterno, A. Cisterna, *Il legislatore interviene ancora sul* data retention*, ma non è finita*, in «Diritto penale e processo» 2009, p. 282; A. Stracuzzi, Data retention: *il faticoso percorso dell'art 132* Codice Privacy *nella disciplina della conservazione dei dati di traffico*, in «Diritto informazione e informatica» 2008, p. 585; F. Bignami, *Protecting Privacy against the Police in the European Union: the Data Retention Directive*, in «Chicago Journal of International Law» 2007; Duke Science, Technology & Innovation Paper No. 13, reperibile all'URL: http://ssrn.com/abstract = 955261.

zione: essi devono essere cancellati o resi anonimi quando non più necessari ai fini della trasmissione della comunicazione elettronica. Tale limite incontra, però, delle eccezioni che si fondano sull'esigenza di contemperare la tutela del diritto all'oblio nei confronti delle informazioni relative all'utilizzo di una comunicazione elettronica con l'esigenza di conservare una documentazione la più possibile dettagliata e precisa con riferimento al traffico telefonico e telematico: ciò al fine di permettere al fruitore stesso di controllare l'esattezza delle pretese di pagamento del fornitore. È, appunto, l'art. 123, co. 2, a garantire la possibilità di conservare i dati necessari per la fatturazione e indispensabili per pretendere il pagamento o per dimostrare la veridicità delle somme addebitate (in un limite di tempo comunque non eccedente i sei mesi). Il trattamento di questi dati è comunque sottoposto al vincolo della relativa finalità, la quale consiste unicamente nella fatturazione e nei pagamenti di interconnessione.

Veniamo alla *data retention*, che rappresenta un'ulteriore deroga al regime ordinario di ritenzione dei dati relativi al traffico motivata dalla volontà di accertare e reprimere specifiche fattispecie criminose.

La questione ha incontrato notevole interesse anche e soprattutto in ambito comunitario. Dopo lunghi e accesi dibattiti sul tema, si decise di dare finalmente il via a una direttiva che, negli intenti dei promotori, fosse condivisa e accettata. Veniva, così, emanata la dir. 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE. Essa prevede l'obbligo per gli operatori telefonici e gli ISP 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 e 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.

La direttiva trova chiaramente origine nel clima di incertezza successivo agli attentati di Londra del luglio del 2005 e in essa hanno prevalso le ragioni di *sicurezza a ogni costo*. Molteplici sono, infatti, gli aspetti di criticità che la nuova disciplina presenta. Innanzitutto, i costi dell'operazione ricadono interamente sugli operatori telefonici e di Internet (e, quindi, di rimando sugli utenti): non è, infatti, prevista alcuna forma di rimborso per le spese 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 ad altri, diversi, reati. Infine, è tutta da dimostrare la reale efficacia di questo tipo di strumenti di contrasto a fronte di una così palese compressione della *privacy* dei singoli.

La regola europea è stata recepita nell'ordinamento giuridico italiano dal d. lgs. 30 maggio 2008, n. 109, *Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, il quale, oltre a novellare gli articoli del *Codice Privacy* dedicati alla *data retention*, fornisce in maniera sicuramente più puntuale rispetto al passato, la descrizione della categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica (art. 3, d. lgs. 109/2008) [49]. Il nuovo articolo 132, co. 1, *Codice Privacy* prevede, così, che i dati relativi al traffico telefonico sono

> *conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni,*

[49] Si veda anche il Provvedimento a carattere generale del Garante per la protezione dei dati personali *Sicurezza dei dati di traffico e telefonico e telematico – 17 gennaio 2008*.

sono conservati dal fornitore per dodici mesi. [50]

I dati relativi alle chiamate senza risposta sono, invece, conservati per soli trenta giorni (art. 132, co. 1-bis *Codice Privacy*). I dati possono essere acquisiti presso il fornitore (ISP) solamente tramite decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, co. 3, *Codice Privacy*) [51].

4. CONCLUSIONI

Nel 1994 l'*Internet Architecture Board* (IAB), un'organizzazione istituita sia come commissione dell'*Internet Engineering Task Force* (IEFT) che come organo consultivo dell'*Internet Society*, presentò un *report* dal titolo *Security in the Internet Architecture*, nel quale si metteva in luce come Internet necessitasse di un maggiore livello di sicurezza.

[50] Precedentemente si prevedeva invece la possibilità di ritenere i dati relativi al traffico telematico per sei mesi. Tale periodo risultava, poi, estendibile di ulteriori ventiquattro e sei mesi, esclusi sempre i dati relativi al contenuto delle comunicazioni, *per ulteriori sei mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici*.

[51] Da ultimo, l'art. 132 è stato novellato con l'inserimento del comma 4-*ter* a opera dell'art. 10 della l. 18 marzo 2008, n. 48 contenente la ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001. Ivi si prevede che: *Il Ministro dell'Interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati*.

Tra le aree più importanti in cui si rendeva opportuno intervenire vi erano la sicurezza delle infrastrutture di rete nei confronti di attività di monitoraggio non autorizzate, il controllo del traffico di rete e la sicurezza delle comunicazioni tra utenti, mediante l'utilizzo di sistemi di autenticazione e di criptazione [52].

Nel tempo il numero degli attacchi alla rete delle reti, e ai sistemi collegati a essa, è cresciuto caratterizzandosi per un sempre maggior livello di complessità: gli attacchi sono diventati via via più seriali e automatizzati, aumentando così la loro capacità di provocare gravi danni.

Questo incremento è coinciso con una progressione nell'utilizzo della Rete e con l'aumento nella complessità dei protocolli e delle applicazioni. Gli utenti, dal canto loro, hanno cominciato a fare affidamento sulla sicurezza di Internet, e-mail, Web e applicazioni a questo collegate. Ciò ha richiesto un maggior sforzo per implementare tecnologie e strumenti atti a contrastare gli attacchi crescenti.

Da un punto di vista strettamente informatico esistono diversi approcci alla sicurezza [53]. Tra le numerose proposte per affrontare il problema troviamo delle soluzioni più prettamente *ingegneristiche*: queste propongono di ridisegnare i sistemi operativi al fine di renderli più sicuri; altre opzioni suggeriscono, invece, di modificare le metodologie di programmazione. Altri approcci ancora si concentrano sulla necessità di modificare l'hardware stesso dei personal computer. L'ultimo approdo è qui rappresentato dal cosiddetto *Trusted Computing* (TC), tecnologia innovativa derivata dai lavori svolti dal *Trusted Computing Group* (TCG) [54]. Tale progetto è teso a

[52] Il documento è reperibile all'URL: http://datatracker. ietf.org/doc/rfc1636/.

[53] A proposito di tale argomento cfr. in generale S. Schoen, *Trusted Computing: Promise and Risk*, reperibile all'URL: http://www.eff.org/Infrastructure/trusted_ computing/20031001_tc.php.

[54] Il nucleo iniziale del *Trusted Computing* risiedeva nella *Trusted Computing Platform Alliance* (TCPA) fondata da Compaq, HP, IBM, Intel e Microsoft. I compiti di quest'ultima sono stati, poi, assorbiti e ampliati dal *Trusted Computing Group* (TCG), un'organizzazione no-profit promossa da sette imprese (le cinque fondatrici della TCPA oltre a Sony Corporation e Sun Microsystems). Si veda il sito Web: http://www.trustedcomputinggroup.org. Per approfondimenti, R. Caso, *Un* rapporto di minoranza*: elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine*

sviluppare, definire e promuovere specifiche per ottenere standard aperti di hardware: l'obiettivo è quello di creare ambienti informatici più sicuri di quelli attuali senza per questo compromettere l'integrità funzionale di siffatti sistemi, della *privacy* e dei diritti individuali. Tutto questo dovrebbe realizzarsi promuovendo la costruzione di sistemi hardware e software non abilitati a determinate funzioni, che siano in potenza 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 [55]. La logica TC parte dall'idea che la sicurezza di un computer possa essere messa a rischio dal proprietario o dall'utente del computer stesso. Ciò si basa su due fondamenti: il primo è dato dalla limitazione preventiva (e fisica) delle funzionalità del sistema informatico; il secondo risiede nella dislocazione del controllo del sistema informatico dall'utente finale verso i soggetti che producono l'hardware e il software, nonché verso quelli che sono deputati a sorvegliare – mediante Internet – che siano rispettate le limitazioni di funzionalità imposte dal produttore. L'approccio ora descritto è stato, però, oggetto di numerose e accese critiche [56].

---

del Trusted Computing, in R. Caso (a cura), *Sicurezza informatica: regole e prassi*. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005, Cedam, Padova 2006, pp. 4 ss.

[55] Il computer rappresenta sempre più una proiezione della nostra esistenza, delle nostre faccende quotidiane, delle nostre emozioni. Questo tipo di approccio pone due problemi di fondo, estremamente rilevanti su un piano giuridico. Innanzitutto, il processo di elaborazione degli standard tecnologici dell'architettura TC, così come la sicurezza di essa, è riposto completamente nelle mani di privati, i quali non necessariamente agiscono in base a processi trasparenti e democratici. Inoltre, la sicurezza dipende dall'architettura informatica la quale incorpora alcune regole implicite, che si connotano per rigidità, predeterminatezza e potenziale infallibilità; diversamente dal diritto che, invece, è per sua natura caratterizzato da regole elastiche, verificabili solo *ex post* e sempre potenzialmente fallibili. Sul punto cfr. R. Caso, *Un* rapporto di minoranza*: elogio dell'insicurezza informatica* … cit., *passim.*

[56] Si vedano, fra tutte, le osservazioni sollevate da R. Anderson, *'Trusted Computing' Frequently Asked Question*, Versione 1. 1 agosto 2003, reperibile all'URL: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html. Nell'Unione Europea sono stati avanzati dubbi sulla compatibilità delle architetture TC con il quadro normativo derivante dalle già citate direttive 95/46/CE e 2002/58/CE. La discussione che ne è nata ha susci-

Il diritto gioca anche in tale contesto un ruolo fondamentale. Esso è il solo strumento in grado di governare la complessità e le contraddizioni di un mondo digitale che sempre più si confonde con quello reale e di indicare la via per giungere a soluzioni che garantiscano un corretto bilanciamento tra gli interessi coinvolti. La minaccia, d'altronde, è il realizzarsi di uno scenario simile a quello che così magistralmente descriveva Orwell nel suo profetico capolavoro:

> *Si doveva vivere (o meglio si viveva, per abitudine che era diventata, infine, istinto) tenendo presente che qualsiasi suono prodotto sarebbe stato udito, e che, a meno di essere al buio, ogni movimento sarebbe stato visto.* [57]

tato 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*):* cfr. 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, reperible all'URL: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_en. pdf.

[57] G. Orwell (1949), *1984*, Mondadori, Milano 2000.