Agenti software e sicurezza informatica

Versione 1.0 – maggio 2008

Paolo Guarda

Agenti software e sicurezza informatica

Versione 1.0 maggio 2008

Paolo Guarda[*]

«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»
da "1984" di George ORWELL

1. La sicurezza informatica

La sicurezza informatica assume nei nostri giorni un'importanza primaria.

Si pensi alle infinite questioni relative alla sicurezza e alla gestione di banche dati pubbliche, i record, che contengono un vastissimo numero di dati sensibili: il fatto che oramai questi archivi siano stati trasposti dal supporto cartaceo, che li vincolava alla loro collocazione spaziale, a dei supporti telematici, magari connessi alla rete Internet, crea notevoli problemi circa la loro gestione, organizzazione e sicurezza[1].

Ma la questione della sicurezza informatica non si limita solo a questo. Si pensi, infatti, ai siti e alle banche dati governative o comunque di agenzie ed organismi pubblici deputati alla sicurezza della nazione. La possibilità di tenere segrete le informazioni contenute in questi riservatissimi archivi telematici, costantemente sotto "assedio" da parte di attacchi di pirati informatici sempre più esperti ed "agguerriti", è un problema fortemente sentito ed avvertito dai Governi di tutte le nazioni.

Ha, inoltre, grande rilevanza la necessaria tutela che i privati, intendendo con essi sia i singoli che le società che operano nel campo informatico, debbono vedersi riconosciuta, almeno limitatamente ai loro dati personali, considerato l'attuale contesto storico in cui la propensione a privilegiare questioni di sicurezza pubblica e di interesse

---

[*] Ripubblicazione inalterata di un saggio già pubblicato in G. PASCUZZI (a cura di), *Diritto e tecnologie evolute del commercio elettronico*, Padova, 2004, 315-342. Questa versione 1.0 – maggio 2008 in pdf - Tutti i siti web sono stati consultati l'ultima volta il 10 gennaio 2004.

[1] V. D.J. SOLOVE, *Acces and Aggregation: Public Records, Privacy and the Costitution*, 86 *Minn. L. Rev.* 1137 (2002).

nazionale tende a ridimensionare drasticamente la sfera della prima ritenuta quasi intoccabile[2].

Il punto di equilibrio, il giusto and balance tra l'istanza della sicurezza e quella della riservatezza dev'essere ricercato ad un livello più generale rispetto alla contingenza storica determinata dall'emergenza del terrorismo internazionale, collocandolo nella più ampia tematica del diritto nell'era tecnologica.

La questione su cosa debba essere nascosto e cosa debba essere reso accessibile nella sicurezza informatica merita molta più attenzione di quanta ne abbia ricevuta sinora. Da un lato, la teoria economica preconizza che una maggiore accessibilità al flusso delle informazioni porterà ad un maggior livello di efficienza; infatti noi siamo propensi a credere che Internet dovrebbe lavorare su c.d. standard, dal momento che la "trasparenza" degli standard di comunicazione permette ad ogni interlocutore di connettersi ad ogni altro. Dall'altro lato, tendiamo a credere che i difetti del sistema di sicurezza siano un po' come le informazioni segrete militari: rendere noti i difetti appare quasi come aiutare il nemico a sapere come attaccarci, e sicuramente la risposta corretta non sempre corrisponde a rendere pubblica ogni informazione sulla sicurezza del sistema informatico[3].

La sicurezza informatica non è semplicemente una materia che dovrebbe essere lasciata agli esperti tecnici o solo ai venditori e compratori di software e sistemi di sicurezza, perché vi sono significativi failure suscettibili di emergere a causa di uno sbagliato livello di accessibilità e segretezza. Ci sono, inoltre, anche rischi nel lasciare la decisione nelle sole mani degli esperti di sicurezza che operano nelle organizzazioni governative demandate a risolvere tale problema: sussistono, infatti, fortissimi incentivi e stimoli che inducono a nascondere le informazioni sulla sicurezza informatica.

Il tema della trasparenza o segretezza è stato centrale in molti dei dibattiti che hanno avuto come tema Internet e le sue problematiche: utilizzazione libera contro forti copyrights; vasta diffusione delle informazioni personali contro la protezione della ; software contro software di proprietà. Internet, in parte, è un grande motore per l' perché consente di condividere a basso costo informazioni in moltissime maniere tra un numero enorme di persone. Determinare un corretto livello di accessibilità ed apertura nella sicurezza informatica è di cruciale importanza per evitare che l'incomparabile utilità di Internet venga gravemente compromessa. In un modo o nell'altro, per mantenere i vantaggi derivanti da Internet per l'educazione, il commercio, la democrazia, e tutte le altre sue possibili applicazioni, noi dobbiamo trovare il modo di implementare la tecnologia, le leggi, e le istituzioni che siano in grado di realizzare la giusta combinazione tra ed nella sicurezza informatica.

[2] V. K. BASHO, *Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 *Cal. L. Rev.* 1507 (2001); T.R. DAUB, *Surfing the net safely and smoothly: a new standard for protecting personal information from harmful and discriminatory waves*, 79 *Wash. U. L. Rev.* 913 (2001); T. FRANKEL, *Trusting and Non-Trusting on the Internet*, 81 *B. U. L. Rev.* 457 (2001).

[3] V. P.P. SWIRE, *What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory*, in www.arxiv.org/abs/cs.CY/0109089; H. NISSENBAUM, *Securing Trust Online: Wisdom or Oxymoron*, 81 *B. U. L. Rev.* 635 (2001).

Tutto questo va ora vagliato alla luce di quanto successo l'11 settembre 2001 negli Stati Uniti[4]: tale avvenimento ha completamente rivoluzionato l'attività di *intelligence* delle autorità americane, ampliandone le capacità e quindi, di converso, acuendo il contrasto tra sicurezza e *privacy*, soprattutto nel settore informatico.[5] I catastrofici atti terroristici dell'11 settembre, messi a segno da un'organizzazione che si era occultamente insediata ed efficacemente ramificata nel tessuto della società americana, hanno costretto le autorità statunitensi a potenziare, sia sul piano normativo che su quello operativo, l'intero apparato dei servizi di sicurezza, con la conseguenza di obbligare il legislatore e l'opinione pubblica a riconsiderare la sfera personale dei diritti del cittadino messa a rischio dall'incremento dei poteri di sorveglianza in capo agli organi esecutivi dello Stato[6].

Crescente importanza hanno, inoltre, assunto gli studi riguardanti l'impatto sulla società e sul tradizionale right to privacy delle nuove tecnologie applicate nell'ambito

---

[4] Cfr. L.K. COMFORT, *Managing Bureaucracies and Administrative Systems in the Aftermath of September 11Rethinking Security: Organizational Fragility in Extreme Events*, 62 Suppl.1 *P.A.R.* (2002); D. CARR, *The Futility of "Homeland Defense". Don't even try to close the holes in a country, and a society, designed to be porous*, in http://foi.missouri.edu/homelandsecurity/futility.html; R.A. MANN, B.S. ROBERTS, *CyberLaw: A Brave New World*, 106 *Dick. L. Rev.* 305 (2001).

[5] Si veda D. CARPENTER, *Keeping Secrets*, 86 *Minn. L. Rev.*, 1097 (2002); M. ROTENMBERG, *Privacy and Security After September 11*, 77 *Minn. L. Rev.* 1115 (2002); D.J. SOLOVE, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 *Stanf. L. Rev.* 1939 (2001); P. SCHWARTZ, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, *Wiss. L. Rev.* 743 (2000); R. LEGER, *'National security' puts citizens at risk*, in http://www.springfieldnews-leader.com/opinions/leger072102.html**;** *Nothing Has Changed. Therefore Anything Must Change*, in http://www.notbored.org/change.html.

[6] La risposta immediata del Congresso americano agli attacchi dell'11 settembre, come già ricordato sopra, fu l'*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 - Pub. L. No. 107-56, 115 Stat. 272 (2001)), promulgato dal Presidente Bush il 26 ottobre 2001. La legge contiene 1016 sezioni e apporta modifiche ad oltre 15 differenti statute precedenti (si veda EFF Analysis of USA PATRIOT Act, in http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html; M.T. MCCARHTY, *Usa Patriot Act*, 39 *Harv. J. on Leg.* 435 (2002); B. PARELLA, *Entra in vigore l'USA Patriot Act*, in http://www.apogeonline.com/webzine/2001/10/30/13/200110301301; S.H. RACKOW, *How the USA PATRIOT Act Will Permit Governmental Infringment upon the Primary of Americans in the Name of "Intelligence" Investigations*, 150 *U. Pa. L. Rev.* 1651 (2002). Tale legge ha suscitato attenzione e forti critiche soprattutto in riferimento alle disposizioni che autorizzano nuove e piú invasive forme di sorveglianza.

Il 25 novembre 2002 venne emanato l'*Homeland Security Act* (Pub. L. No 107-296, 116 Stat. 2135 (2002)). Tale legge, che ha come scopo quello di rafforzare e ristrutturare l'azione del Governo Federale per meglio contrastare gli attentati alla sicurezza interna, crea una nuova Agenzia governativa, il *Department of Homeland Security*, che ha come missione primaria quella di aiutare a prevenire gli atti criminosi, proteggere gli obiettivi sensibili, rispondere agli attacchi terroristici sul suolo americano (si vedano G.W. BUSH, *Homeland Security Act of 2002*, in www.foi.missouri.edu/homelandsecurity/hsact2002.html; P. SWIRE, "*Homeland Security Act": No Privacy Safeguards*, in http://lists.insecure.org/lists/politech/2002/Jun/0090.html; S. COHEN, W. EIMICKE, J. HORAN, *Homeland Security: The State and Local CrucibleCatastrophe and the Public Service: A Case Study of the Government Response to the Destruction of the World Trade Center Authors*, 62 Suppl. *P.A.R.* (2002); *New Provisions in the Homeland Security Act*, in http://www.house.gov/hyde/prov.htm. Cfr. anche K. ANDERSON, *Homeland Security and Privacy*, in http://www.probe.org/docs/c-homeland2.html; J. MINTZ, *Homeland Agency Launch. Bush signs Bill to Combine Federal Security Functions*, in http://foi.missouri.edu/homelandsecurity/homelandagency.html).

delle intercettazioni telefoniche e telematiche, ed in generale nell'attività investigativa di intelligence[7]. La possibilità di utilizzare sistemi di intercettazione telematica 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 e prese di posizione di quanti denunciano l'eccessivo carattere intrusivo di tali strumenti e i possibili abusi che la loro implementazione presenta.

Lo stesso concetto di sicurezza informatica assume una rilevanza importantissima soprattutto a riguardo di cosa debba essere tenuto nascosto e cosa invece liberamente reso accessibile nell'ambito della computer security, in un mondo, quale quello di Internet, che fa della facilità di comunicazione e della libertà nell'accesso e scambio dei dati, i principi primi che regolano la "comunità telematica"[8]. I concetti di closedness e openness necessitano di una ridefinizione e regolamentazione affinché l'attuale esigenza di sicurezza non si traduca in una posizione oscurantistica nei confronti dei "prodotti" culturali in senso lato, per i quali Internet rappresenta la nuova frontiera della ricerca e dello sviluppo intellettuale dell'uomo.

In tutto questo irrompe ora la tematica degli agenti software, definibili come programmi informatici dotati di autonomia, che operano in ambienti complessi. La loro utilizzazione ed implementazione, quali strumenti a difesa della sicurezza informatica, apre prospettive giuridiche di ricerca completamente nuove[9]. Questi software sono caratterizzati da alcune qualità fondamentali: l'autonomia (operano senza un diretto intervento umano), l'apprendimento induttivo, la capacità di interagire con altri agenti e operatori umani attraverso alcuni tipi di linguaggio di comunicazione, il fatto di esser goal oriented (hanno cioè uno scopo predeterminato), la mobilità, la razionalità[10].

---

[7] V. D. BANISAR, S. DAVIES, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 *J. Marshall J. Computer & Info L. 1* 11 (1999); M.G. YOUNG, *What Big Eyes and Ears You Havel: A New Regime for Covert Governmental Surveillance*, 70 *Fordham L. Rev.* 1017 (2001) o in http://www.google.it/search?q=cache:9nDSRQts_CgC:law.shu.edu/faculty/fulltime_faculty/soloveda/DatabasePrivacy%2520FINAL.pdf+%22Privacy+and+Power:+Computer+Databases+and+Metaphors+for+Information+Privacy%22&hl=it&ie=UTF-8; *Q&A: Trusted Computing and the Privacy/Security Debate After September 11*, in http://www.microsoft.com/PressPass/features/2001/nov01/11-05trustedcomputing.asp.

[8] In N. NEGROPONTE, *Essere digitali*, Milano, Sperling&Kupfer editori, 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".

[9] V. G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto*, *Contratto e impresa*, 2002, 465; ID., *L'intenzionalità dei sistemi informatici e il diritto*, *Riv. Trim. Dir. e Proc. Civ.*, 2003, 23; ID., *Gli agenti software e la disciplina degli strumenti cognitivi*, *Dir. inf.*, 2003, 55; S.J. RUSSEL, P. NORVIG, *Artificial Intelligence. A Modern Approach*, Englewood Cliffs (NJ), Prentice Hall, 1995; G. WEISS, *Multiagent System. A Modern Approach to Distributed Artificial Intelligence*, Cambridge (Mass), MIT, 1999; M. WOOLRIDGE, *Reasoning about Rational Agents*, Cambridge (Mass), MIT, 2000; B. BURG, *Agents in the World of Active Web-Services*, in http://www.hpl.hp.com/org/stl/maas/docs/HPL-2001-295.pdf; L. LESSIG, *Randolph W. Thrower symposium: Legal issues in cyberspace: hazards on the information superhighway: Article: riding the Constitution in Cyberspace*, 45 *Emory L. J.* 869 (1996); M. ADLER, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Searc*, 105 *Yale L. J.* 1093 (1996).

[10] V. B. HERMANS, *Intelligent Software Agents on the Internet*, in http://www.firstmonday.dk/issues/issue2_3/ch_123/index.html; L. FONER, *What's an Agent, Anyway? A Sociological Case Study*, in http://foner.www.media.mit.edu/people/foner/Julia/Julia.html; J. JANSEN, *Using an Intelligent Agent to Enhance Search Engine Performance*, in

Alcuni dei software che vengono utilizzati nella sicurezza informatica possiedono queste caratteristiche, o quanto meno alcune di esse[11], e ciò li rende peculiari e, in un certo qual senso, unici rispetto agli strumenti di intercettazione telematica e di difesa della riservatezza che venivano impiegati in precedenza. La capacità di apprendere induttivamente, la mobilità nella rete, l'autonomia nell'agire, sono attributi che rendono questi nuovi programmi altamente efficienti da un punto di vista di lotta alla criminalità e salvaguardia della sicurezza pubblica, e che, sul versante della tutela dei propri dati e della propria riservatezza garantiscono una difesa specifica agli interessi del singolo utente. Il loro utilizzo indiscriminato, però, può condurre a forme di controllo sociale con modalità e caratteristiche, in un contesto poi non cosí futuribile, che mai prima d'ora si sarebbe potuto concepire: l'elevato numero di dati controllabili e catalogabili e la notevole facilità con cui tali operazioni possono essere svolte, acuisce la difficoltà di trovare dei giusti contemperamenti tra interessi di carattere generale e interessi del singolo.

2. Tecnologia e sicurezza

Quando si tratta di sicurezza nella rete, vari e diversi sono i software che vengono in considerazione: alcuni sono utilizzati dalle agenzie di intelligence, altri sono delle vere e proprie minacce alla riservatezza, e soprattutto al controllo dei propri dati da parte dei cittadini, altri ancora fanno parte delle utility di ogni utente della rete, vedi i filtri anti-spam. Ma andiamo ora di seguito a dare esempi di tutto ciò.

La sicurezza informatica è stata profondamente segnata dall'implementazione, da parte delle autorità americane, di nuovi strumenti di investigazione telematica che presentano notevoli problemi in quanto fortemente invasivi delle libertà e della riservatezza dei cittadini[12]. Nel luglio del 2000 l'FBI ha presentato "Carnivore"[13]: si

---

http://firstmonday.dk/issues/issue2_3/jansen/index.html; T. BERNERS-LEE, J. HENDLER, O. LASSILA, *The Semantic Web, A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities*, in http://www.scientificamerican.com/print_version.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21.

[11] Non vi è ancora consenso su quali siano le caratteristiche fondamentali di un agente software e nemmeno di quale sia la relativa importanza di ognuna di queste. V. HERMANS, .

[12] V. M.D. BIRNHACK, N. ELKIN-KOREN, *The Invisibile Handshake: The Reemergence fo the State in the Digital Environment*, 8 *Va. J. L.* Draft (2003), dove gli autori sostengono che i tragici eventi dell'11 settembre hanno rafforzato il trend in atto in quanto hanno cambiato il modo in cui le persone considerano lo Stato e le sue responsabilità e hanno rimarcato il suo tradizionale ruolo di custode della sicurezza pubblica; v. anche J. IPPOLITO, *Don't Blame the Internet*, in http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A43828-2001Sep29&notFound=true; L.M. BOWMAN, *FBI digs deeper into the Web*, in http://news.com.com/2100-1023-933183.html?tag=bplst; J.A. SEGURA, *Is Carnivore Devouring Your Privacy?*, 75 *Southern Cal. L. Rev.* 231 (2001).

[13] V. i contributi di Swire, *What Should be Hidden and Open in Computer Security…*,cit. 50-51; D.M. Kerr, *Internet and Data Interception Capabilities Developed by FBIFourth Amendment Issues Raised by the FBI's "Carnivore" Program. Hearing before the House Committee on the Judiciary, Subcommittee on the Constitution, 106th Cong., 1st session*, in www.fbi.gov/congress/congress00/kerr072400.htm; A. ETZIONI, *Implications of Select New Technolgies for Individual Rights and Publcíic Safety*, 15 *Harv. J. of L. & Tech.* (2002), disponibile anche su www.jolt.law.harvard.edu/articles/Etzioni.doc; 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); M.T.

tratta di un programma per computer in grado di "catturare" messaggi e-mail di persone sospette o di "tracciare" messaggi spediti verso, e da, il suo indirizzo di posta elettronica. Carnivore ha un filtro che può essere impostato per passare in rassegna diversi "pacchetti digitali" per specifiche stringhe di testo o con ben definiti target di messaggi provenienti da un determinato computer o indirizzo e-mail. Il programma può lavorare secondo due differenti impostazioni: *pen* o *full*. In *pen mode*, esso intercetterà solo le informazioni relative agli indirizzi, che includono l'indirizzo e-mail del mittente, del destinatario e l'oggetto: tale impostazione risulta utile per le pubbliche autorità anche qualora il contenuto del messaggio non possa essere letto a causa della presenza di un sistema di criptazione, perché notevoli vantaggi possono comunque essere ottenuti dall'analisi degli indirizzi. In *full mode*, invece, Carnivore intercetterà l'intero contenuto del messaggio.

Il programma non è abilitato per trasmettere informazioni: i dati che vengono raccolti sono salvati su un disco fisso rimuovibile che è sostituito con frequenza da un agente. Questa caratteristica fa sì che Carnivore non possa essere contaminato da alcuna rete informatica alla quale è collegato.

Una volta che i "pacchetti" desiderati sono stati raccolti e successivamente salvati, l'FBI deve allora ricostruirli per successive analisi. Tale procedura richiede due altri programmi: il Pakteer ed il Coolminer. Il primo ricostruisce la sessione TCP (Control Protocol) dagli IP dei "pacchetti", di seguito salvati in maniera tale da poter essere letti dal Coolminer. Questo è un programma di lettura che permette all'FBI di visualizzare la sessione TCP nuovamente ricostruita. In aggiunta, tale ultimo programma, tramite una specifica impostazione, permette all'FBI di selezionare e ridurre i dati che si vogliono visualizzare.

Poiché è predisposto per registrare le sole informazioni che sono raccolte attraverso il filtro, l'ordine del giudice dovrà appunto determinare il "settaggio" di questo per meglio adattarlo alle circostanze del caso e alle esigenze normative. Nonostante l'implementazione di Carnivore, il Governo americano era stato notevolmente ostacolato dall'impossibilità di decifrare un numero di messaggi sempre crescente a causa della diffusione della c.d. "criptazione forte"[14]. La crittografia è una

---

HEFLIN, *Who's Afraid of the Big Bad Wolf: Why the Fear of Carnivore Is an Irrational Product of the Digital Age*, 107 *Dick. L. Rev.* 343 (2002); G.S. DUNHAM, *Carnivore, the FBI's e-mail surveillance system: devouring criminals, not privacy*, 54 *Federal Comm. L. J.* 25 (2002); S.D. HELLUMS, *Bits and bytes: the Carnivore iniative and the search and seizure of electronic mail*, 10 *Wm. & Mary Bill of Rts. J.* 827 (2002); G.A. NORTH, *Carnivore in cyberspace: extending the Electronic Communications Privacy Act's framework to Carnivore surveillance*, 28 *Rutgers Comp. & Tech. L. J.* 155 (2002)**;** P.J. GEORGITON, *The FBI's Carnivore: how federal agents may be viewing your personal e-mail and why there is nothing you can do about it*, 62 *Ohio St. L. J.* 1831 (2001); M.M.J. GRIER, *Criminal procedure: the software formerly known as "Carnivore": when does e-mail surveillance encroach upon a reasonable expectation of privacy?*, 52 *South Carolina L. Rev.* 875 (2001); T.R. MCCARTHY, *Don't fear Carnivore: it won't devour individual privacy*, 66 *Miss. L. Rev.* 27 (2001).

[14] Con terminologia anglosassone si parla di "encryption". V. SWIRE, *What Should be Hidden and Open in Computer Security…*,cit., 11-13; ETZIONI, *Implications of Select New Technolgies for Individual Rights and Publcíic Safety*, 11-12; A.M. FROOMKIN, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, in *U. Chi. L.l Forum* 15 (1996); 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); D.H. KAYE, *Encryption source code and the First*

scienza che utilizza algoritmi matematici per criptare e decriptare dei dati, dando, cosí, la possibilità di immagazzinare informazioni o trasmetterle in maniera sicura attraverso reti per loro stessa natura insicure, quali Internet. Un algoritmo crittografico è una funzione matematica nel processo di criptazione e decriptazione; esso lavora in combinazione con una chiave (una parola, un numero o una frase) per criptare il testo. La sicurezza dei dati così criptati dipende da due cose: la forza dell'algoritmo crittografico e la segretezza della chiave. I software che usano la c.d. "criptazione forte" sono facilmente disponibili sul mercato a basso costo. Nonostante gli ordini delle corti, tale sistema di scrittura cifrata ha frustrato l'attività investigativa in un sempre crescente numero di casi.

Per ovviare a tale inconveniente, l'FBI ha sviluppato da tempo dei software detti "Logger System" (KLS)[15], che una volta installati fisicamente sul pc del sospetto, usano un dispositivo di "*keystroke capture*" per registrare le chiavi di accesso nel momento in cui sono digitate sul computer. 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[16].

Nel novembre del 2001, l'FBI ha fatto sapere di aver sviluppato un tipo di tecnologia, ad agenti software, che risulta essere meno invasiva, da un punto di vista fisico, in quanto permette di introdurre il software su di un computer senza installare fisicamente alcun dispositivo. Tale software è il c.d. "Lantern"[17], un tipico *trojan*, cioè un programma che consente l'accesso al computer altrui, da parte di un altro utente collegato in rete, composto da due file, uno client ed uno server: il file server è un programma eseguibile, che una volta lanciato in esecuzione si installerà in maniera nascosta sul computer ed aprirà le porte a chiunque possegga un client equivalente al server[18]. Viene spedito attraverso Internet, per esempio via e-mail, e si auto-installa sul computer da sorvegliare, cominciando a registrare le chiavi digitate su quel computer e a spedire le informazioni raccolte all'FBI, mentre il sospetto è connesso ad Internet. Il tipo di informazioni che un tale tipo di 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

---

Amendement, 40 *Jurimetrics J.* 444 (2000); A.C. HANSEN, *Decrypting encryption*, 26 *Legal Times* 33 (2003); A. ROSSATO, *Firma digitale e documento informatico*, tratto dalla tesi di dottorato.

[15] V. ETZIONI, *Implications of Select New Technolgies for Individual Rights and Publcíic Safety*, cit., 19-20; B. SULLIVAN, *FBI Software cracks encryption wall*, in http://www.msnbc.com/news/660096.asp?cp1=1; J. LEYDEN, *AV vendors split over FBI Trojan snoops*, in http://www.theregister.co.uk/content/55/23057.html; M. SPOSATO, *FBI's Magic Lantern*, in http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=25471.

[16] Tra l'altro, l'intercettazione di comunicazioni elettroniche richiederebbe un ordine (order) di intercettazione che è piú difficile da ottenere rispetto ad un mandato (warrant). Si veda 18 U.S.C. §§ 3122-3123, 2516.

[17] Si v. ETZIONI, *Implications of Select New Technolgies for Individual Rights and Publcíic Safety*, cit., 19-20; C. WOO, M. SO, *The Case for Magic Lantern: September 11 highlights the need for increased surveillance*, 15 *Harv. J. of Law & Technology* 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 *The John Marshall J. of Computer & Information L.* 287 (2002).

[18] Una volta spedito dall'FBI, per essere efficace lantern rimane nascosto sul computer su cui è stato spedito. Ovviamente il suo utilizzo sarebbe fortemente agevolato se i produttori di software anti-virus predisponessero i loro programmi in maniera tale da non rilevare lantern.

governative per decriptare i sistemi di "criptazione forte" utilizzati dai criminali e dai terroristi per nascondere le loro informazioni.

Le caratteristiche fondamentali che fanno di questo software un agente sono: l'autonomia, in quanto, una volta lanciato, esso agisce in maniera indipendente dall'utente, in questo caso l'agente di polizia o i servizi di intelligence, ma soprattutto la mobilità[19], in quanto è in grado di muoversi nella rete senza che il sospettato se ne renda conto. Tali peculiarità fanno sì che l'utilizzo di questo software da parte dell'FBI, e di chiunque altro se ne serva, sia non solo fondamentale per la maggior parte delle operazioni di intercettazione telematica, nell'ottica della lotta ad una criminalità organizzata e soprattutto ad un terrorismo che sempre pi˚ pianificano i loro progetti criminosi on-line, ma risulti anche difficilmente rilevabile dai sospettati, soggetti a tale tipo di investigazione e sia quindi potenzialmente lesiva della riservatezza e in generale dei diritti costituzionali dei soggetti.

Sulla strada dell'implementazione di nuovi tipi di tecnologie ad agenti, il DARPA (Defense Advanced Research Projects Agency) sta sviluppando un software, chiamato "Information Awareness" (TIA)[20] che darà la possibilità agli analisti delle agenzie di investigazione impegnate nella lotta al terrorismo di comparare ed esaminare praticamente la totalità dei database. Questo strumento non sarà dotato di un suo specifico archivio, bensì sarà strutturato in maniera tale da riconoscere i formati di tutti i database presenti sulla rete e di tradurre le ricerche, tutto questo grazie ad una interfaccia software: ciò imprimerà una notevole accelerazione alle operazioni di contrasto al terrorismo internazionale fornendo in tempi brevissimi, nel linguaggio proprio di colui che compie la ricerca, tutte le informazioni disponibili sui soggetti sospetti. Tale tipo di tecnologia ad agenti software avrà tre diverse caratteristiche: sarà dotata di avanzati strumenti di ausilio all'attività di analisi dei dati[21], di software che permettano la traduzione simultanea dei testi reperiti[22], e di tecnologie adatte alla ricerca dei dati[23] e alla protezione della privacy[24]. Il DARPA sta compiendo studi per l'implementazione di tecnologie maggiormente volte alla tutela della *privacy* e per

[19] La caratteristica della mobilità degli agenti software fa sí che questi siano suddivisibili in tre sotto-categorie: i cd. agent, che semplicemente si muovono in maniera casuale nella rete; i cd. 'agents', che sono piú sofisticati e che ad ogni passo nella rete scelgono il "nodo" su cui muoversi, con preferenza su quelli non ancora esplorati; i cd. 'agents', che usano per decidere i propri movimenti sia l'esperienza da loro accumulata che le conoscenze imparate dagli altri agenti. V. BERNERS-LEE, HENDLER, LASSILA, .

[20] V. R.C. SHELBY, *September 11 and the Immunity of Reform in the U.S. Intelligence Community*, in http://www.darpa.mil/iao/Excerpt.pdf; *FAQ Total Information Awareness (TIA) Program*, in http://www.darpa.mil/iao/TIA_FAQs.pdf; *Report to Congress Regarding the Terrorism Information Awareness Program*, in http://www.darpa.mil/body/tia/tia_report_page.htm; *Defence Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project*, in http://www.darpa.mil/iao/iaotia.pdf.

[21] Il programma *Genoa II*. V. http://www.darpa.mil/iao/GenoaII.htm.

[22] Il programma Translingual Information Detection, Extraction and Summarization (TIDES). V. http://www.darpa.mil/iao/TIDES.htm.

[23] Il programma Evidence Extraction and Link Discovery (EELD). V. http://www.darpa.mil/iao/EELD.htm.

[24] Si veda S. HARRIS, *Tech Insider: Total information unawareness*, in http://www.govexec.com/dailyfed/1102/112002ti.htm; G. EDMONSON, *Defence Dept. backs tracking of personal data. Worries about individuals' privacy dismissed*, in http://seattlepi.nwsource.com/national/96568_defense21.shtml.

questo motivo il *TIA* sarà dotato di un c.d. *audit trail*, accessibile solo agli organi supervisori, particolarmente criptato e reso sicuro contro possibili tentativi di manomissione: con tale strumento sarà possibile individuare gli abusi che potranno esser perpetrati attraverso il suo utilizzo e identificare i responsabili. Inoltre un sistema di auto-analisi dei dati proteggerà i dati anche dopo che questi siano recuperati da un database. Ritroviamo quindi anche in questo software le caratteristiche dell'agente intelligente: esso è, infatti, dotato di una notevole mobilità nella rete, di una elevata capacità di confrontare dati provenienti da più database, ha uno scopo ben determinato, è continuamente attivo nella rete ed è provvisto di funzioni semi-automatiche che imparano il comportamento di un gran numero di utilizzatori del sistema per meglio specificare ed eseguire le ricerche richieste[25].

Esistono, però, anche agenti software che hanno come scopo predeterminato quello di attentare alla privacy degli utenti di Internet. Ultimo, in ordine di tempo, tra questi è il c.d. "Internet content"[26], un piccolissimo software che entra, auto-installandosi segretamente, nelle reti di computer e fornisce una enorme mole di dati digitali. Esso può essere utilizzato per esplorazioni elettroniche, sondaggi, vendite via e-mail, *spamming*, furti elettronici, *cybercrime*, cyber-terrorismo, furto di informazioni riguardanti l'identità e perdite economiche. Sintomi della presenza di un *Active Internet content* sul proprio computer sono: ricezione di mail con il proprio indirizzo, rallentamento nella velocità di elaborazione dei dati ed eccessiva vibrazione dell'hard disk, connessioni esterne non autorizzate, cancellazione di siti web, *instant messaging* e *peer-to-perr* non autorizzati e non voluti, *Trojan horse* inglobati in software per la manutenzione del sistema, re-indirizzamento automatico delle reti IP di destinazione. L'estrema mobilità e la capacità di nascondersi di questo agente software fanno sí che sia anche non rintracciabile dai tradizionali anti-virus, non predisposti alla sua ricerca.

Oltre alle tecnologie complesse che abbiamo avuto modo di analizzare finora, esistono software dotati di simili caratteristiche e peculiarità che aiutano, invece, l'utilizzatore della rete a proteggere i propri dati e a tutelare, in senso lato, la sua riservatezza in Internet[27]. Tali agenti software sono, infatti, previsti per la difesa della *riservatezza* del singolo utente. Tra questi, esempio sicuramente interessante è quello rappresentato dai filtri anti-spam, e più in particolare da quelli che utilizzano sistemi *bayesiani* di filtraggio. Tutti conosciamo il problema della c.d. *junk mail*, messaggi spazzatura che intasano i nostri account di posta elettronica e ci impegnano in

[25]Il Congresso ha deciso di non finanziare più tale progetto viste le numerose critiche che esso aveva sollevato. Ciononostante, progetti compresi formalmente nel TIA continuano ad essere sviluppati da numerose agenzie governative.

[26] *Active eIRM Security Tools Help Detect and Avoid These New Forms of Electronic Assault*, in http://www.quantos-stat.com/crm-news/news37.htm; *A Greater Threat than Software Viruses?*, in http://advisor.com/doc/11501; *Active Internet content a threat: report*, in http://www.theage.com.au/articles/2002/09/20/1032054954409.html; B. WOODS, *Active Internet content Dangerous – Report*, in http://boston.Internet.com/news/article.php/1466341; *A Greater Threat than software Viruses?*, in http://networkingadvisor.com/doc/11501.

[27] Su tale tematica si veda G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2002, 61-66, dove l'Autore sottolinea il fatto che la tecnologia determina sí il verificarsi di nuove situazioni che possono attentare alla riservatezza degli individui, ma predispone anche dei rimedi da utilizzare per la difesa dei propri dati personali, quali le cd. enhancing technologies (PET). Nell'opera si parla infatti de "tecnologia minaccia, la tecnologia protegge".

noiosissime attività di pulizia della nostra casella postale. Le *junk mail* non solo sprecano il nostro tempo, ma anche riempiono velocemente lo spazio che i server hanno per la registrazione dei file, specialmente nei siti di grandi dimensioni con migliaia di utilizzatori che possono avere numerosi doppioni delle stesse[28]. Con il crescere di tale problema, si è resa necessaria l'implementazione di sistemi di filtraggio che fossero in grado di distinguere la c.d. *legitimate mail*, cioè le mail che sicuramente ci riguardano, dalle migliaia di messaggi spazzatura. Una prima generazione di filtri anti-spam semplicemente era basata sul riconoscimento di parole chiave: ciò risultava però altamente inefficace e il più delle volte anche dannoso in quanto si rischiava che venissero cancellati dei messaggi che l'utente, invece, avrebbe desiderato leggere. In una seconda fase si sono utilizzati, ma tutt'ora questi sistemi sono in uso, filtri basati su differenti combinazioni: i c.d. *scoring system*, che si basano su un sistema di punteggi positivi e negativi assegnati ai termini che si rinvengono nella mail che nella sommatoria finale dovrebbero aiutare ad individuare le mail non volute; i c.d. *collaborative filtering*, i quali fanno sí che il computer si connetta a dei database contenenti le "impronte digitali" dei messaggi già individuati come spam; i c.d. *challenge/response*, i quali si basano su di un software che, se arriva un messaggio da qualcuno che non si trova nella rubrica, automaticamente invia un messaggio di risposta contenente una particolare richiesta che permetta di verificare la legittima provenienza della mail comprovandone la "bontà"[29].

Tutti questi sistemi di filtraggio presentano, però, delle lacune e non sempre son in grado di distinguere la posta reale dai messaggi non voluti, o, cosa ancor più grave, a volte possono riconoscere come mail un messaggio invece del tutto legittimo! Per ovviare a tutto questo si è ultimamente cercato di sviluppare un sistema di filtraggio basato su calcoli probabilistici chiamato "Bayesian classifier"[30], meglio conosciuto come *Bayesian classifier*. Questi filtri assegnano delle probabilità a tutti gli elementi che rinvengono in una mail, sia buoni che cattivi: le parole che si rinvengono raramente nelle spam-mail contribuiscono a far decrescere la probabilità quanto quelle "cattive". Ma elemento fondamentale di tale tipo di filtri è la previsione di un algoritmo che permette loro di apprendere induttivamente dal comportamento dell'utente il quale, nella sua attività quotidiana di eliminazione della mail non voluta, istruisce in un certo qual modo il suo filtro anti-spam rendendolo sempre più efficace e soprattutto più

[28] A.E. HAWLEY, *Taking Spam out of you Cyberspace Diet: Common law applied to bulk unsolicited advertising via electronic mail*, 66 *UMKC L. Rev.* 381 (1997).

[29] K.D. SHERWOOD, *Second-Generation Anti-Spam Solutions*, in http://www.overcomeemailoverload.com/advice/AntiSpamTools.html.

[30] M. SAHAMI, S. DUMAIS, D. HECKERMAN, E. HORVITZ, *A Bayesian Approach to Filtering Junk E-Mail*, in ftp://ftp.research.microsoft.com/pub/ejh/junkfilter.pdf; P. GRAHAM, *A plan for Spam*, in http://www.paulgraham.com/spam.html; ID., *Better Bayesian Filtering*, in http://www.paulgraham.com/better.html; ID., *Will Filters Kill Spam*, in http://www.paulgraham.com/wfks.html; ID., *Plan for Spam FAQ*, in http://www.paulgraham.com/spamfaq.html. Per alcuni esempi di filtri bayesiani, v.: www.citeseer.nj.nec.com/sahami98bayesian.html; www.paulgraham.com/paulgraham/index.html; www.interstice.com/drewes/cs676/spam-nn/spam-nn.html; www.citeseer.nj.nec.com/369286.html; www.overcomeemailoverload.com/advice/AntiSpamTools.html.

adeguato alle sue necessità[31]. Esempi di agenti software che sono utilizzati come filtri anti-spam sono: il *Maildrop*, per Linux e Unix; il *Mailfilt*, per Windows, Linux e Unix; lo *Spam Stayer*, per Windows; lo *SpamEater Pro*, per Windows; lo *Spamkiller Made E-Z*, per Windows[32].

Resta da ultimo il dar conto di un'altra tecnologia di cui si è proposta l'implementazione: un sistema di sorveglianza, il c.d. **"**Recognition system", basato sulla possibilità di collocare una serie di camera che hanno la capacità di confrontare in tempo reale le immagini delle persone riprese in ambienti pubblici o privati con database di immagini facciali pre-registrate[33]. Le probabilità che sia un agente software a regolare tale sistema di sorveglianza, magari in stretto contatto ed interconnessione con altri sistemi di intercettazione telematica ed ambientale, si muovono sulla via di quella che viene chiamata "*Active Enviroments*"[34], e cioè della possibilità di interconnettere gli 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.

3. L'esperienza americana

In questo paragrafo si intende valutare l'interazione tra l'utilizzazione degli agenti software nella sicurezza informatica e il contesto giuridico americano, dove già ora troviamo la necessità di armonizzare tali tipi di tecnologie con il substrato legale. Si partirà da un *excursus* delle intercettazioni e si prenderà quindi a modello il Lantern, in quanto ultimo ritrovato nella lotta alla criminalità ed al terrorismo.

Preliminare allo studio dell'evoluzione storica delle tecniche di intercettazione e della normativa prevista in riferimento è l'analisi del IV Emendamento[35] della

[31] I. ANDROUTSOPOULOS, G. PALIOURAS, V. KARKALETSIS, G. SAKKIS, C.D. SPYROPOULOS, P. STAMATOPOULOS, *Learning to Filter Spam E-Mail: A Comparison of a Naïve Bayesian and a Memory-Based Approach*, in http://citeseer.nj.nec.com/cache/papers/cs/17257/ http:zSzzSzwww.di.uoa.grzSz~takiszSzpkdd00.pdf/learning-to-filter-spam.pdf; W.W. COHEN, *Learning Rules that Classify E-Mail*, *Proceedings of the AAAI Spring Symposium on Machine Learning in Information Access*, Stanford, California, 1996; T.M. MITCHELL, *Machine Learning*, McGraw-Hill, 1997.

[32] Per una rapida descrizione di questi filtri si veda www.intelligent-agents.com/Mail_Agents/Filtering/.

[33] Cfr. ROTENMERG, cit. 1121-1122; 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*, in http://dlis.gseis.ucla.edu/people/pagre/bar-code.html; *Face recognition useless for crowd surveillance*, in www.epic.org/privacy/facerecognition; T.C. Greene, *Face recognition useless for crowd surveillance*, in http://www.theregister.co.uk/content/4/21916.html.

[34] X. ALAMAN, E. ANGUIANO, F. CORBACHO, F. GOMEZ, P.A. HAYA, J. MARTINEZ, G. MONTORO, *ODISEA: Active Enviromnments for Intelligent Offices and Homes*, reperibile su http://citeseer.nj.nec.com/; M.H. COHEN, *Design Principles for Intelligent Environments*, *Proceedings of the AAAI Spring Symposium on Intelligent Environments*, 1998.

[35] U.S. CONST. amend. IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause…".

Costituzione americana[36]. 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 ha utilizzato la disposizione costituzionale, alla luce degli interessi protetti da essa, per decidere quali e con quali modalità gli strumenti governativi potessero essere impiegati per contrastare la criminalità in genere o semplicemente per far applicare la legge in maniera più efficace. Anche se la ratio potrebbe apparire ispirata alla tutela della privacy, il IV Emendamento trova la sua motivazione prima nella tutela del potere: esso è meglio compreso se considerato come uno strumento per preservare la potestà del popolo sul governo e garantisce alla sovranità popolare la possibilità di determinare come e in che modo il governo possa introdursi nelle vite dei cittadini ed influenzarne il comportamento[37]. Il IV Emendamento finisce cosí 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, regole che devono essere seguite al fine di poter effettuare l'attività di sorveglianza.

Nel decidere quando sia applicabile il IV Emendamento la Corte Suprema richiede che si stabilisca 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 essere similare, allora essa è considerata un "search" e la Costituzione ne limiterebbe il potere imponendo il requisito di una autorizzazione supportata da una "probable cause". Se l'attività, invece, non è ritenuta essere simile, allora gli agenti governativi saranno liberissimi di intraprendere la loro attività di investigazione senza dover sottostare ad alcuna costrizione o vincolo. Con riferimento alle nuove tecnologie di intercettazione telematica ed ambientale, questa interpretazione lascia aperta la possibilità che il loro utilizzo non possa assolutamente essere disciplinato dalle previsioni costituzionali in quanto, secondo una interpretazione rigidamente letterale, la Corte non le considera "search" ai sensi del IV Emendamento[38].

In un recente caso, Kyllo v. United States[39], la Corte Suprema ha compiuto un primo passo verso una interpretazione non basata, e quindi limitata, alla definizione della tutela della 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 conclude affermando che

[36] D.A. SKLANSKY, *Back to the Future: Kyllo, Katz, and Common law*, *Miss. L. J.*, in www.ssrn.com/Abstract_id=321450; ID., *The Fourth Amendment and Common Law*, 100 *Colum. L. Rev.* 1739 (2000); T. MACLIN, *The Complexity of the Fourth Amendment: A Historical Review*, 77 *B. U. L. Rev.* 296 (1997).

[37] W.J. STUNTZ, *Privacy's Problem and the Law of Criminal Procedure*, 93 *Mich. L. Rev.* 1016 (1995).

[38] 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).

[39] 533 U.S. 27, (2001).

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"[40]. In altre parole, piuttosto che chiedersi se i primi redattori della Carta costituzionale avrebbero considerato l'azione in questione un "search", la Corte dovrebbe chiedersi se questi avrebbero approvato tale livello di intrusività da parte dell'attività di sorveglianza del Governo a fini di garantire la sicurezza. La decisione in oggetto ha le potenzialità per far ritornare il Quarto Emendamento al suo ruolo originario, in quanto potrebbe cosí assoggettare tutte le attività investigative effettuate con l'ausilio delle nuove tecnologie alle limitazioni che esso prevede[41].

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. Un tale tipo di interpretazione significherebbe muoversi verso la riconciliazione del IV Emendamento con la dottrina della separazione dei poteri e riconoscere nuovamente nel popolo l'autorità sovrana nel compito di fare le leggi, al di là ed oltre l'appropriato livello di riservatezza e sicurezza.

Ma veniamo ora a delineare l'evoluzione storica e normativa delle tecnologie impiegate nell'attività di investigazione e sorveglianza.

Prima del 1980, quando il più diffuso, e in molti casi l'unico, mezzo di comunicazione era il telefono "di rete fissa", l'attività di sorveglianza delle comunicazioni era praticata con facilità allacciando un semplice congegno alla linea telefonica. Nel torno di pochi anni, milioni di persone cominciarono ad utilizzare nuove e più convenienti forme di comunicazione, quali i telefoni cellulari e le e-mail. Lo sviluppo di queste tecnologie ha limitato grandemente l'utilità dei metodi tradizionali di sorveglianza adottati dalle autorità pubbliche.

Vi sono due tipologie di sorveglianza delle comunicazioni: o le autorità pubbliche possono ottenere un mandato di c.d. register e and trace per raccogliere solo informazioni riguardanti i numeri composti in uscita o in entrata da uno specifico telefono; oppure possono essere investite di un più intrusivo mandato di intercettazione, c.d. intercept, che permette di ascoltare il contenuto della telefonata. I termini register e and trace si riferiscono ai congegni originariamente utilizzati per eseguire l'ordine di registrazione delle comunicazioni. Anche se le tecnologie sono cambiate, questa terminologia è ancora comunemente utilizzata[42]. Sono stati fatti tentativi di utilizzare le vecchie leggi per le nuove tecnologie, ma ciò non ha avuto risultati soddisfacenti. La disciplina che governa le c.d. *full intercept* si ritrova nel *Title III of the Omnibus Crime Control Safe Streets Act*[43] del 1969, il quale originariamente richiedeva che l'ordine della corte di compiere intercettazioni specificasse il luogo in cui si trovava il

[40] *IDEM*, 34.

[41] V. 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).

[42] V. sull'argomento: P.P. SWIRE, *Administration Wiretap Proposal Hits the Right Issues But Goes too Far*, in www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm.

[43] 18 U.S.C. §§ 2510-2522 (1994 & SUPP. 1998).

dispositivo utilizzato per le comunicazioni al fine di sottoporlo a sorveglianza, e che fosse indicato e dimostrato il motivo per cui la prova della condotta criminale doveva essere raccolta sorvegliando quel particolare dispositivo. La crescita delle comunicazioni basate su Internet limitò grandemente la capacità delle autorità pubbliche di condurre attività di intercettazione in base alla vecchia legge. Il *Title III* non parlava esplicitamente di comunicazioni telematiche; inoltre la terminologia in uso non appariva chiaramente applicabile alle e-mail. Per ovviare a ciò, le corti cominciarono ad applicare la normativa riguardante le intercettazioni telefoniche anche ai messaggi via Internet, ma ciò non senza problemi. La natura decentralizzata di Internet, infatti, dà luogo a nuove difficoltà nel cercar di attuare i *pen/trap orders*: le e-mail possono passare tramite diversi *service provider* di Internet ("ISPs") in differenti luoghi, attraverso differenti nazioni, costringendo gli agenti ad ottenere le informazioni da una catena di *service provider*, incontrando notevoli problemi dovuti alle barriere giurisdizionali.

Una disposizione dell'Communications Privacy Act del 1986 (ECPA)[44] ha cercato di aggiornare le leggi che disciplinavano le intercettazioni di comunicazioni, per renderle più efficaci, prevedendo un sistema di "*Roving Intercept"* (letteralmente "intercettazione itinerante") nelle investigazioni criminali. Queste sono ordini di *full intercept* disposti nei confronti di una specifica persona invece che di uno specifico congegno di comunicazione: le forze dell'ordine sono cosí autorizzate a compiere intercettazioni di comunicazioni da un telefono o computer usato da un sospetto senza dover prima specificare quali dispositivi saranno sottoposti a controllo. Il procedimento per ottenere tale nuovo mandato è più rigoroso di quello tradizionale, in quanto l'*Attorney General* degli Stati Uniti dovrà approvarne l'impiego prima che questo sia sottoposto al giudizio del giudice. Prima dell'11 settembre, l'FBI non poteva ottenere l'autorizzazione ad utilizzare le *roving intercept* per raccogliere informazioni di *intelligence* di origine estera o per investigazioni sul terrorismo. L'USAPA, emendando il FISA[45] e sostituendo al requisito del semplice "*purpose"* quello del "*significant purpose*", ha consentito tale forma di intercettazione anche in risposta al terrorismo.

In questo contesto si inserisce l'utilizzazione di Lantern[46]. Il IV Emendamento della Costituzione americana, come abbiamo sopra accennato, garantisce alle persone il diritto che non vengano violati le loro "*persons, houses, papers and effects*" contro "*unreasoneable searches and seizures*"[47]. La relazione di tale Emendamento con la sorveglianza elettronica è stata esplicitata nel famoso precedente *Katz v. United States*[48]: in tale circostanza l'FBI aveva connesso un dispositivo elettronico di ascolto e registrazione ad un telefono pubblico, e cosí aveva registrato il contenuto delle conversazioni ed utilizzato i dialoghi come prove di colpevolezza contro colui che

[44] 18 U.S.C. §§ 3121-3127 (1994 & Supp. 1998). Cfr. SCHULTZ, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, cit., 1236-1239.

[45] 50 U.S.C.A. 1801-1863 (1994 & Supp. V 1999). Cfr. SCHULTZ, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, cit., 1232-1234.

[46] V. WOO, SO, *The Case for Magic Lantern: September 11 highlights the need for increased surveillance*, cit.; HARTZOG, *The "magic lantern" revealed…*, cit..

[47] CFR. R.S.R. KU, *The Founders' Privacy: the Fourth Amendment and the Power of Technological Surveillance*, 86 *Minn. L. Rev.* 1325 (2002); S. KERR, *The Fourth Amendment in Cyberspace: Can Encription Create a "Reasonable Expecatition of Privacy?"*, 33 *Conn. L. Rev.* 503 (2001).

[48] In U.S. 347 (1967), disponibile su http://www.augustana.edu/Users/Podehnel/260/Katz%20ed.htm.

parlava. L'FBI sostenne che non vi era stata violazione del IV Emendamento in quanto non c'era stata una violazione "*physical*" dell'area occupata da Katz. La Corte rigettò questa ricostruzione e decise che andava valutata la "*reasonable expectancy of privacy*", la ragionevole aspettativa di riservatezza che ogni individuo ha. Utilizzando questo principio, in quel caso la Corte ritenne che l'attività posta in essere dall'FBI era in contrasto col IV Emendamento. Il principio sviluppato in *Katz v. United States* se applicato a *Magic Lantern* pone le corti di fronte al problema di stabilire se un individuo abbia o meno un "*reasonable expectancy of privacy*" nei confronti delle *keystroke* che immette nel suo computer.

Nel caso *States v. Scarfo*[49] l'FBI aveva ottenuto un *search warrant* al fine di poter usare un *Key logger system* sul computer di Scarfo. La questione verteva sullo stabilire se i *warrant* che autorizzano l'uso di *KLS* violano il IV Emendamento: il Governo aveva sí la possibilità di catturare e registrare le *keystroke* rilevanti ad ottenere la "*passphrase*" per decriptare il file, ma anche otteneva una sovrabbondanza di dati non necessari all'investigazione. Una volta che un'attività investigativa è qualificata come "*search*", cosí come previsto dal IV Emendamento, gli agenti devono ottenere un *search warrant* per continuare la loro attività. In *Scarfo* la Corte stabilí che i *KLS* non violano il IV Emendamento se, una volta ottenuto il *warrant*, l'attività investigativa viene intrapresa seguendo le particolari condizioni ivi indicate. Ciò risulta molto utile se applicato a *Magic lantern* perché è evidente che, ai sensi del IV Emendamento, le due tecnologie assolvono alle medesime funzioni. Se l'FBI ha ottenuto un dettagliato *search warrant* o un *wiretap order* per utilizzare *Magic lantern* con una completa lista di obiettivi da porre sotto intercettazione, ciò eviterà che sia possibile poi porre questioni di legittimità in forza del IV Emendamento. Quindi se l'FBI al fine di utilizzare questo software ottiene un *warrant* che indichi, con sufficiente precisione, gli obbiettivi da porre sotto investigazione, allora, secondo quanto stabilito in *Scarfo*, ciò impedirà la violazione del IV Emendamento.

Vi sono poi una serie di leggi che disciplinano l'attività di sorveglianza e la nell'attività del Governo e non è ancora chiaro quale tra queste sarà applicabile.

L'ECPA, di cui sopra abbiamo già avuto modo di trattare, fu emanato nel 1986 per emendare il III the Omnibus Crime Control Safe Streets Act, che autorizzava l'attività di intercettazione telefonica con i c.d. "III warrants". L'ECPA protegge contro l'accesso non autorizzato, l'intercettazione, o la divulgazione di comunicazioni private[50] ed è diviso in due parti: il *Title I* pone vincoli alle intercettazioni orali, telefoniche, e alle comunicazione elettroniche mentre esse avvengono ("*in transit*"), mentre il *Title II* si riferisce all'acquisizione e alla divulgazione di comunicazioni già registrate. Ciò che interessa alla nostra ricerca è il sottolineare l'estrema difficoltà di ottenere un'autorizzazione per compiere attività di sorveglianza ai sensi dell'ECPA a differenza della procedura che occorre per ottenere un *search warrant*[51], dove si richiede semplicemente una "*probable cause*". L'istanza per richiedere un *surveillance order*, in

[49] 180 F. Supp. 2d 572.

[50] S.E. GINDIN, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 *South Dakota L. Rev.* 1153 (1997).

[51] M.J. ANNIS, *Electronic Surveillance: Does it Bug You ?*, *Attorneys' Bulletin*, Sept. 1997.

particolare, deve contenere una dettagliata e completa lista di tutti gli obbiettivi che saranno posti sotto intercettazione, deve provenire dall'ufficio dell'*Attorney General*, deve essere approvata da un giudice federale, e occorre dar prova che tutte le altre tecniche di investigazione sono inutili, potenzialmente inutili, o troppo pericolose. La forma di comunicazione applicabile in teoria a Magic lantern tra quelle previste dall'ECPA è l'"electronic communication" che viene definita come "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce"[52]. Se *Magic Lantern* sarà configurato in maniera tale da non registrare informazioni che viaggiano su Internet, ma solo le *keystroke* digitate "offline", allora si potrebbe ritenere che le agenzie di investigazione pubblica non saranno obbligate ad ottenere un *authority granted* ai sensi del *Title I* dell'ECPA per utilizzare il nostro software.

In conclusione, il problema fondamentale consiste nel definire il termine "interception", ai sensi dell'ECPA. Se l'utilizzo di Lantern sarà qualificato come interception of electronic language, il fatto che le keystroke siano allora definite electronic communication o meno dipenderà dalle specifiche configurazioni dell'agente software (configurazioni che sono per la maggior parte ancora sconosciute): in tal caso, per poter utilizzare il nostro agente, sarà allora necessario ottenerne l'autorizzazione tramite il rigoroso procedimento descritto nel I dell'ECPA[53] e qualsiasi cambiamento si potrà apportare al "*setting*" del programma dovrà essere valutato caso per caso in base al tipo di informazioni che avrà raccolto.

L'utilizzo di questo agente software non sarà probabilmente disciplinato dall'ECPA, e ciò principalmente per il fatto che il linguaggio di questo testo normativo è fortemente legato alla volontà di disciplinare tecnologie più simili a Carnivore, software in grado di intercettare comunicazioni non molto diverse da quelle raccolte attraverso i tradizionali sistemi di intercettazione telefonica[54].

Alla luce dei recenti atti terroristici, la legge che più di ogni altra potrebbe essere applicata per l'utilizzazione del nostro software è il FISA, Intelligence Surveillance Act del 1978, il quale autorizza le intercettazioni telefoniche, dopo che una Corte abbia riscontrato l'esistenza di una cause, allo scopo di ottenere informazioni di straniere. Nessun mandato è richiesto se non sono implicati nell'investigazione cittadini americani, ma solamente la certificazione da parte dell'General. Se invece è implicato un cittadino americano il FISA richiede che vi sia uno specifico mandato emesso da una speciale Corte, la "Intelligence Surveillance Court". Affinché il FISA sia applicabile a Magic Lantern bisogna prima che questo rientri nella definizione di "electronic surveillance": "an installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable

[52] 18 U.S.C. 2510 (12).

[53] 18 U.S.C. 2510-2522.

[54] Si veda 18 U.S.C. 2510. La legge fa continuamente riferimento a parole come "" o "n", facendo un chiaro riferimento a tecnologie come i o che intercettano comunicazioni "in transito" attraverso Internet o i fili del telefono, e non a digitate sulla tastiera di una singola persona.

expectation of privacy and a warrant would be required for enforcement purposes"[55]. In quanto *Magic Lantern* è uno strumento di intercettazione telematica utilizzato per registrare *keystroke*, esso rientra sicuramente all'interno della prima parte della definizione del FISA. L'importanza che il nostro agente software rientri nell'ambito di applicazione del FISA consiste nel fatto che i prerequisiti richiesti per autorizzare una sorveglianza elettronica sono caratterizzati da un onere della prova meno gravoso; risulta, quindi, più facile ottenerlo rispetto a quanto avviene per l'emanazione di un *warrant* o di un *wiretap* in una investigazione criminale. L'USAPA, che costituisce un significativo trend in atto negli Stati Uniti nel favorire ed incoraggiare lo sviluppo e l'uso di tecnologie di sorveglianza da parte del Governo, ha, come sopra già detto, emendato il FISA statuendo che il *purpose* richiesto per ottenere delle *foreign intelligence information* non debba necessariamente essere l'intera ragione della sorveglianza, ma semplicemente un *significant purpose*, cosí diminuendo ulteriormente i requisiti per ottenere l'autorizzazione.

Infine resta il dar cenno di altre due previsioni legislative. Il Protection Act (PPA)[56] non pare applicabile in quanto proibisce a tutti gli agenti governativi, mentre investigano o procedono contro un reato, "*to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book broadcast or other similar form of public communication*"[57] e *Magic Lantern*, invece, registra solo *keystroke* e raccoglie materiale memorizzato elettronicamente o magneticamente. Il *Computer Fraud and Abuse Act* (CFAA)[58], principalmente previsto per prevenire l'accesso non autorizzato a reti di computer per proteggere la riservatezza delle comunicazioni, rivestirà una qualche importanza solo se la tecnologia *Magic Lantern* sarà utilizzata anche dai pirati informatici allo scopo di accedere ai computer altrui.

4. Le intercettazioni telematiche in Italia

In Italia si deve ancora porre in maniera rilevante il problema dell'armonizzazione dell'impiego di agenti software nelle intercettazioni telematiche, essendo il nostro paese, da questo punto di vista, sostanzialmente solo in grado di subire le iniziative di altri paesi più "evoluti"[59].

La Legge 23 dicembre 1993 n. 547 ha modificato, sia dal punto di vista sostanziale che da quello procedurale, la disciplina relativa alle intercettazioni come posta nel codice di procedura penale[60].

---

[55] 50 U.S.C. 1801 (f) (4).

[56] 42 U.S.C.A. 2000aa.

[57] 42 U.S.C.A. 2000AA(A).

[58] 18 U.S.C. 1030.

[59] *Privacy e sistemi di controllo globale in Italia*, in www.interlex.it/675/alcei11.htm; *La "sindrome" del pesce rosso" non è una malattia*, in www.interlex.it/675/pescer.htm.

[60] C. DI MARTINO, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile*, *L'indice Penale*, 2001, 219; C. PARODI, *Le intercettazioni. Profili operativi e giurisprudenziali*, Torino, 2002, 287-323; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, *Dig. Disc. Pen.*, vol. X, Torino, 1993, 191.

Oggetto delle intercettazioni informatiche o telematiche devono ritenersi connessioni –fisse o occasionali – tra sistemi informatici o telematici, ossia tra computer tra loro collegati o in rete o via modem o con qualsiasi altra forma. L'intercettazione potrà effettuarsi: o deviando su un computer le comunicazioni intercettate, provvedendo quindi ad una memorizzazione prima della ritrasmissione; o inserendo sul computer un "registro" in grado di memorizzare gli inserimenti e/o alterazioni di dati; o registrando su apposito supporto, nel caso di intercettazione di comunicazioni telematiche, i flussi, dopo aver provveduto ad attivare un'apposita linea telefonica fornita di modem per "ricevere" le comunicazioni[61].

Tornando alla normativa italiana, in particolare l'art. 266 c.p.p. (Intercettazioni di comunicazioni informatiche o telematiche) prevede che "procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi". Tale nuovo articolo permette quindi di compiere intercettazioni anche per reati non indicati nell'art. 266 c.p.p. (articolo riguardante le intercettazioni telefoniche): quando le indagini avranno ad oggetto uno dei reati indicati dall'art. 266 c.p.p., sia o meno commesso con l'impiego di tecnologia informatica, l'autorità inquirente potrà ricorrere sia alle intercettazioni comuni sia a quelle informatiche; quando invece le indagini avranno ad oggetto reati diversi da quelli contenuti nell'elenco di cui all'art. 266 c.p.p., saranno possibili solo le intercettazioni informatiche, sempre che i reati in questione siano stati commessi mediante l'uso di tecnologie informatiche o telematiche. Per quanto riguarda nello specifico l'esecuzione di questo tipo di intercettazioni, il Legislatore ha dimostrato un inusuale senso pratico prevedendo all'art. 268, co. 3° , c.p.p., che "si procede a intercettazione di comunicazioni informatiche o telematiche, il p.m. può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati". L'art. 268 c.p.p., come modificato dalla L. 547/1993, prevede poiche ai difensori delle parti sia immediatamente dato avviso e che questi, entro il termine fissato a norma dei commi 4 e 5, abbiano facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche d'ufficio allo stralcio delle registrazioni e dei verbali di cui sia vietata l'utilizzazione. Il pubblico ministero e i difensori hanno diritto a partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima. Il giudice dispone la trascrizione integrale delle registrazioni ovvero la stampa in forma intelligibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il

[61] G. BUONOMO, *Metodologia e disciplina delle indagini informatiche*, in R. BORRUSO, G. BUONOMO, G. CORASANITI, G. D'AIETTI, *Profili penali dell'informatica*, Milano, 155. In relazione alle comunicazioni elettroniche occorre ricordare la 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, recepita nell'ordinamento italiano con le leggi 3 febbraio 2003, n. 14, e 31 ottobre 2003, n. 306.

dibattimento. I difensori possono estrarre copia delle trascrizioni e fare eseguire la trasposizione della registrazione su nastro magnetico. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa. Particolarmente utile sarà anche l'acquisizione (con decreto di sequestro probatorio) dei dati concernenti le chiamate in entrata ed in uscita da determinate utenze telefoniche (c.d. tracciamento) di cui pu essere utile acquisire non solo il supporto cartaceo (tabulato), ma altresì, ove possibile, la registrazione informatica, onde "ordinare" le numerazioni per blocchi ricorrenti e significativi. Ad esempio si potrà selezionare le utenze interessate per aree territoriali (mediante il prefisso teleselettivo), o evidenziare pi chiamate effettuate in via continuativa o nello stesso arco orario. Le tracce informatiche sono in sostanza una vera e propria alternativa alla intercettazione (e molto meno invasive della riservatezza) e possono costituire una efficace tecnica alternativa per l'accertamento dei crimini informatici.

L'utilizzazione illegittima di agenti software quali Magic Lantern nel contesto italiano potrebbe inoltre configurare una serie di fatti penalmente perseguibili ai sensi della L. 547/1993. L'art. 615 .p. configura il reato di accesso abusivo ad un sistema informatico o telematico. Esso si concretizza nel comportamento di chiunque abusivamente si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo: la pena è della reclusione fino a tre anni (in tal caso si procede a querela della persona offesa), ma, nel caso il reato fosse commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, diviene da uno a cinque anni e si procede d'ufficio. L'art. 615 c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici) punisce (con la reclusione sino ad un anno e con la multa fino a euro 5.164,57) la condotta di chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo. L'art. 615 c.p. (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) punisce (con la reclusione sino a due anni e con la multa sino a euro 10.329,14) la condotta di chiunque diffonda, comunichi o consegni un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. È l'ipotesi che sanziona la produzione e la diffusione dei c.d. "virus", e che comporta seri problemi di accertamento in ordine alla coscienza ed alla volontà dell'azione (coscienza e volontà, indubbiamente consistente nella deliberata introduzione o diffusione di programmi dannosi in qualsiasi forma, anche se la formulazione normativa non contribuisce alla chiara definizione dell'illecito allorquando, riferendosi ai programmi si riferisce tanto allo "scopo" dannoso della relativa progettazione e elaborazione che all'"effetto", adombrando una ipotetica condotta rilevante almeno sul piano colposo o del dolo indiretto). Infine l'art. 617 c.p. (Installazione di apparecchiature atte a intercettare, impedire od interrompere

comunicazioni informatiche o telematiche) col quale si punisce con la reclusione da uno a quattro anni chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra pi sistemi.

Questo, per quanto attiene al profilo penalistico, sia da un punto di vista procedurale che sostanziale. Ma l'utilizzo di agenti software nell'ambito della sicurezza informatica, porta con sè anche problematiche legate alla riservatezza e alla tutela dei dati raccolti[62]. A questo riguardo non si può non ricordare il recente D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione di dati personali) che ha sistematizzato ed armonizzato la materia[63]. Maggiore attenzione, com'è ovvio, viene riservata a quei dati il cui trattamento illecito o inadeguato può esporre l'interessato a gravi conseguenze (tali sono i dati sanitari, quelli relativi all'appartenenza a gruppi politici, religiosi, sindacati, ecc.), definiti dalla norma come "dati sensibili". Naturalmente, sono considerati maggiormente a rischio gli elaboratori elettronici collegati in rete, soprattutto se connessi a reti telematiche disponibili al pubblico, come Internet.

Tre sono gli aspetti che vengono in rilievo nell'approntare le misure di sicurezza destinate a proteggere un sistema informatico: 1) l'autenticazione degli utenti, importante perché consente di accertare in che momento qualcuno fa qualcosa e perché, in caso di sua assenza, tutti gli utenti avrebbero i medesimi privilegi e sarebbe impossibile esercitare qualsiasi tipo di controllo; 2) la tutela dell'integrità, che consente di verificare le attuali condizioni dei dati in relazione alloro stato originale, e, se ci non fosse possibile, non si potrebbe far alcun affidamento sul database che li contiene; 3) la confidenzialità (o riservatezza) delle informazioni memorizzate negli archivi, aspetto fondamentale in quanto l'autenticazione degli utenti e la tutela dell'integrità dei dati sono strumentali per il raggiungimento di tale obiettivo, che richiede, oltre all'utilizzo di strumenti tecnologici, l'adozione degli opportuni meccanismi organizzativi.

Appare inutile evidenziare che le precauzioni di tipo fisico (cancelli, badge per l'accesso ai locali, serrature, ecc.) e logico (UserID, Password, monitoraggio, aggiornamento dei software, ecc.) possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer, ma nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme. È quindi assolutamente necessario curare quelle che dalla norma sono definite misure "organizzative"; è lo stesso decreto legislativo che, all'art. 34, pone l'accento su tale

[62] G. POMANTE, *Privacy e sicurezza informatica*, in http://www.pomante.com/documenti/Privacy%20e%20sicurezza.htm; ID., *La sicurezza informatica*, in http://www.pomante.com/documenti/Sicur1.htm; *Privacy e nuove tecnologie. Aaspetti politici, giuridici e pratici*, in www.olografix.org/gubi/estate/dossier/privacy.txt.

[63] L'art. 183 D.Lgs. 196/2003 ha abrogato la famosa Legge 31 dicembre 1996 n. 675, Legge 3 novembre 2000 n. 325 (Disposizioni inerenti all'adozione di misure minime di sicurezza nel trattamento dei dati personali) ed il D.P.R.28.7.1999, n. 318 (to recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della L.31 dicembre 1996, n. 675).

adempimento, disponendo che, nel caso di trattamento di dati sensibili, sia necessario predisporre un "Documento Programmatico sulla Sicurezza".

Sul tema delle banche dati utilizzate dalle forze di polizia, si deve richiamare il su citato D.Lgs. 30 giugno 2003, n. 196, che ha previsto un apposito Titolo II (artt. 53-57) in cui è disciplinato il trattamento dei dati da parte delle forze di polizia. All'art. 55 si tratta direttamente il problema della gestione dei dati personali attraverso l'uso di particolari tecnologie e si afferma che "Il trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17 sulla base di preventiva comunicazione ai sensi dell'articolo 39": per questo tipo di trattamento occorrerà, quindi, dare preventiva comunicazione al Garante e rispettare le misure e gli accorgimenti che questi prescriverà in favore dell'interessato ed in applicazione dei principi sanciti nel Codice in materia di protezione dei dati personali.

Ha, infine, rilevanza la Legge del 1 aprile 1981, n. 121 (nuovo ordinamento dell'amministrazione della pubblica sicurezza) integrata dal testo del D.P.R. 3 maggio 1982, n. 378 (Regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrati negli archivi magnetici del centro di elaborazione dati di cui all'art. 8 della legge 1 aprile 1981, n. 121) dove si prevede che l'accesso ai dati ed alle informazioni sia consentito all'autorità giudiziaria ai fini degli accertamenti necessari per i procedimenti in corso nei limiti stabiliti dal codice di procedura penale. E', comunque, vietata ogni utilizzazione delle informazioni e dei dati predetti per finalità diverse da quelle previste dall'articolo 6, lett. a)[64], ed ogni circolazione delle informazioni all'interno della pubblica amministrazione fuori dai casi indicati dal suddetto articolo. Viene, poi, stabilito all'articolo 10 che il controllo del corretto utilizzo dei dati venga svolto dal Garante per la protezione dei dati personali nei modi previsti dalle leggi e dai regolamenti. Si sancisce, in conclusione, all'articolo 12, che il pubblico ufficiale che comunichi o faccia uso di dati ed informazioni in violazione delle disposizioni della suddetta legge, o al di fuori dei fini previsti dalla stessa, sia punito, salvo che il fatto costituisca reato più grave, con la reclusione da uno a tre anni, o se il fatto è commesso per colpa, con la pena della reclusione fino a sei mesi.

5. Conclusioni: security v. privacy o security and privacy?

Ultimamente vi è stata una crescente attenzione sul concetto di privacy, sulle sue finalità e le sue tutele. Essa consiste, possiamo dire, nel riconoscere alle persone

[64] L'art. 6, lett. a), L. 121/1981, cosí recita: "Il dipartimento della pubblica sicurezza, ai fini dell'attuazione delle direttive impartite dal Ministero dell'Interno nell'esercizio delle attribuzioni di coordinamento e di direzione unitaria in materia di ordine e di sicurezza pubblica, espleta compiti di: a) classificazione, analisi e valutazione delle informazioni e dei dati che devono essere forniti anche dalle forze di polizia in materia di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità e loro diramazione agli organi operativi delle suddette forze di polizia".

l'"intangibilità" di un certo numero di dati e informazioni personali (i c.d. "dati sensibili"), per i quali la possibilità di utilizzarli e renderli pubblici deve essere bilanciata ed armonizzata con le esigenze dell'individuo[65].

Anche il concetto di sicurezza, negli ultimi anni, ma soprattutto dopo l'11 settembre, ha dato luogo ad un vivace dibattito tra gli analisti delle discipline politico-giuridiche e ha visto crescere intorno a sé l'interesse dell'opinione pubblica.

Tutto ciò, trasportato in ambito telematico, moltiplica esponenzialmente i problemi e le possibili situazioni di lesione degli interessi e delle libertà dei singoli[66]; ciò ancor di più se si diffonderà l'utilizzo di tecnologie, quali quella ad agenti software, le quali, grazie alla loro capacità di muoversi nella rete e di agire in maniera autonoma, si caratterizzano per una maggior efficacia, ma allo stesso tempo, per una maggior pericolosità per la libertà e la *privacy* dei singoli.

Raramente, però, si è cercata una mediazione tra il concetto di privacy e quello di sicurezza: questi sono sempre stati pensati in maniera antagonistica, quasi che l'uno escludesse l'altro. Occorre, invece, capire che non vi può essere reale sicurezza se non attraverso la tutela della privacy, e, viceversa, non vi è tutela della riservatezza degli individui se non attraverso e grazie la sicurezza pubblica. Vero è che un maggior livello di sicurezza può spesso voler significare che le forze dell'ordine, ed in generale il Governo, abbiano il potere di accedere ad informazioni sempre maggiori aumentando il numero di situazioni a rischio; e questo perché spesso garanzia di sicurezza equivale a capacità di sorveglianza. Ma è proprio la protezione della privacy a richiedere un buon livello di sicurezza, attraverso il quale si ponga in essere una corretta utilizzazione delle informazioni. Infatti, il concetto di sarebbe messo fortemente in discussione se vari pirati informatici o estranei potessero entrare nel sistema e rubare le informazioni contenute. È conveniente valutare il problema con un approccio pragmatico che consideri i rischi ed i vantaggi in campo senza incappare in preconcette prese di posizione. Da un lato, occorre regolamentare, definendone i confini, l'attività investigativa di intelligence, che presenta notevoli rischi in ordine al suo inevitabile carattere pervasivo; dall'altro, bisogna tener presente che non esiste sicurezza, e quindi riservatezza, se non attraverso un'attività di prevenzione e contrasto di attività criminose, le quali, avendo come scopo dichiarato proprio quello di minare alle fondamenta il nostro sistema sociale, esse sí per prime rappresentano il vero e proprio attentato alla pacifica e civile convivenza dei consociati.

Ma, forse, molto ancora si può fare con l'implementazione di tecnologie a protezione della sfera privata dei cittadini[67]. Forse vi è un'altra strada da battere per la

---

[65] V. M. ROTENMBERG, *Privacy Law Sourcebook 2001*, 2001; P.P. SWIRE, *The Surprising Virtues of the NewFinancial Privacy Law*, 86 *Minn. L. Rev.* 1263 (2002).

[66] Si vedano A. DAVIDSON, *Increasing Security without Decreasing Privacy and Freedom*, *Law Rev. Mich. St. U.-Det. C.L.* 783 (2002); A. GIDARI, *Balancing open access and national security goals*, *Law Rev. Mich. St. U.-Det. C.L.* 765 (2002); A. CAVOUKIAN, *Technology Can Ensure Both Privacy and Security*, *Kitchner-Waterloo Rec.*, Jan. 10, 2002, 13.

[67] V. *Security with Privacy. ISAT 2002 Study* , in http://www.darpa.mil/iao/secpriv.pdf, dove si suggeriscono tre diversi tipi di strategie: la *Selective Revelation* , la *Strong audit* e la *Rule Processing Technologies* ; J. MARKOFF, *Study Seeks Technology Safeguards for Privacy , in http://www.interesting-people.org/archives/interesting-people/200212/msg00082.html;* S. LAU , *Balancing the need for*

difesa e la tutela dei singoli e dei loro dati personali non basata sull'utilizzo di strumenti di "forza bruta", quali i vari Carnivore o Magic Lantern, che presentano esternalità negative nel loro utilizzo a volte superiori ai benefici. La strada di cui parliamo è a tutt'oggi ancora un sentiero stretto e difficile che si basa sull'implementazione di metodi di autodifesa come la criptazione o la tecnologia ad agenti software del tipo dei filtri anti-spam che utilizzano sistemi di filtraggio a base statistica (cioè i filtri c.d. bayesiani)[68]. Lo sviluppo di sistemi di difesa basati sugli agenti software, con le indubbie positive particolarità di cui questi si connotano, fornirebbe ai singoli una tutela diretta ed efficace dei loro dati e della loro sfera personale, vista l'ormai acquisita consapevolezza che, in un mondo cosí vasto ed in continuo cambiamento quale quello di Internet, le tradizionali organizzazioni governative predisposte alla tutela pubblica saranno sempre più nell'impossibilità di operare validamente e di garantire l'integrità dei sistemi informatici. L'attenzione si deve spostare sui singoli utilizzatori della rete, siano essi privati cittadini o enti pubblici: su questi occorre investire e soprattutto a questi occorre fornire programmi e dispositivi flessibili nel loro utilizzo, facilmente aggiornabili e dotati di autonoma attività.

Infine, solo alcune riflessioni sul nuovo ruolo dello Stato nella rete.

I tragici eventi dell'11 settembre e i suoi inevitabili strascichi hanno rafforzato un trend in atto: essi hanno cambiato il modo in cui la gente concepisce lo Stato e le sue responsabilità ed hanno sottolineato il suo tradizionale ruolo di custode della sicurezza.

Occorre, però, anche tenere in considerazione il fatto che il ritorno dello Stato nel mondo digitale influisce sulle idee, sulle ideologie e sui valori che ne modellano e caratterizzano l'impianto generale. È ormai largamente condivisa l'idea secondo la quale la tecnologia non sia priva di valori. La struttura di un software, l'architettura dell'ambiente digitale, o semplicemente, il codice, riflettono e formano allo stesso tempo i valori. Vi è un rapporto complesso tra la storia delle idee e il cambiamento tecnologico. I cambiamenti tecnologici possono provocare cambiamenti economici, oltre che trasformazioni nelle istituzioni sociali. Ma la relazione tra tecnologia ed idee agisce anche in senso inverso.

Lo stato di guerra, il riemergere delle identità nazionali e di confini nazionali, e la fiducia o la diffidenza nei confronti dell'armonia globale, tutto ciò crea un nuovo ambiente sociale e politico. Il fatto che lo Stato divenga più visibile su Internet nel dopo 11 settembre è probabile che modifichi le nostre aspettative nei confronti delle reti digitali. Queste aspettative formeranno sicuramente la struttura dell'ambiente digitale nel prossimo futuro.

Securitywith Economic Imperatives and Societal Values, in http://www.oecd.org/pdf/M00038000/M00038708.pdf.

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