Un “rapporto di minoranza”: elogio dell’insicurezza informatica e della fallibilità del diritto. Note a margine del *Trusted Computing*

Versione 1.0 maggio 2007

Roberto Caso

Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del *Trusted Computing*

Versione 1.0 maggio 2007[*]

Roberto Caso

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

In questa relazione che introduce i lavori del convegno, vorrei mettere in risalto l'importanza e la complessità dei problemi giuridici che ruotano attorno al tema della sicurezza informatica. Non mi cimenterò nel compito (inane) di definire il concetto di sicurezza informatica e passare in rassegna le questioni che essa porta all'attenzione del giurista. Prenderò invece una scorciatoia, soffermandomi su quella che appare l'ultima frontiera del tema in discussione. Il riferimento è al *Trusted Computing* (TC). "Trusted

[*] Articolo già pubblicato in R. CASO (cur.), *Sicurezza informatica: regole e prassi. Atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 6 maggio 2005*, Trento, 2006.

Computing" è una delle molteplici (cangianti) espressioni usate per denominare il coordinamento di alcune iniziative che fanno capo ad imprese leader del settore dell'hardware e del software. Il nucleo iniziale di queste iniziative risiedeva nella *Trusted Computing Platform Alliance* (TCPA) fondata da Compaq, HP, IBM, Intel e Microsoft. I compiti della TCPA sono stati poi assorbiti ed ampliati dal *Trusted Computing Group* (TCG), un'organizzazione no profit promossa da sette imprese (le cinque fondatrici della TCPA più Sony Corporation e Sun Microsystems, Inc.)[1].

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

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

I principali produttori di microprocessori (Intel e AMD) si stanno muovendo velocemente verso l'incorporazione di specifiche TC nei propri apparecchi. Si pensi in particolare all'Intel LaGrande Technology[3]. D'altra parte, anche la Microsoft va nella stessa direzione. In questa prospettiva si spiega l'azione della Microsoft volta a sviluppare la Next-Generation Secure Computing Base (NGSCB)[4], prima nota come Palladium, destinata ad essere incorporata nella prossima generazione di Windows, denominata prima "Longhorn" e da ultimo "Vista". Insomma la NGSCB costituisce una

[1] V. il sito Web: https://www.trustedcomputinggroup.org.
[2] V. l'URL: https://www.trustedcomputinggroup.org/about/
[3] V. il sito Web: http://www.intel.com/technology/security/
[4] V. il sito Web: http://www.microsoft.com/resources/ngscb/default.mspx.

delle possibili e delle più importanti – stante la posizione di Microsoft sul mercato informatico – applicazioni del TC[5]. Persino Linux nelle sue ultime versioni incorpora funzionalità TC[6]. In sintesi, a partire dal 2004, vi è una diffusa tendenza da parte dei produttori di hardware e degli sviluppatori a convergere verso l'architettura TC[7].

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

Nel racconto fantascientifico intitolato "Minority Report" (in italiano: "Rapporto di minoranza") il genio visionario di Philip Dick racconta di un futuro nel quale il connubio tra mutazioni genetiche degli uomini e computer conferisce alla polizia il potere di conoscere in anticipo la commissione di un crimine, consentendo in questo modo di usare la forza repressiva prim'ancora che il reato venga consumato[8]. Il giudizio prognostico (o, nella terminologia di Dick, "precognitivo") sulla commissione del delitto si basa su un meccanismo che fa leva sulle premonizioni di tre esseri umani geneticamente mutati – i "precog" – e sulle macchine (computer). Questo giudizio prognostico può basarsi sulla completa convergenza delle premonizioni, oppure molto più frequentemente su due premonizioni (che vedono il delitto) ed una invece dissonante (il "rapporto di minoranza" appunto). La morale del racconto sembra risiedere nella ferma condanna della repressione preventiva, vista come potere conferito dal progresso tecnologico. La conclusione del racconto è pessimista: il protagonista, comandante della sezione specializzata della polizia che si occupa della repressione

---

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

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

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

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

preventiva – Precrimine –, viene a sapere di essere accusato dalle premonizioni di un futuro omicidio, ma successivamente scopre un (veritiero?) rapporto di minoranza che lo assolve. Tuttavia, per non screditare (e consegnare allo smantellamento) la sua polizia, decide di commettere ugualmente l'omicidio per confermare il rapporto di maggioranza.

La logica del TC è simile a quella delle macchine premonitrici di Dick: invece di intervenire *ex post*, si crea *ex ante* un ambiente sicuro. Nel caso del TC si tratta "solo" di un ambiente digitale, un ambiente *trusted* ("fidato" o "sicuro") che diminuisce o addirittura azzera il rischio di attacchi ai sistemi informatici o "utilizzi impropri" del computer. Però, come nell'inquietante futuro di Dick, la sicurezza è ottenuta al prezzo della compressione della libertà delle persone. Infatti alla base della logica del TC vi è la limitazione delle funzionalità e la dislocazione del controllo del computer dall'utente a chi gestisce la sicurezza informatica. Il fatto che nel caso dell'ambiente digitale sia in gioco "solo" la sicurezza informatica non deve rassicurare. Il computer è sempre più uno strumento nel quale proiettiamo quelle attività quotidiane (come l'ascolto di una musica e la visione di un film o come la raccolta di dati personali) che presuppongono libertà fondamentali (quali la libertà di pensiero e di autodeterminazione). Inoltre, l'approccio TC alla sicurezza informatica pone due problemi di fondo che sono assai rilevanti sul piano giuridico:

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

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

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

informatico con i principi della normativa comunitaria in materia di protezione dei dati personali, nel paragrafo 5 si traggono alcune brevi conclusioni.

2. Lineamenti essenziali del Trusted Computing

Nell'ambito informatico, l'espressione *trusted system* (traducibile approssimativamente con "sistema fidato" o "sistema sicuro") è usata in varie accezioni. Secondo una prima accezione che deriva dall'ingegneria della sicurezza, un sistema si definisce "trusted" quando si è costretti a farvi affidamento[9]. Il fallimento di un *trusted system* mette a rischio l'intera politica sicurezza[10]. Secondo un'altra accezione – più vicina a quella utilizzata anche nella *policy analysis*[11]– un sistema è reso "trusted" dal fatto che

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

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

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

l'hardware ed il software sono costretti ad operare secondo "regole" predeterminate[12]. Questa seconda accezione identifica la sicurezza o l'affidabilità con la limitazione preventiva di funzionalità del sistema, in quanto il rischio maggiore deriverebbe dalla libertà d'azione gli agenti (persone o software)[13]. In termini rovesciati: un sistema informatico è insicuro se gli agenti possono controllarlo e modificarlo liberamente.

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

Attualmente il TC risponde alla seguente logica[16]. Un sistema è sicuro o

---

that behavior within systems complies with expected or authorized parameters".

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

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

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

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

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

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

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

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

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

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

L'ingrediente di base del TC è rappresentato dalla crittografia digitale. La crittografia è lo studio delle tecniche utilizzate per trasformare un testo leggibile (c.d. testo in chiaro) in crittogramma (processo che viene detto anche "crittazione" o

---

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

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

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

"cifratura") e viceversa (processo che viene detto anche "decrittazione" o "decifratura")[19], uno studio che fa leva su una storia millenaria[20]. Nell'era digitale l'utilizzo della crittografia è diventato pervasivo, ponendo anche complessi problemi giuridici[21].

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

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

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

---

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

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

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

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

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

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

[23] Il profilo della sicurezza si interseca con il carattere segreto o pubblico delle procedure che generano il sistema di crittografia. Molti studiosi di crittografia ritengono che l'unico modo per valutare la sicurezza di una data tecnologia sia quello di analizzare le procedure sulle quali essa si basa (l'atteggiamento dei crittografi si basa sul c.d. principio di Kerckhoffs, in base al quale la sicurezza di un

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

- segretezza dei dati;

- integrità dei dati;

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

Al fine di rendere operative queste finalità, l'architettura TC deve far leva sull'interazione di tre elementi: l'hardware, il software e l'infrastruttura (PKI) per la

---

sistema di crittografia non dovrebbe fondarsi sulla segretezza dell'algoritmo, ma sulla segretezza delle chiavi: v., nella letteratura giuridica, ZICCARDI, *Il diritto d'autore dell'era digitale*, Milano, 2001, 174). In generale, più il sistema crittografico è ritenuto resistente, più è sottoposto a verifiche della comunità scientifica ed attacchi di soggetti indipendenti. Ciò ha un riflesso sul mercato della crittografia, poiché solo sistemi che si basano su algoritmi pubblici e sottoposti a scrutinio dovrebbero essere appetibili.

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

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

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

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

gestione della certificazione crittografica[28].

La componente hardware fondamentale dell'architettura è rappresentata dal *Trusted Platform Module* (TPM) un microchip che svolge funzioni crittografiche[29]. Nel TPM infatti vengono generati e custoditi i certificati, le password e le chiavi crittografiche. Tra le chiavi crittografiche riveste una fondamentale importanza la c.d. *Endorsement Key* che è finalizzata ad identificare il TPM come originale (cioè non manipolato o contraffatto)[30].

---

[28] V. KUHLMANN, GEHRING, *Trusted Platforms, DRM, and Beyond*, cit., 182 ss. Come rilevato da R. A. GHERING, *Trusted Computing for Digital Rights Management,* in *Indicare Monitor*, vol. 2, 2006, 387, 389, disponibile all'URL attualmente le speciche TCG riguardano i seguenti elementi:

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

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

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

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

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

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

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

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

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

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

(all'URL: https://www.trustedcomputinggroup.org/groups/glossary/) l'*Endorsement Key* è una "an RSA Key pair composed of a public key (EKpu) and private (EKpr). The EK is used to recognize a genuine TPM. The EK is used to decrypt information sent to a TPM in the Privacy CA and DAA protocols, and during the installation of an Owner in the TPM".

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

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

[33] V. il documento TCG intitolato *Trusted Platform Modules Strengthen User and Platform Authenticity*, gennaio 2005, reperibile all'URL: https://www.trustedcomputinggroup.org/specs/TPM/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf: "[o]ne frequent system attack involves making unauthorized changes to a platform's configuration. This allows misuse of the device and its contents as well as access to the networks to which the device is connected. In devices that use TPM chips, platform integrity is protected by secure storage of the platform configuration values and by secure reporting of the values. This enables attestation of the device by verifying that its configuration is intact. The mechanism is based on the chain of trust used in creating the hash values of the pre-boot information of the platform. It is common industry practice to check the integrity of a platform by comparing configuration settings when a platform is rebooted against the settings when it was set up. A 'hash' algorithm is used to calculate a value from information stored in the Platform Configuration Registers (PCRs) when the platform is setup. When the platform is re-booted, a new hash value is calculated and compared against the original. If the values match, the computer or cell phone or other platform starts up and login proceeds. In unprotected systems, PCRs are accessible and the hash values are stored in system memory that is subject to compromise. In TPM-capable platforms, the hash value is calculated using the SHA-1 algorithm, access to the PCRs requires trusted authorization, and the hash values are stored within the TPMs in secure, non-volatile memory. These values are used to create Attestation Identity Keys (AIKs) that cannot be used unless a hash value is the same at the time of use as when the AIK was created. This makes it possible to determine if trusted-state configuration parameters are corrupted. If they are corrupted, use of the device may be denied".

[34] V. *TCG Specification Architecture Overview - Specification Revision 1.2*, cit.: "[a]ttestation is the process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. All forms of attestation require reliable evidence of the attesting entity. Attestation can be understood along several dimensions, attestation by the TPM, attestation to the platform, attestation of the platform and authentication of the platform. Attestation by the TPM is an operation that provides proof of data known to the TPM. This is

Nell'architettura TC l'interazione dei tre elementi ora sommariamente descritti serve a rendere operative alcune funzioni di sicurezza e a limitare altre funzioni che sono normalmente riconducibili alla malleabilità della parte logica (software) del computer. La letteratura che si riferisce agli attuali sviluppi delle applicazioni TC individua le seguenti funzioni come le più rilevanti[35].

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

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

---

done by digitally signing specific internal TPM data using an attestation identity key (AIK). The acceptance and validity of both the integrity measurements and the AIK itself are determined by a verifier. The AIK is obtained using either the Privacy CA or via a trusted attestation protocol. Attestation to the platform is an operation that provides proof that a platform can be trusted to report integrity measurements; performed using the set or subset of the credentials associated with the platform; used to issue an AIK credential. Attestation of the platform is an operation that provides proof of a set of the platform's integrity measurements. This is done by digitally signing a set of PCRs using an AIK in the TPM. Authentication of the platform provides evidence of a claimed platform identity. The claimed identity may or may not be related to a user or any actions performed by the user. Platform Authentication is performed using any non-migratable signing key. Certified keys (i.e. signed by an AIK) have the added semantic of being attestable. Since there are an unlimited number of non-migratable keys associated with the TPM, there are an unlimited number of identities that can be authenticated".

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

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

[37] Cfr. *LaGrande Technology Architectural Overview*, cit.: "Protected Execution: [p]rovides applications with the ability to run in isolated protected execution environments such that no other unauthorized software on the platform can observe or compromise the information being operated upon. Each of these isolated environments has dedicated resources that are managed by the processor, chipset and OS kernel".

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

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

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

---

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

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

[40] Cfr. *LaGrande Technology Architectural Overview*, cit.: “Protected Launch: [p]rovides for the controlled launch and registration of the critical OS and system software components in a protected execution environment”; nonché la pagina Web del sito di Microsoft dedicata NGSCB (all’URL: http://www.microsoft.com/resources/ngscb/default.mspx): “[o]ur first delivery on the vision is a hardware based security feature in Longhorn called Secure Startup. Secure Startup utilizes a Trusted Platform Module (TPM 1.2) to improve PC security and it meets some of the most critical requirements we heard from our customers-specifically, the capability to ensure that the PC running Longhorn starts in a known-good state, as well as protection of data from unauthorized access through full volume encryption”.

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

modificarlo ed impedisce altresì che il file contenente il diario possa essere modificato anche quando sia processato su un altro computer.

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

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

- la gestione delle risorse informatiche e dei rischi a cui esse sono esposte (rischi come la perdita accidentale o il furto di dati di persone fisiche o imprese)[42];

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

---

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

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

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

- il commercio elettronico[44].

Alcuni commentatori rilevano che uno degli utilizzi più promettenti è rappresentato dall'*Enterprise Rights Management* (ERM), cioè dal controllo accentrato dell'accesso ai documenti all'interno di un'organizzazione[45]. Ad esempio, l'ERM può essere utilizzato per programmare la distruzione di documenti confidenziali, o per evitare che i documenti prodotti dai computer dell'organizzazione possano essere letti da altri sistemi informatici.

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

---

system processes that use the PCR values in a TPM to identify unsafe configurations at system boot thereby preventing inadvertent network connection while in an unsafe mode".

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

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

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

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

infrastrutture (i sistemi informatici) sulle quali la stessa informazione viaggia[48].

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

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

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

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

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

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

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

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

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

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

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

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

- di rendere possibili restrizioni alla concorrenza nel mercato informatico[52];

---

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

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

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

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

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

D. L. BURK, *Market Regulation and Innovation: Legal and Technical Standards in Digital Rights Management*, 74 *Fordham L. Rev.* 537, 556-557 (2005): "[i]n a secured, rights-managed environment, therefore, interoperation and the ability to produce viable interoperative products depend not only on the

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

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

- di minacciare la privacy degli utenti.

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

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

Lo logica TC parte dall'idea che la sicurezza di un computer (e anche dell'ambiente digitale in cui si colloca) può essere messa a rischio dal proprietario o dall'utente dello stesso computer. Di là dalle critiche che possono essere mosse ad un approccio alla sicurezza che vede nel proprietario o nell'utente del computer il nemico da combattere, vanno ora riconsiderati i due fondamenti di questa logica ai quali si è prima accennato.

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

Il secondo fondamento sta nella dislocazione del controllo del sistema

---

standard for technical compatibility, but on the standard for defining and implementing 'trust'. A full discussion of the technical and operational parameters of trust management lies well beyond the scope of this paper, but since security is never absolute, such parameters are not necessarily objective in all dimensions, requiring at minimum a judgment as to how secure is secure enough. Where interoperation is at issue, the potential for considerable anticompetitive mischief may lie in such judgments; one can well imagine the possessor of a dominant market position protecting that position by excluding rival products from interoperation, ostensibly on security concerns, but clandestinely on strategic criteria. Even if the alleged security concerns leading to exclusion are wholly legitimate, concealing no illegitimate anticompetitive motivation, the practical effect of the exclusion may be the same, barring entry to innovative complementary or competing products".

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

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

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

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

Da sempre, la lettura di un testo letterario o l'ascolto di una musica rappresentano attività nelle quali si rispecchiano i tratti più intimi della personalità di un uomo, come i gusti artistici o le idee politiche e religiose. La riproducibilità in serie dell'opera dell'ingegno ha poi esaltato la possibilità di rendere private e anonime tali attività. Nell'era predigitale, il contratto tra fornitore e fruitore dell'opera dell'ingegno avviene usualmente prescindendo dall'identificazione di quest'ultimo.

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

---

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

[55] COHEN, *DRM and Privacy*, cit., 576 ss.

[56] COHEN, *DRM and Privacy*, cit., 577-578: "[s]urveillance and compelled disclosure of information about intellectual consumption threaten rights of personal integrity and self-definition in subtle but powerful ways. Although a person cannot be prohibited from thinking as she chooses, persistent, fine-grained observation subtly shapes behavior, expression, and ultimately identity. The inexorable pressure

La dimensione spaziale concerne, invece, quei luoghi (fisici) privati – non necessariamente oggetto di proprietà – nei quali i comportamenti della persona sono liberi dal condizionamento altrui. Tali comportamenti possono includere quelli che risultano aberranti per le norme sociali dominanti e quelli che semplicemente non sono destinati ad essere assunti in pubblico. Tra questi comportamenti vi sono molte forme di consumo intellettuale. In definitiva, la seconda dimensione della privacy delimita uno spazio (fisico) nel quale la persona è libera di esplorare i propri interessi intellettuali[57].

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

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

Occorre poi aggiungere che, oltre alla restrizione diretta e al monitoraggio del

---

toward conformity generated by exposure, and by loss of control over uses of the gathered information, violates rights of self-determination by coopting them. Additionally, surveillance and exposure devalue the fundamental dignity of persons by reducing the exposed individuals to the sum of their 'profiles'. For these reasons, in circumstances where records of intellectual consumption are routinely generated – libraries, video rental memberships, and cable subscriptions – society has adopted legal measures to protect these records against disclosure. Privacy rights in information about intellectual activities and preferences preserve the privacy interest in (metaphoric) breathing space for thought, exploration, and personal growth".

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

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

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

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

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

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

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

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

accostato alla società prefigurata da Foucalt nella sua famosa rilettura dell'idea benthamiana del Panopticon[62].

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

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

La pubblicazione delle varie versioni delle specifiche TC ha sollevato questioni relative al trattamento dei dati personali. Nell'Unione Europea sono stati avanzati dubbi sulla

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

V. inoltre il sito Web del *Trusted Systems Project* all'URL: http://trusted-systems.info/, nel quale si legge: "Trusted systems for purposes of this research are systems in which some conditional prediction about the behavior of people or objects within the system has been determined prior to authorizing access to system resources. For example, trusted systems include the use of 'security envelopes' in national security and counterterrorism applications, 'trusted computing' initiatives in technical systems security, and the use of identity or credit scoring systems in financial and anti-fraud applications; in general, they include any system (i) in which probabilistic threat or risk analysis is used to assess 'trust' for decision-making before authorizing access or for allocating security resources against likely threats (including their use in the design of systems constraints to control behavior within the system), or (ii) in which deviation analysis or systems surveillance is used to insure that behavior within systems complies with expected or authorized parameters.. The adoption of these authorization-based security strategies (where the default state is DEFAULT=DENY) for counterterrorism and anti-fraud is helping accelerate the ongoing transformation of modern societies from a notional Beccarian model of criminal justice based on accountability for deviant actions after they occur, see Cesare Beccaria, On Crimes and Punishment (1764), to a Foucauldian model based on authorization, preemption, and general social compliance through ubiquitous preventative surveillance and control through system constraints. See Michel Foucault, Discipline and Punish (1975, Alan Sheridan, tr., 1977, 1995). In this emergent model, 'security' is geared not towards policing but to risk management through surveillance, exchange of information, auditing, communication, and classification. These developments have led to general concerns about individual privacy and civil liberty and to a broader philosophical debate about the appropriate forms of social governance methodologies. Our work in this area examines these issues".

compatibilità delle architetture TC con il quadro normativo derivante dalle direttive 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche. La discussione che ne è nata ha suscitato l'interesse del Gruppo di Lavoro per la Tutela dei Dati Personali istituito in base all'art. 29 della dir. 95/46/CE, il quale il 23 gennaio 2004 ha adottato il "Documento di lavoro sulle piattaforme fidate, in particolare per quanto riguarda il lavoro effettuato dal Trusted Computing Group (Gruppo TCG)"[63].

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

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

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

b) la funzione di *remote attestation* che si riconnette all'*Endorsement Key* e al ruolo della *Privacy Certification Authority* (che sarebbe uno degli strumenti deputato, nell'ambito delle specifiche TCG, a garantire la privacy degli utenti)[65].

---

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

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

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

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

Le specifiche dei TPM distinguono tra il ruolo del "proprietario dei diritti" e il ruolo dell'utente. Tale distinzione non ha conseguenze nell'ambito privato, nel quale il proprietario si identifica con l'utente, ma potrebbe sollevare talune questioni a livello di imprese. Nell'impresa il dipendente è l'utente, mentre il datore di lavoro è il proprietario. Il proprietario può prendere una serie di decisioni che riguardano il dipendente ed i dati personali che vengono trattati. In questo caso è responsabilità del proprietario (datore di lavoro) informare l'utente e garantire una tutela adeguata degli individui. La versione 1.2 delle specifiche ha introdotto alcuni miglioramenti di questa situazione aggiungendo un sistema di delega per le decisioni relative alle varie funzioni del TPM. Tuttavia, il proprietario dispone sempre del controllo finale e può decidere di delegare o no talune funzioni chiave. In tal caso non è possibile affermare (come fanno talune società TCG sul proprio sito Internet o nelle comunicazioni ufficiali) che gli individui hanno la totale libertà di accettare o no l'impiego del sistema. Allo stato attuale delle specifiche, la possibilità dell'utente di decidere di utilizzare o no una piattaforma con un TPM esisterebbe solo al di fuori dell'ambiente delle imprese. Peraltro occorre chiedersi per quanto tempo ancora. L'impiego di TPM, incoraggiato dall'industria, potrebbe diventare uno standard di fatto, un presupposto necessario per partecipare alla società dell'informazione. Ciò potrebbe avere conseguenze non solo per la tutela dei dati, ma anche per i diritti fondamentali come la libertà d'espressione[66].

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

Per limitare la trasmissione di identificatori e quindi la compilazione da parte di terzi di profili dell'utente, il gruppo TCG prevede la possibilità d'intervento da parte di un terzo fidato che certifica l'identità degli utenti e li conferma al corrispondente senza rivelare l'identità dell'utente. Il ruolo del terzo fidato (denominato anche "Privacy Certification Authority" dal TCG) deve essere studiato in dettaglio. La concentrazione di dati comporta sempre rischi supplementari e quindi vanno prese le dovute precauzioni. Per quanto riguarda i TPM esistono scenari in cui un unico terzo fidato controlla enormi quantità di informazioni di autenticazione. La versione 1.2 delle specifiche consente di evitare il terzo fidato mediante l'utilizzo della funzione di "Direct

---

authorization before participating in AIK credential issuance protocols. A TPM can further be disabled or deactivated to further control TPM use".

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

Anonymous Attestation (DAA)", che consente all'utente di creare una "Attestation Identity Key" (AIK- chiave di attestazione dell'identità) senza presentare la chiave di approvazione (*Endorsement Key*, EK), che è un identificatore univoco. Il Gruppo di Lavoro ritiene che si tratti di un miglioramento, ma sottolinea che la scelta tra terzo fidato e DAA sarà fatta a livello di applicazioni. Le specifiche attuali permettono ancora le due funzioni. La DAA è quindi una possibilità supplementare, ma non una caratteristica standard del sistema. Il Gruppo di Lavoro ritiene che l'introduzione della funzione DAA costituisca un miglioramento, ma ricorda che non si può più parlare di anonimato quando è possibile creare un legame con l'identità dell'utente o delineare profili degli utenti. Il Gruppo di Lavoro invita il TCG a promuovere l'impiego di tale funzione in modo da tutelare la privacy ed i dati, cioè facendo leva su *random identifiers* e limitando l'uso dei nomi al periodo più breve possibile nei casi in cui sia necessaria la revoca o l'identificazione. Il Gruppo di Lavoro ribadisce l'importanza della fiducia nei sistemi basati sui TPM. La fiducia deve esistere in tutta la catena degli operatori interessati, da chi realizza specifiche, al venditore delle applicazioni fino all'utente del sistema. È necessario tutelare i dati in tutte le fasi[67].

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

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

- introdurre meccanismi volti a controllare che l'applicazione delle specifiche TCG rispettino le leggi in materia di tutela dei dati personali (ad esempio, "[l]a creazione di un logo o di un programma di certificazione riguardante la conformità dei prodotti è stata proposta nel corso del dialogo con i membri del gruppo TCG")[69].

Successivamente, il TCG ha pubblicato nel maggio 2005 un documento intitolato "Design, Implementation, and Usage Principles for TPM Based Platforms"

---

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

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

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

che in qualche modo risponde alle critiche avanzate da più parti[70].

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

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

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

- Scelta ("Choice): il proprietario di sistemi TCG dovrebbe disporre di una reale scelta e del controllo circa il trasferimento di informazioni personali. Gli utenti di sistemi TCG dovrebbero poter disabilitare le funzionalità TCG in modo da non violare le policy del proprietario e al tempo stesso da avere il controllo sul trasferimento di informazioni personali.

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

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

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

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

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

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

necessario.

- Proporzionalità ("Proportionality"): i dati personali raccolti e trasferiti attraverso funzionalità TCG devono essere rilevanti e non eccessivi rispetto agli scopi per i quali sono stati raccolti. La chiavi private, che giocano un ruolo fondamentale nella piattaforma, non dovrebbero mai essere rivelate. La proporzionalità è parte fondamentale del modello di sicurezza rispondente alle specifiche TCG. Il TPM TCG incorpora un unico duraturo e stabile identificatore chiamato *Endorsement Key* (EK). Dal momento che il TPM è legato alla piattaforma, la EK diventa un'informazione relativa ad una persona identificabile. Al fine di ridurre la capacità di aggregare dati personali, le specifiche TCG proibiscono l'uso generalizzato della EK. Le stesse specifiche richiedono che la EK sia invece utilizzata per generare degli *alias* che non devono essere riconducibili esplicitamente all'EK. Questo obiettivo può essere raggiunto in vari modi, tra i quali figurano l'utilizzo di *zero-knowledge protocols*, di una *Privacy Certification Authority*, l'utilizzo congiunto di *zero-knowledge protocols* e di una *Privacy Certification Authority*, etc. L'uso di questi strumenti protegge la privacy dell'utente rendendo più difficile l'aggregazione dei dati. Il TCG raccomanda che le implementazioni e gli sviluppi di sistemi TCG consentano il più alto livello di anonimato da ritenersi appropriato rispetto ad una determinata situazione.

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

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

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

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

5. Conclusioni

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

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

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

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

c) La forza di una regola giuridica dipende da vari fattori, tra i quali spicca il grado di condivisione che la stessa incontra nella comunità di riferimento. La forza di una regola informatica dipende essenzialmente dalla sua efficacia tecnologica (ad esempio, l'architettura TC può essere considerata efficace solo se è virtualmente

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

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

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

impossibile "rompere" gli algoritmi crittografici sui quali si basa), nonché dal suo grado di diffusione (ad esempio, l'architettura TC potrà dirsi davvero condizionante del comportamento umano solo se e quando assurgerà a standard tecnologico accettato da una moltitudine di utenti). La diffusione di uno standard è cosa diversa dalla condivisione di una regola giuridica.

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

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

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

L'architettura TC costituisce la dimostrazione paradigmatica di quanto ora rilevato circa la natura delle regole informatiche e del processo che le produce. Il lavoro del TCG e dell'organizzazione che l'ha preceduto è iniziato lontano dai riflettori dei media e dalla discussione politica. Sebbene il TCG si occupi del primissimo stadio di sviluppo dell'architettura informatica, cioè delle specifiche che poi dovranno essere tradotte nelle molte componenti tecnologiche di riferimento, le sue decisioni delineano i valori che prevalgono all'interno della stessa architettura. Nonostante l'ambiguità del linguaggio utilizzato nelle specifiche, risulta evidente che i valori che sono a ridosso della privacy sono sacrificati a vantaggio di una certa visione della sicurezza informatica. In particolare, la limitazione preventiva di funzionalità e la dislocazione del controllo dei sistemi informatici delineano un ambiente digitale dove la sicurezza è ottenuta al prezzo della compressione *ex ante* dei margini di libertà legati alle dimensioni spaziale e informazionale della privacy. Si tratta di scelte di fondo che ben

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

difficilmente potranno essere riviste, se non nell'ottica di rivoluzionare la logica TC e dare avvio ad una nuova architettura della sicurezza. D'altra parte, il processo di traduzione in applicazioni hardware e software è già in moto (inerziale) da tempo e segue le dinamiche di standardizzazione tipiche dell'industria informatica. Il dialogo avviato tra TCG ed alcune istituzioni politiche (come il Gruppo di Lavoro per la Tutela dei Dati Personali) può portare solo ad alcuni miglioramenti marginali dell'architettura. Ad esempio, la possibilità di disattivare le funzionalità TC, che viene spesso indicata come la garanzia del mantenimento del controllo del TC, appare come un'arma tanto irrinunciabile quanto spuntata. In un ambiente digitale colonizzato dalla logica TC e dunque dalla limitazione (fisica e) preventiva dei margini di manipolabilità dei sistemi informatici, tale possibilità potrebbe rivelarsi del tutto illusoria.

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