LA NUOVA FRONTIERA DEL CONTROLLO GLOBALE: IL TRUSTED COMPUTING, FRA INVOLUZIONE INFORMATICA E CRITICITÀ GIURIDICHE

Gianluigi Fioriglio[*]

SOMMARIO: 1. CENNI INTRODUTTIVI – 2. IL *TRUSTED COMPUTING:* ASPETTI GENERALI – 3. LE IMPLICAZIONI DEL *TRUSTED COMPUTING* – 4. CONSIDERAZIONI GENERALI SU DIRITTO E INFORMATICA – 5. DALLA TUTELA DELLA PROPRIETÀ INTELLETTUALE AL CONTROLLO GLOBALE – 6. *TRUSTED COMPUTING* E MONOPOLI – 7. INVOLUZIONE INFORMATICA E CRITICITÀ GIURIDICHE

1. Cenni introduttivi

Negli ultimi decenni l'informatica ha avuto uno sviluppo repentino ed inarrestabile. Da patrimonio di pochi eletti è diventata sempre più di massa, ed il *target* di riferimento dei prodotti informatici appare quanto mai vario, poiché abbraccia fasce ben diverse, dalle piccole aziende alle multinazionali, dagli uffici periferici alle burocrazie centrali, dai piccoli laboratori ai grandi centri di ricerca, dagli individui meno abbienti a quelli più ricchi. Tali modificazioni sul fronte della domanda si sono riverberate, ovviamente, anche su quello dell'offerta, diventata sempre più di massa, e così soprattutto il mercato del *software* è oggi dominato da grandi aziende che oltretutto in taluni settori operano in un regime di monopolio di fatto.

In un futuro non troppo remoto, inoltre, diventeranno realtà i sistemi informatici integrati che permetteranno la gestione non solo di singoli elettrodomestici ma addirittura di intere abitazioni sotto ogni loro aspetto. Attualmente è possibile controllare intere catene di produzione industriale tramite robot gestiti da *software* creato *ad hoc* (*software* c.d. proprietario); la diminuzione dei costi di produzione degli strumenti elettronici consentirà una aumentata intrusione dei sistemi informatici nella vita di tutti i giorni, come è già avvenuto per i personal computer.

Difatti, nonostante fino al recente passato l'idea stessa di case elettroniche i cui componenti dialoganо reciprocamente e si connettono alle reti telematiche fosse patrimonio quasi esclusivo degli scrittori di fantascienza, oggi si moltiplicano gli esempi di prototipi realmente funzionanti che saranno commercializzati negli anni a venire quando il naturale abbassamento dei costi di produzione ne consentirà la distribuzione di massa.

Gli aspetti benefici della gestione automatizzata di numerose attività tediose oggi svolte dall'uomo sono *in re ipsa*; tuttavia, non bisogna pretermettere una valutazione *ex ante* delle probabili conseguenze negative, in quanto l'ulteriore sviluppo della rete Internet e l'interconnessione fra apparecchiature diverse (dal computer al telefono cellulare, dall'impianto *hi-fi* agli elettrodomestici) appaiono astrattamente idonei ad aumentare ancor di più il controllo che già oggi viene effettuato su ciascun individuo, e ciò sia a livello statuale che privato.

[*] Dottore di ricerca. Docente di Informatica nell'Università di Roma "La Sapienza", Facoltà di Scienze Politiche, Polo di Pomezia.

Già i noti casi *Echelon*[1] ed *Information Awareness Office*[2] rendono palese come l'uomo moderno sia un "uomo di vetro". Tale efficace espressione, usata sempre più spesso negli ultimi anni, chiarisce come tutti noi siamo sempre più esposti agli occhi indiscreti del mondo esterno. Inoltre, l'evoluzione della tecnologia porterà, qualora non correttamente instradata, alla mutazione dei solidi domicili materiali in "case di vetro" ed alla sempre più forte connotazione della società moderna quale "società sorvegliata"[3]. Ciò desta tanto più stupore qualora si consideri che la limitazione della libertà umana è usualmente connaturata ai regimi totalitari e dovrebbe essere ripudiata dai moderni stati democratici, che invece si rendono protagonisti di violazioni di quegli stessi principi di libertà che dovrebbero tutelare, come nelle fattispecie appena richiamate.

L'*homo technologicus*, dunque, non trarrà alcun giovamento dal chiudere l'uscio di casa, perché nell'era informatica le barriere materiali possono agevolmente essere superate, e l'avvento del c.d. *Trusted Computing* (d'ora in poi, TC) porterà, insieme a questa, conseguenze ben più gravi.

2. Il Trusted Computing: *aspetti generali*

Il TC non è certo un argomento di dominio pubblico, nonostante sia idoneo ad incidere profondamente sulla vita di chiunque utilizzerà un qualsiasi prodotto elettronico di nuova generazione nei prossimi anni[4]. La discussione in merito è infatti sorta soprattutto su riviste specializzate, siti Internet e gruppi di discussione (*newsgroups*) e non sembra estendersi oltre. Ciò non sembra dovuto, unicamente, alla specificità ed al tecnicismo intrinseci all'argomento, la cui piena comprensione richiede, quanto meno, la conoscenza dei principi strutturali di funzionamento di un sistema informatico. Probabilmente anche la "forza" dei soggetti che stanno portando avanti il progetto contribuisce a sopire le eventuali discussioni in merito, mentre i suoi numerosi cambi di denominazione, unitamente alle solenni dichiarazioni degli stessi soggetti su di esso, contribuiscono ad aumentare la confusione in materia.

Tale progetto è portato avanti da un consorzio denominato *Trusted Computing Group* (TCG), fondato nel 2003 e composto dalle maggiori aziende del settore. Membri promotori sono AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft, Sun. Fra gli altri membri si possono qui ricordare Dell, Lexmark, Motorola, Nokia, Philips, Samsung, Siemens, Sony, Vodafone. Il TCG, invero, era già stato fondato nell'ottobre del 1999 da Microsoft, IBM, Intel[5], Compaq e HP con lo

---

[1] Echelon è un sistema di sorveglianza globale creato nel 1948 da Stati Uniti, Nuova Zelanda, Gran Bretagna, Canada e Australia, nel quadro del c.d. patto UKUSA. Su di esso cfr., fra gli altri, la relazione del Parlamento europeo 2001/2098 (INI) "sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione ECHELON)" (reperibile *on line* all'URL http://www.privacy.it/ueechelon.html), nonché i seguenti testi: D. CAMPBELL, *Il mondo sotto sorveglianza: Echelon e lo spionaggio elettronico globale*, tr. it., Eleuthera, Roma, 2003; N. HAGER, *Secret Power - New Zealand's Role in the International Spy Network*, Craig Potton Publishing, Nelson, New Zealand, 1996; K. J. LAWNER, *Post-Sept. 11th International Surveillance Activity – A Failure of Intelligence: the Echelon Interception System & the Fundamental Right to Privacy*, in *Pace International Law Review*, 2002, 14, pp. 435-480; L. D. SLOAN, *Echelon and the Legal Restraints on Signals Intelligence: a Need for Reevalution*, in *Duke Law Journal*, 2001, 50, pp. 1467-1510.

[2] L'Information Awareness Office era stato costituito negli Stati Uniti nell'ambito del Defence Advanced Research Project Agency al fine di sviluppare le tecnologie di sorveglianza e controllo globale più avanzate al mondo. Le numerose proteste suscitate da un così palese intento hanno spinto nel 2003 gli Stati Uniti a chiudere ufficialmente tale progetto. Per maggiori approfondimenti sia consentito rinviare a G. FIORIGLIO, *La privacy e i sistemi di controllo e di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2002, 1, http://www.lircocervo.it.

[3] Sul punto cfr. D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, tr. it., Feltrinelli, Milano, 2003.

[4] Dunque, si ribadisce, non solo un personal computer, ma anche oggetti di uso ancor più comune, come i telefoni cellulari, i lettori DVD, i forni a microonde, le lavatrici, ecc. Ovviamente i *chip* che garantiranno il funzionamento del *trusted computing* saranno introdotti prima nei sistemi più avanzati tecnologicamente e, in una fase successiva, anche nell'elettronica di consumo a più ampia diffusione.

[5] La Intel non è nuova ad iniziative come quella di cui trattasi: nel 1993 aveva infatti introdotto il concetto del numero di serie per ogni microprocessore (CPU, Central Processing Unit), integrato nei primi esemplari di Pentium III; ciò

scopo dichiarato di migliorare la sicurezza dei sistemi informatici e, all'epoca, era denominato *Trusted Computing Platform Alliance*. Appare evidente che le società appena citate[6] sono perfettamente in grado di piegare ai propri voleri l'andamento dello specifico settore di mercato in cui operano, potendo facilmente imporre ai loro potenziali clienti (grandi e piccoli) l'acquisto di beni e/o l'acquisto di servizi rispondenti a certe caratteristiche da loro definite: se dovessero essere prodotti solo sistemi rispondenti alle specifiche TCG è ovvio che l'acquirente di apparecchiature informatiche (e non) non avrebbe alcuna scelta, perché sarebbe il mercato a stabilire cosa poter acquistare.

Di fatto, ciascun sistema rispondente alle specifiche del TCG includerà un *microchip*, denominato ufficialmente *Trusted Platform Module* (TPM) ma noto con il nome di *Fritz*, che contiene una chiave crittografica. Tutte le informazioni che attraverseranno il sistema saranno criptate da questa chiave e, dunque, qualsiasi dato dovrebbe essere vagliato dal TPM, che avrebbe, quindi, il controllo totale del sistema. Pertanto, il legittimo utilizzatore di un sistema (inteso in senso lato) viene spogliato del controllo immediato su ciò che si svolge in esso; il controllo mediato viene inoltre trasferito ai produttori del sistema. È bene ricordare ancora una volta, per dar conto dell'ampiezza della questione, che tale *chip* sarà incluso non solo nei computer, che talora già oggi lo ospitano, ma anche in telefoni cellulari, elettrodomestici, e così via.

Le "funzionalità" del TC non saranno tuttavia affidate unicamente al TPM, le cui capacità saranno presumibilmente estese da altre tecnologie attualmente in corso di sviluppo, come "LaGrande Technology" di Intel e "Presidio" di AMD[7].

Ovviamente la creazione del TC, per quanto portata avanti dai soggetti denominati in precedenza, deve quanto meno trovare una giustificazione plausibile ed astrattamente sostenibile, che, nel caso di specie, fa leva sul diffuso senso di sfiducia nei confronti della sicurezza dei sistemi informatici: *"Concerns about the security of communications, transactions, and wireless networks are inhibiting realization of benefits associated with pervasive connectivity and electronic commerce. These concerns include exposure of data on systems, system compromise due to software attack, and lack of user identity assurance for authorization. The latter concern is exacerbated by the increasing prevalence of identify theft. In addition, as users become more mobile, physical theft is becoming a growing concern. Users and IT organizations need the industry to address these issues with standards-based security solutions that reduce the risks associated with participation in an interconnected world while also ensuring interoperability and protecting privacy*"[8].

Pertanto, a detta del TCG, la diffusione del TC dovrebbe consentire la sconfitta di fenomeni come i *virus* informatici ed il furto di identità, fra cui il c.d. *phishing*[9], restituendo agli utilizzatori la *fiducia* (*trust*) nei confronti del sistema informatico. Del resto, la progettazione, l'implementazione e l'utilizzo del TC dovrebbero essere ispirati al rispetto di diversi principi (sicurezza, *privacy*, interoperabilità, portabilità dei dati, controllabilità, facilità di utilizzo), così come chiarito dal

---

avrebbe appunto permesso di identificare ogni personal computer e dunque potenzialmente anche il proprietario dello stesso. Le forti critiche hanno spinto poi l'azienda statunitense a tornare sui propri passi.

[6] Le aziende citate nel testo sono solo una piccola parte di quelle che compongono il TCG: per una lista completa cfr. https://www.trustedcomputinggroup.org/about/members/.

[7] Sul punto, cfr. A. BOTTONI, *Blindature oltre il TPM*, in *Punto Informatico*, 2006, 2471, http://punto-informatico.it/p.asp?i=57677; INTEL CORPORATION, *LaGrande Technology Architectural Overview*, 2003, http://download.intel.com/technology/security/downloads/LT_Arch_Overview.pdf;

[8] TRUSTED COMPUTING GROUP, *Backgrounder*, 2005, in https://www.trustedcomputinggroup.org/downloads/background_docs/TCGBackgrounder_revised_012605.pdf.

[9] La tecnica nota con questo nome consiste nell'inviare messaggi di posta elettronica ingannatori tesi a portare il lettore a comunicare al *phisher* dati assai delicati come il proprio numero di carta di credito, il proprio nome utente e *password*, e così via. Solitamente i messaggi di posta elettronica sembrano provenire da un istituto di credito o da siti di aste *on line* e consistono nella richiesta, fatta al cliente, di comunicare nuovamente i propri dati seguendo un collegamento che sembra portare al sito ufficiale, ma che in realtà porta l'incauto utente a siti simili in tutto e per tutto a quelli "istituzionali". Una volta acquisite le informazioni, il *phisher* le utilizzerà per i propri fini (ad esempio, trasferendo denaro sul proprio conto corrente).

TCG[10]. Tuttavia, la creazione di sistemi rispondenti a tali specifiche, con ogni probabilità, potrebbe portare a conseguenze opposte, soprattutto in tema di tutela della riservatezza.

3. Le implicazioni del Trusted Computing

Il TC, come si è visto, si concretizza nel controllo delle informazioni che sono memorizzate o che transitano in un sistema informatico, ivi compresi i siti *web*. Il sistema può, dunque, impedire l'installazione sul proprio personal computer di *software* non certificato, così come è in grado di bloccare l'accesso a *file* o documenti non *trusted*; lo stesso principio verrà applicato anche alle modalità di svolgimento della navigazione su Internet, con la conseguenza che sarà possibile visitare solo quei siti che abbiano ottenuto la certificazione, mentre gli altri non saranno accessibili. Una simile limitazione della libertà individuale è, chiaramente, inconcepibile ed ingiustificabile.

Orbene, anche se innumerevoli tentativi sono stati fatti e sono per lo più falliti per limitare la libertà informatica in Rete, in questo caso potrebbe ottenersi una censura *ab origine* dei siti che, in via astratta e discrezionale, non rispondano ad imprecisati ed arbitrari criteri di sicurezza e di rispetto della *privacy*. Con precipuo riferimento proprio a quest'ultimo aspetto, giova tuttavia ricordare che sinora le aziende *leader* del settore hanno tutelato questo diritto solo di facciata, ponendo in essere palesi violazioni dello stesso. Basti pensare alla questione del "lettore multimediale" integrato in Microsoft Windows, che è identificato da un numero univoco per ogni elaboratore; se nel momento in cui l'utente utilizza tale *software* il computer è collegato ad Internet, il programma effettua automaticamente alcune operazioni, come il controllo degli aggiornamenti dello stesso o il reperimento dei titoli dei *file* musicali memorizzati nel computer. Le relative informazioni confluiscono in un *database*, consentendo la ricostruzione delle preferenze di *quel singolo utente*, permettendone la profilazione[11]. Anche se è possibile disabilitare questa funzione, bisogna considerare che su tematiche così specifiche sarebbe necessario fornire una corretta informazione nei confronti dell'utenza e, comunque, evitare di preimpostare simili opzioni.

L'esempio ora citato fa capire quanto già oggi si possa verificare un controllo occulto delle azioni effettuate da ciascun utilizzatore di un personal computer, ma i futuri e potenziali rischi di lesione della libertà informatica e della riservatezza degli utenti appaiono assai gravi qualora si tengano presenti le modalità di funzionamento del TC, di cui si è detto in precedenza. Si consideri, infatti, che lo spostamento dell'asse del controllo di ciascun sistema dall'utilizzatore al produttore comporta, altresì, che quest'ultimo assuma anche il ruolo di controllore dei dati personali ivi memorizzati stabilmente od anche temporaneamente. La lesione della riservatezza è, dunque, palese ed appare idonea a realizzarsi non solo quando le informazioni sono trattate da sistemi intuitivamente idonei a cagionarle, come computer o telefoni cellulari, ma anche qualora esse siano inerenti alle attività umane svolte quotidianamente per mezzo di apparecchi di uso comune come gli elettrodomestici, il cui utilizzo potrebbe essere monitorato dall'esterno.

Quanto detto sinora, comunque, non implica *ex se* una valutazione negativa del fine che, in via astratta, si vuole perseguire con l'introduzione del TC, in quanto esso è, in linea di principio, meritevole di tutela: assicurare elevati livelli di sicurezza informatica nella più ampia accezione possibile. Si afferma, infatti, che grazie al TC sarebbe possibile effettuare una crittazione dei dati secondo metodologie ben più sicure di quelle odierne, assicurandone dunque la confidenzialità e la protezione da accessi abusivi; potrebbe essere sconfitto il fenomeno dello *spamming*, ossia del ricevimento di e-mail "spazzatura"; ancora, il *software* dovrebbe essere più sicuro in quanto sottoposto a particolari processi di rispondenza alle specifiche tecniche. Dal punto di vista informatico, comunque, tutto ciò non risponde a verità: attualmente i dati possono essere crittati secondo numerose metodologie grazie all'ausilio di chiavi di cifratura e di decifratura, senza il

---

[10] TCG BEST PRACTICES COMMITTEE, *Design, Implementation, and Usage Principles (Version 2.0)*, 2005, in https://www.trustedcomputinggroup.org/specs/bestpractices/Best_Practices_Principles_Document_V2_0.pdf.

[11] Sulla profilazione cfr. G. MACCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitarie* online *e tutela della privacy*, in *Il diritto dell'informazione e dell'informatica*, 2001, 3, pp. 425-444.

bisogno di aderire alle specifiche del TCG ed utilizzando anche *software* gratuito e/o *open source*[12]. Con riferimento allo *spamming*, non è ben chiara l'innovazione rispetto a strumenti come i cc.dd. filtri, che permettono di decidere quali messaggi ricevere e quali cancellare *ab origine* con un procedimento totalmente trasparente per l'utente e valutabile anche *ex post* mediante la verifica dell'operato dei filtri medesimi. Infine, l'ultimo aspetto riguarda una tematica ben più vicina all'aspetto della programmazione del *software* che all'introduzione di specifiche nuove che in realtà non influiscono su quelle caratteristiche di stabilità e di buon funzionamento che sono attinenti al c.d. *kernel*[13] del sistema operativo

Il fine della sicurezza si può quindi attualmente raggiungere in altri modi senza per questo limitare la libertà dell'utente, il quale non potrebbe decidere l'organizzazione ed il funzionamento del proprio sistema informatico secondo criteri autonomamente determinati, ma piuttosto secondo principi stabiliti da altri soggetti, che se oggi riguardano soprattutto il settore informatico, in futuro assumeranno ancora maggior importanza in virtù delle accennate e progressive informatizzazione ed automatizzazione delle attività quotidiane.

Appare chiaro, quindi, che, da un punto di vista più generale, chiunque controllasse il sistema ideato dal TCG accentrerebbe in sé un potere enorme[14], essendo l'unico punto di controllo di tutte le moderne apparecchiature rispondenti alle specifiche stabilite dal TCG. Concedere un potere di verifica ad entità anche sovranazionali non allevierebbe di certo il problema, perché verrebbe creato una sorta di "grande fratello" in grado di controllare tutti i dati che circolano per via informatica, comprese dunque anche le *e-mail*, la cui segretezza, in Italia ed in altri paesi, è tutelata in massimo grado. A titolo esemplificativo, si consideri che l'art. 15 Cost. dispone che "la libertà e la segretezza delle comunicazioni sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".

Si è anche proposto di concedere, direttamente, le chiavi di decrittazione ad organismi, enti od istituzioni statali, come ad esempio l'FBI: ciò violerebbe, comunque, la citata disposizione costituzionale che sancisce l'inviolabilità delle comunicazioni, perché concederebbe una sorta di "mandato generale" al controllo delle informazioni personali di ciascun individuo, in palese violazione, altresì, della normativa sulla *privacy*. Le deroghe a questo principio sono tassative e solo l'autorità giudiziaria è legittimata a farlo in casi concreti, non essendo possibile che l'eccezione diventi regola. Come se ciò non bastasse, è stata addirittura avanzata la proposta che *soggetti diversi dall'utente (proprietario del sistema* hardware *nonché legittimo utilizzatore del* software*)*, abbiano le *root keys* che permettono un controllo assoluto sul sistema: è assolutamente palese l'illiceità di una simile proposta. Oltretutto, l'interconnessione dei sistemi informatici a livello mondiale darebbe la possibilità a soggetti stranieri di controllare dati personali sui quali non ha potere neanche lo Stato nazionale se non nei limiti previsti dalla legge.

Le conseguenze negative dell'implementazione del TC non potrebbero evitarsi concedendo la possibilità di disattivare il sistema, perché si forzerebbero comunque gli utenti ad utilizzarlo disabilitando al contempo funzioni essenziali: in altri termini, si svuota di qualsiasi significato e contenuto la "concessione" di tale libertà. Inoltre, affinché il TC sia operativo è necessario che il *software* sia scritto appositamente per sfruttarlo: ne consegue che se esso dovesse diventare uno standard, tutti i programmi sarebbero adeguati ad esso, con la conseguenza ulteriore che se il singolo utente decidesse di disattivare il sistema, il *software* non potrebbe funzionare. Pertanto, gli utenti potranno scegliere se attivare il TC ed utilizzare il nuovo programma oppure disattivarlo ed utilizzare il *software* scritto in precedenza, rinunciando dunque alle nuove funzionalità.

---

[12] V. gli specifici riferimenti in R. STALLMAN, *Can you trust your computer?*, in http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19. Tale contributo è altresì presente in J. GAY (edited by), *Free Software, Free Society: Selected Essays of Richard M. Stallman*, GNU Press, Boston, Massachusetts, 2002 (il volume è disponibile gratuitamente *on line* all'URL http://www.gnu.org/philosophy/fsfs/rms-essays.pdf).

[13] Ossia il "cuore" del sistema operativo: fornisce quelle che vengono poi utilizzate dagli altri programmi, evitando che essi debbano colloquiare direttamente con l'*hardware*.

[14] R. ANDERSON., *TCPA FAQ*, in http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html.

Nell'ipotesi da ultimo citata, tuttavia, i produttori potrebbero decidere che dopo la scadenza delle autorizzazioni l'accesso ai dati creati con programmi autorizzati dal TCG venga impedito dal sistema oppure che i dati non siano accessibili da chi non possiede un sistema considerato *trusted*. In tutta evidenza, ciò costringerebbe chiunque, volente o nolente, ad adeguarsi, stante la sempre maggiore importanza nella vita quotidiana, lavorativa e non, dei sistemi informatici e delle informazioni in formato digitale.

4. Considerazioni generali e preliminari su diritto e informatica

L'avvento del TC reca con sé la nascita di nuove problematiche che toccano il delicato ambito disciplinare costituito dall'intersezione fra il mondo del diritto e quello dell'informatica. Tali questioni possono talora essere proficuamente affrontate e risolte solo in seguito ad un'operazione di ripensamento delle tradizionali categorie giuridiche che le adegui, poi, alle mutate necessità della società moderna oppure ne crei di nuove qualora ciò si renda necessario. Questi, però, sono compiti improbi, forse perché impongono la considerazione o la teorizzazione di diritti non ancora metabolizzati dalla coscienza sociale, probabilmente a causa della repentina crescita del livello tecnologico. Ciò appare ancor più difficoltoso in relazione ai profili giuridicamente rilevanti del TC; tuttavia, prima di esaminarli, sembra utile riflettere brevemente sullo strano atteggiarsi del diritto dinanzi a fattispecie che sono in qualche modo collegate all'informatica.

Muoviamo da un caso ipotetico: Tizio acquista un armadio di gran pregio dal mobiliere Caio. Giunto nella propria abitazione, decide di non utilizzarlo nella propria stanza da letto per riporvi i propri indumenti, ma lo sistema nella propria cantina al fine di conservarvi i propri attrezzi da *bricolage*. Caio non potrà dolersi del fatto che Tizio non stia utilizzando l'armadio per il fine suo proprio: il diritto non riconosce alcuna posizione giuridica soggettiva a Caio, che non è più proprietario dell'armadio in questione. Ai sensi dell'art. 832 cod. civ., del resto, "il proprietario ha diritto di godere e disporre delle cose in modo pieno ed esclusivo, entro i limiti e con l'osservanza degli obblighi stabiliti dall'ordinamento giuridico".

Prendiamo, ora, in esame una fattispecie del tutto identica nei suoi elementi essenziali, stavolta riferita al settore informatico. Tizio acquista una *console* per videogiochi da Sempronio; perfezionato l'acquisto, si rende conto che il bene appena acquistato presenta determinate limitazioni e che nonostante sia dotato di un disco rigido e contenga componenti che consentirebbero, in astratto, di installarvi un sistema operativo Linux, ciò non può esser fatto perché il produttore della *console* ha impedito tale possibilità. Egli, però, viene a sapere che sono in vendita determinati *chip* che consentono di superare detta limitazione e decide, dunque, di acquistarne uno e di installarlo sulla propria macchina, anche se consapevole che in tal modo non potrà più godere della garanzia del produttore. Come nel caso dell'armadio, Tizio è proprietario dell'oggetto legittimamente acquistato e, pertanto, dovrebbe poter goderne e disporne in modo pieno ed esclusivo. Eppure, i produttori delle *console* da gioco hanno intentato numerose cause per sconfiggere detto fenomeno (dei c.d. *modchip*), ritenendo di poter disporre ulteriormente dei prodotti di cui *già* hanno disposto ponendoli in vendita e acquisendo il corrispettivo. Si potrebbe replicare affermando che la *console* potrebbe essere utilizzata per fini illeciti e dunque ciò giustificherebbe una sorta di controllo globale attribuito a determinati soggetti. Tuttavia, anche altri oggetti sono utilizzabili a fini illeciti e di un tale potere mai si è parlato. A mero titolo esemplificativo si pensi ai coltelli, certamente idonei a ledere beni giuridici, come la vita e la salute dell'uomo, ben più importanti di quelli tutelati con veemenza forse eccessiva dalle attuali normative sul diritto d'autore.

Negli Stati Uniti è in vigore il contestato *Digital Millennium Copyright Act* (DMCA), ai sensi del quale essi devono ritenersi illegali, perché consentono di aggirare i sistemi di protezione[15].

[15] Sul DMCA cfr., fra gli altri, J. P GINSBURG, *Il "Digital Millennium Copyright Act" ed il "Sonny Bono Copyright Term Extension Act": due novità dagli Stati Uniti*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 1999, 7-8, pp. 625-668; P. MARZANO, *Diritto d'autore e digital technologies. Il Digital Copyright nei*

In Italia, tuttavia, la giurisprudenza di merito si è di recente pronunciata su una fattispecie simile, ritenendo che i sistemi di protezione contenuti nelle *console* costituiscono ingiustificate limitazioni alla facoltà di godimento di tali beni che i singoli utenti hanno legittimamente acquistato, per cui i dispositivi che consentono di aggirarle non violano alcuna disposizione legislativa[16].

Tanto premesso, è bene precisare che in questa sede non si vuole analizzare compiutamente il fenomeno dei *modchip*, che è stato tuttavia richiamato al fine di evidenziare come fattispecie del tutto simili nei loro elementi essenziali vengano valutate in maniera diversa a seconda dei diversi interessi in gioco anche quando tale valutazione non dovrebbe e non potrebbe essere compiuta. Soprattutto, è d'uopo sottolineare che sovente le aziende operanti nel settore informatico avanzano pretese inconcepibili, chiedendo e talvolta ottenendo una tutela assolutamente sproporzionata rispetto al bene giuridico astrattamente tutelabile: in questo senso si veda la tutela penale riservata al *software*, di cui al d.lgs 29 dicembre 1992, n. 518 ed alla l. 18 agosto 2000, n. 248[17], ma soprattutto le contestate norme di cui al d.l. 22 marzo 2004, n. 72, meglio noto come "decreto Urbani" (dal nome del ministro proponente), ed alla relativa legge di conversione (l. 21 maggio 2004, n. 128)[18], nonché alle successive disposizioni di cui al d.l. 31 gennaio 2005, n. 7, poi convertito, con modificazioni, in l. 31 marzo 2005, n. 43.

---

trattati OMPI, nel DMCA e nella normativa comunitaria, Giuffrè, Milano, 2005; T. A. MITCHELL, *Copyright, Congress and Constitutionality: how the Digital Millennium Copyright Act Goes Too Far*, in *Notre Dame Law Review*, 2004, 79, pp. 2115-2182; E. MORELATO, *Strumenti informatici per la protezione del diritto d'autore*, in *Contratto e impresa*, 2001, 2, pp. 731-759; P. MOORE, *Steal this disk: Copy protection, consumers' rights, and the Digital Millennium Copyright Act*, in *Northwestern University Law Review*, 2003, 97, 3, pp. 1437-1470; P. SAMUELSON, *Anticircumvention Rules: Threat to Science*, in *Science*, 2001, pp. 2028-2031.

[16] Sul punto merita una particolare menzione la sentenza 20 dicembre 2005 del Tribunale di Bolzano (reperibile all'indirizzo Internet http://www.interlex.it/testi/giurisprudenza/bz051220.htm), che si è pronunciata sulla presunta violazione dell'art. 171 *ter*, lett. F-*bisi*, l. aut., da parte di un'azienda che aveva venduto *chip* di modifica della *console* Sony Playstation 2. Tali componenti consentono di superare determinate limitazioni, come l'impossibilità di riprodurre film od eseguire videogiochi di area geografica diversa rispetto all'Italia, nonché di eseguire copie di videogiochi. Nel caso di specie, il pubblico ministero aveva portato avanti la tesi normalmente sostenuta da Sony e dalle altre aziende del settore secondo cui tali *chip* sono idonei ad incitare alla violazione del diritto d'autore. Come correttamente sostenuto dai difensori della ditta imputata, tuttavia, i produttori di *hardware* non possono impedire all'acquirente del loro prodotto di utilizzarlo come meglio ritengono, ivi compresa la possibilità di sfruttarne lecitamente tutte le potenzialità, comprese quelle artatamente limitate o rese inaccessibili dai produttori medesimi. Si tenga presente, inoltre, che la stessa ditta aveva avvisato gli acquirenti dei *chip* incriminati che essi potevano essere utilizzati anche a fini illeciti e che in tal caso essa si sollevava da qualsiasi responsabilità. Il Tribunale di Bolzano ha, giustamente, assolto con formula piena il titolare della ditta summenzionata. Precedentemente, comunque, il Tribunale del riesame di Bolzano aveva già rilevato, pronunciando sulla medesima fattispecie, che l'utilizzo degli anzidetti *chip* è del tutto legittimo, in quanto la legge sul diritto d'autore non può impedire a chi acquista un bene di goderne nel modo più ampio ed esclusivo. In senso contrario si era però pronunciato il medesimo Tribunale, con sentenza n. 138/05 del 28 gennaio 2005 (reperibile *on line* all'URL http://www.interlex.it/testi/giurisprudenza/bz050128.htm). Detta decisione, resa da un altro magistrato, è però basata su presupposti fattuali palesemente errati (ad esempio: "I videogiochi invece non sono costituiti da solo software (come sostenuto dalla Difesa), dato che si basano su di un programma che permette il funzionamento delle immagini, dei suoni e dei testi, ma rappresentano delle vere e proprie opere d'ingegno"). Come ha affermato Andrea Monti, "stiamo parlando veramente di una brutta sentenza. Rispettabile – anche se non condivisibile – la diversità di opinioni sull'applicazione della legge. Ma che almeno il dissenso sia basato sulla corretta cognizione della realtà fattuale" (*Decisioni opposte sullo stesso fatto: quale è corretta?*, in *Interlex*, http://www.interlex.it/copyright/amonti83.htm).

[17] Sulla legge 248/00 cfr., fra gli altri, G. GABRIELE, *Il diritto d'autore tra vecchie e nuove formulazioni (l. 18 agosto 2000, n. 248)*, in *Le nuove leggi civili* commentate, 2000, 6, pp. 1218-1249; C. MONTELEONE, *Note a margine del novellato art. 171-bis della recente legge italiana sul diritto d'autore*, in *Ciberspazio e diritto*, 2000, 1, 4, pp. 499-507; P. ONORATO, *La tutela penale del diritto d'autore. Le fattispecie incriminatrici dopo la legge 248/2000*, in *Cassazione penale*, 2003, 2, pp. 675-689.

[18] Si consideri che, nella vigenza della legge citata, anche la mera acquisizione illecita di una sola canzone, mediante un programma di *file sharing*, poteva rendere l'utilizzatore soggetto alla pena *minima* di un anno di reclusione nonché di € 2.582,28, nonostante, in ipotesi, la stessa canzone potesse essere acquistata *on line* per soli 99 centesimi. È, dunque, evidente quanto la pena fosse sproporzionata e quanto fortemente il legislatore avesse tutelato il diritto d'autore. Come si vedrà appresso, tale fattispecie costituisce ancor oggi un illecito penale, per quanto punito con minore severità ma, comunque, in misura eccessiva. Del resto, nonostante sia notorio che le case discografiche e cinematografiche tentino di instillare nel grande pubblico la convinzione che effettuare il *download* non autorizzato di una canzone o di un

5. Dalla tutela della proprietà intellettuale al controllo globale

Le aziende che operano nel settore informatico e dell'*entertrainment* godono, com'è noto e come è stato sinora evidenziato, di una posizione di particolare favore nell'ambito di diversi ordinamenti giuridici. A mero titolo esemplificativo, basti pensare al citato DMCA statunitense, oppure alla legge italiana sul diritto d'autore. Tuttavia, come ha osservato Nicholas Negroponte nel 1995, "la legislazione sui diritti d'autore (*copyright*) è del tutto anacronistica. È un retaggio di Gutenberg ed è probabile che vada in frantumi ancor prima di essere corretta"[19]. Ciò nonostante, tale legislazione, sovente corretta in modo alquanto maldestro, è attualmente vigente, e, nei vari ordinamenti giuridici, solitamente riconosce e tutela con forza le pretese dei detentori dei diritti d'autore, anche qualora ciò comporti una ingiustificata compressione dei diritti dei legittimi utilizzatori.

Con precipuo riferimento alla normativa italiana, basti pensare all'art. 102 *quater*, commi 1 e 2, della l. aut.[20], ai sensi del quale "i titolari di diritti d'autore e di diritti connessi nonché del diritto di cui all'art. 102-bis, comma 3, possono apporre sulle opere o sui materiali protetti misure tecnologiche di protezione efficaci che comprendono tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti. Le misure tecnologiche di protezione sono considerate efficaci nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o del materiale protetto, ovvero sia limitato mediante un meccanismo di controllo delle copie che realizzi l'obiettivo di protezione".

Tale disposizione, dunque, concede una particolare forma di autotutela *ex ante* ai titolari di diritti d'autore, consentendogli l'utilizzo delle tecnologie c.d. di *digital rights management* (DRM) per impedire l'effettuazione di atti non autorizzati[21]. Inoltre, la rilevanza penale delle violazioni

---

lungometraggio costituisca un "furto" e che sia giusto comminare la sanzione della reclusione, accompagnata da una pesante pena pecuniaria nessun "furto" si realizza in tale ipotesi. Sul punto, si considerino gli effetti della condotta medesima. È fuor di dubbio che essa sia illecita. Tuttavia, quale perdita concreta si realizza nella sfera del titolare dei diritti d'autore? Il danno emergente è nullo, perché nessuna privazione dell'opera viene posta in essere, ma se ne effettua una semplice duplicazione. L'unica perdita potenziale può individuarsi nel lucro cessante, perché potrebbe ritenersi che l'utente, effettuando il *download*, non acquisti la canzone suddetta oppure non noleggi e/o acquisti una regolare copia del film, comportando un utile mancato nei confronti del soggetto sopra citato. A titolo esemplificativo si consideri, però, che attualmente una canzone, sotto forma di *file* musicale, può essere legalmente acquistata *on line* al prezzo, in media, di 99 centesimi. Ne consegue che il danno che un singolo *download* può comportare è davvero limitato. Si potrebbe sostenere che più *download* illeciti vengono effettuati, più "danni" devono essere sopportati dal titolare dei diritti d'autore. Ciò è vero, ma punire con eccessiva forza un singolo utente equivale ad introdurre surrettiziamente una nuova ipotesi di responsabilità oggettiva, per cui una singola persona che scarica un *file* illecitamente dovrebbe rispondere anche per tutti coloro che scaricano il medesimo *file*! L'applicazione di tale principio ad altri settori della società comporterebbe, ad esempio, che chi è condannato per un omicidio, dovrebbe scontare non solo la pena per il delitto commesso, ma anche quella che dovrebbero scontare i rei degli omicidi insoluti. Appare palese, dunque, la pretestuosità di simili motivazioni, così come appare evidente l'eccessiva severità del legislatore.

[19] N. NEGROPONTE, *Essere digitali*, tr. it., Sperling & Kupfer, Milano, 1999, p. 55. Oltretutto, come ha sottolineato efficacemente Carlo Gubitosa, "se il copyright fosse un diritto naturale in vigore dall'alba dei tempi oggi il pianeta sarebbe governato dagli eredi degli inventori della ruota, che grazie allo sfruttamento economico della loro fondamentale avrebbero potuto acquistare il controllo su tutte le altre invenzioni dell'uomo" (*Elogio della pirateria*, Altreconomia, Milano, 2005, p. 44).

[20] La norma citata è stata introdotta dal d.lgs. 9 aprile 2003, n. 68, che ha recepito la direttiva del Parlamento europeo e del Consiglio del 22 maggio 2001, n. 29, "relativa all'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione". Sul d.lgs. n. 68/03 cfr., fra gli altri, E. O. POLICELLA, *Le principali novità in materia di diritto d'autore introdotte dal D.Lgs n. 68/2003*, in *Diritto industriale*, 2003, 4, pp. 372-386; M. S. SPOLIDORO, *Una nuova riforma per il diritto d'autore nella società dell'informazione*, in *Il corriere giuridico*, 2003, 7, pp. 845-848.

[21] La realtà fattuale mostra come taluni sistemi di DRM possano essere palesemente illeciti ed addirittura dannosi, come nel celebre caso, avvenuto nel 2005, del *rootkit* Sony BMG, ossia di un programma (nella fattispecie, proprio un *root*

forse più comuni, come la condivisione via Internet, senza scopo di lucro, di opere protette dalla l. aut.[22], rafforza notevolmente la tutela *ex post*.

Dal versante opposto, però, il legittimo utilizzatore può dirsi tutt'altro che tutelato. Non si deve dimenticare, infatti, che l'art. 102 *quater* l. aut. non autorizza i titolari dei diritti d'autore a limitare le facoltà di godimento sorte in capo a ciascun legittimo utilizzatore. In linea di principio, dunque, gli atti autorizzati non potrebbero essere limitati mediante tecnologie di DRM. Eppure, la comune esperienza dimostra che tali misure limitano, in maniera spesso non giustificata, anche gli atti autorizzati. Così, taluni *compact disc* musicali non possono essere riprodotti sui lettori CD e/o DVD dei personal computer oppure su quelli meno recenti, perché le tecnologie di riproduzione ne impediscono la lettura oppure la rendono possibile, nel primo caso, solo previa installazione di uno specifico programma. I problemi che ne derivano sono di diverso ordine (compatibilità fra sistemi operativi diversi, utilizzo di risorse del computer, ecc.) ma l'illegittimità di dette limitazioni appare sostenibile, perché esse limitano anche gli atti autorizzati. Nessun *disclaimer* presente su tali prodotti, tra l'altro solitamente scritto in caratteri minuscoli, può legittimare un siffatto *modus operandi*, perché incide troppo profondamente sulla posizione del legittimo utilizzatore che si troverebbe in balia della forza contrattuale dei detentori dei diritti d'autore[23].

Cosa può fare, dunque, il legittimo utilizzatore dinanzi alla violazione dei suoi diritti? Il caso dei *modchip* chiarisce la strategia delle aziende del settore finalizzata a togliere l'unica arma in mano ai loro clienti per superare le limitazioni ingiustificate a loro imposte[24]. Inoltre, la strada giudiziaria appare, invero, impervia e difficilmente percorribile, per tempi e per costi, considerando i lunghi tempi della giustizia.

In altri termini, sembra che il legislatore sia stato sin troppo solerte nel garantire i detentori dei diritti d'autore senza però curarsi di tutelare anche i loro aventi causa[25]. Inoltre, tale quadro rischia di diventare ancor più problematico qualora si consideri che tale posizione di preminenza

---

kit) che si installava, all'insaputa dell'utente, quando questi inseriva nel lettore CD o DVD del proprio computer uno dei numerosi compact disc musicali prodotti e distribuiti dalle medesima società. Tale programma si nascondeva all'utente anche durante la sua esecuzione ed ha creato problemi a numerosi sistemi informatici (ad esempio, blocchi di sistema). Come ha affermato Corrado Giustozzi, "scaricare brani piratati di artisti Sony è addirittura più sicuro per l'utente che comprare i dischi originali. Non è questo un agghiacciante paradosso?" (*L'affare Sony/BMG: utenti colpiti da fuoco amico*, in *Interlex*, in http://www.interlex.it/copyright/corrado26.htm). Sui DRM cfr. anche l'ottimo dossier apparso sul n. 335/2005 di Interlex (http://www.interlex.it/numeri/051115.htm).

[22] L'art. 171 l. aut., da ultimo novellato dal d.l. 7/05, punisce con la pena della multa" chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, [...] mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa". Ai sensi del comma 2 del medesimo articolo, quanto meno, chi commette tale reato "è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato". La possibilità dell'oblazione non fa venir meno il carattere di illecito penale riconosciuto in tali ipotesi, in spregio alla concezione del diritto penale come *extrema ratio*.

[23] Oltretutto, neanche l'accettazione di un accordo di licenza "dà diritto al fornitore di fare ciò che vuole su un sistema altrui, e non consente neppure di derogare a principi del diritto assai più generali" (così C. GIUSTOZZI, *L'affare Sony/BMG: utenti colpiti da fuoco amico*, in *Interlex*, in http://www.interlex.it/copyright/corrado26.htm).

[24] In materia, Daniele Coliva ha giustamente osservato che "se il conflitto tra le ragioni (essenzialmente economiche) dell'industria culturale e i diritti degli utenti finali ha una precisa giustificazione, assume invece i caratteri dell'abuso l'introduzione di sistemi di protezione che limitano le possibilità di fruizione di contenuti creati dall'utente finale medesimo. Si potrà, infatti, discutere nel primo caso dell'impatto sull'efficienza complessiva del sistema, sulla tutela dell'autore, e così via, proprio perché nella fattispecie è logico che il titolare dei diritti cerchi, anche con la tecnologia, di spostare a suo favore il punto di equilibrio tra il suo interesse a massimizzare il ritorno economico di ogni atto di fruizione, mentre l'utente finale è tendenzialmente propenso a cogliere ogni possibile occasione di utilizzazione dell'opera dell'ingegno acquistata" (*Proprietà intellettuale, antitrust e diritti degli utenti*, in *Interlex*, http://www.interlex.it/forum10/relazioni/32coliva.htm).

[25] "Se infatti le misure tecnologiche di protezione sono costruite in maniera tale da incidere in misura fortemente restrittiva sulla possibilità di fruizione di opere o contenuti creati dall'utilizzatore finale, sulle quali quindi non esistono diritti di terzi, allora si determina una incomprensibile intrusione nella sfera anche patrimoniale altrui, e l'affermazione di una posizione dominante che trascende scopi e funzione della protezione dei diritti di proprietà intellettuale" (D. COLIVA, *op. cit.*).

potrebbe essere utilizzata anche per porre in essere palesi violazioni della *privacy* degli utenti, con dolo qualora i dati personali vengano volontariamente acquisiti oppure con colpa nel caso in cui l'illecito trattamento sia conseguenza non voluta, ancorché naturale e prevedibile, dell'implementazione di misure tecnologiche di protezione, in generale, e del TC, in particolare.

Del resto, l'informatizzazione della società, in sé considerata, ha sinora portato all'aumento del numero dei casi di lesione della *privacy*, come aveva previsto Negroponte nel 1995[26]; tale tendenza non potrà che consolidarsi di pari passo con la diffusione ed il perfezionamento delle tecnologie di tutela della proprietà intellettuale, perché sempre più invasive ed onnipresenti. Tuttavia, la tutela del diritto d'autore non può risolversi in una automatica lesione della altrui *privacy*, che, quanto meno nell'ordinamento giuridico italiano, è diritto di rango superiore rispetto al primo. Per di più, in tal caso si concretizza un controllo da parte di soggetti privati su altri soggetti privati in ragione del maggior potere economico dei primi sui secondi. Non si può neanche argomentare che comunque l'utente è libero di non acquistare l'*hardware* e il *software*: in primo luogo, la probabile integrazione del sistema in ogni componente informatico non lascerebbe comunque possibilità di scelta, in quanto numerosi prodotti elettronici consentono ormai il soddisfacimento di diversi bisogni primari della persona umana; in secondo luogo, essendo i sistemi informatici entrati nella quotidianità soprattutto dal punto di vista lavorativo, la scelta sarebbe costituita da due estremi: adeguarsi od emarginarsi.

Le aziende informatiche, quindi, potrebbero avere il controllo non solo sul *software* da esse creato, ma anche sulle creazioni dei propri clienti effettuate tramite lo stesso. L'anonimato sarebbe solo di facciata, visto che tramite controlli incrociati si potrebbe risalire ai singoli soggetti, grazie alla sempre crescente interconnessione dei computer ad Internet. Ogni computer potrebbe essere utilizzato solo se dotato di connessione alla Rete, per poter avere i certificati necessari per il funzionamento del *software*. Ogni computer collegato ad Internet è, però, identificato da un numero univoco (il c.d. indirizzo IP), dal quale si può risalire a chi si collega alla rete tramite i fornitori di accesso ad Internet (ISP, *Internet Service Provider*). Nel caso dei paesi in via di sviluppo, inoltre, si realizzerebbe un ulteriore ostacolo al progresso tecnologico, perché, insieme ai ben più gravi problemi sussistenti, si affiancherebbe la mancanza di infrastrutture adeguate e l'impossibilità di utilizzare un qualunque computer.

6. Trusted Computing *e monopoli*

La liceità dell'implementazione del TC non può essere sostenuta ritenendo che l'iniziativa economica nel relativo settore di incidenza non debba essere sottoposta a limiti imposti dall'esterno al libero mercato, il cui sviluppo dovrebbe essere lasciato alla libera azione delle aziende che operano nel settore. Tuttavia, esse da un lato non vogliono vincoli, ma dall'altro chiedono e spesso ottengono la tutela dei propri interessi in maniera alquanto discutibile, come dimostrano le normative in tema di tutela della proprietà intellettuale. In altri termini, si moltiplicano le pretese di creazione di nuove e moderne tipologie di patti leonini, nel cui ambito una parte avrebbe solo diritti e l'altra solo doveri. Si verificherebbe un impensabile squilibrio nel sinallagma negoziale, già oggi pericolosamente squilibrato in favore dei contraenti forti, come si è detto in precedenza in ordine al discusso tema del DRM. Oltretutto, oggi vi è un monopolio *de facto* da parte della Microsoft nel campo del *software*, soprattutto con riferimento al sistema operativo, dal momento che la famiglia dei prodotti "Windows" è installata sulla grandissima maggioranza dei computer di tutto il mondo e lo stesso dicasi per il software da ufficio (ossia "Office").

Invero, il libero mercato costituisce il paravento dietro il quale nascondersi per consentire ad aziende monopoliste di controllare il mercato le informazioni di pertinenza dei singoli individui. È la stessa situazione di monopolio *de facto* a livello di sistema operativo a porre l'esigenza di una regolamentazione che impedisca a taluni soggetti di controllarne altri. È notorio che, in una

[26] N. NEGROPONTE, *op. cit.*, p. 237.

situazione di monopolio quasi totale, la libertà di scelta sia fortemente limitata: anche se l'adeguamento allo standard produce innegabili vantaggi in termini di supporto tecnico, in quanto lo stesso può essere indirizzato alla risoluzione di problematiche uniformi perché presenti su sistemi rispondenti a specifiche comuni, bisogna considerare che difficilmente si avrà la possibilità materiale di discostarsi dallo standard, per problemi di varia natura. Da quanto detto risulta evidente, infatti, che un cartello effettuato dalle aziende del settore non solo eliminerà qualsiasi potenziale concorrente ma permetterà di ottenere un controllo senza precedenti su un mercato in fortissima espansione.

L'implementazione del TC potrebbe concretizzare un abuso di posizione dominante da parte delle aziende (e soprattutto di Microsoft), perché limiterebbe lo sviluppo tecnico in questo settore, risultando dunque in contrasto con l'art. 82, comma 2, lett. b), del Trattato istitutivo della CE ed eliminando di fatto la possibilità di sviluppare *software* liberamente. Ciò che si contesta non è la posizione dominante delle aziende in questione, che costituisce la conseguenza naturale e tangibile del forte successo delle varie attività commerciali, ma piuttosto un "comportamento aggressivo ed ingiustificato nei confronti dei concorrenti o dei consumatori"[27], la cui posizione (rispettivamente commerciale e contrattuale) risulta fortemente squilibrata in favore dell'impresa dominante. Il compito dello Stato è dunque quello di ristabilire il principio della "parità delle armi" e di tutelare chi si trova in una situazione di inferiorità, affinché l'iniziativa economica privata non si svolga "in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana" (art. 41, comma 2, Cost.).

Questo possibile sviluppo introduce seri problemi di conflitto tra normativa *antitrust* e diritto della proprietà intellettuale, fino ad oggi risolti in linea generale nel senso della prevalenza della tutela del secondo sulla prima. Se il *trend* industriale sarà in questa deprecabile direzione, allora sarà opportuno un doveroso ripensamento delle regole affinché la zona franca dalle disposizioni sulla concorrenza della quale ha fino ad oggi goduto il settore della proprietà intellettuale non degeneri in un monopolio che si pone in totale contraddizione con il concetto stesso di innovazione

7. Involuzione informatica e criticità giuridiche

Il quadro giuridico-fattuale sinora delineato evidenzia come la diffusione del TC nei settori diversi dall'informatica sarà idoneo a ledere la riservatezza degli utenti quando questi utilizzeranno oggetti quali telefoni cellulari o elettrodomestici di consumo. Ben più gravi e numerose saranno, però, le violazioni della *privacy* conseguenti all'implementazione del TC nei computer di nuova produzione, dovute alle motivazioni esposte nel corso della trattazione. Il fine, astrattamente lecito, della sicurezza potrebbe quindi essere visto come una maschera utilizzata allo scopo di celare il fine effettivo del controllo del mercato economico e dei dati personali dei singoli utenti. Stabilire cosa questi possano fare, determinare criteri che impongano scelte considerate migliori da altri, è un attentato alla libertà (non solo informatica) e permetterebbe inoltre l'acquisizione delle informazioni di proprietà degli utenti[28].

Come se tutto ciò non fosse sufficiente, la diffusione del TC potrebbe rallentare l'evoluzione dell'informatica se non, addirittura, spingere verso la sua involuzione. Del resto, già l'idea stessa di spogliare gli utilizzatori del controllo totale sulle macchine da loro legittimamente acquistate e/o utilizzate rende difficile ritenere che si sia fatto un passo avanti, oltre a porre evidenti questioni strettamente giuridiche in ordine alla validità ed all'efficacia del rapporto negoziale sottostante.

---

[27] M. C. VENUTI, *Monopoli (disciplina antimonopolistica)*, voce, in *Digesto delle discipline privatistiche, sezione commerciale*, Utet, Torino, 1994, X, p. 41.

[28] Ad esempio, le varie richieste di certificazione inviate ad un *server* remoto possono consentire di tenere traccia delle preferenze degli utenti ed anche qualora esse siano anonime costituirebbero un profitto illecito per le aziende che accederebbero a tali dati. Da un lato vi sarebbe la perdita del controllo delle proprie informazioni da parte degli utenti; dall'altro poche aziende otterrebbero gratuitamente le informazioni suddette.

Inoltre, oggi come alcuni decenni or sono, il progresso in questo settore non è lasciato unicamente nelle mani delle grandi aziende del settore, ma ad esso contribuiscono in maniera determinante i numerosi appassionati presenti in ogni parte del pianeta, che non sono più isolati grazie alla ormai capillare diffusione delle reti telematiche e, in particolare, di Internet. A titolo esemplificativo, si pensi al ben noto sistema operativo Linux, creato da Linus Torvalds, il cui sviluppo prosegue anche grazie ad una folta comunità di appassionati. Si pensi, ancora, a Napster, creato da uno studente statunitense, che ha reso semplice e veloce lo scambio di *file* musicali *on line*, oppure al *software* DeCCS, che ha permesso la decrittazione dei flussi video posti su DVD e crittati con il CCS (*Content Scrambling System*), consentendone la copia su *hard disk* oppure la creazione di copie di riserva[29].

Tuttavia, se il TC venisse integrato in tutti i nuovi computer nonché nei nuovi *software*, la creazione di nuovi programmi risulterebbe fortemente ostacolata e la libertà dell'utenza potrebbe ridursi ancora, perché anche il *software* libero dovrebbe essere certificato dal consorzio, con i relativi costi. Per ridurre le polemiche, il TCG potrebbe anche decidere di rilasciare gratuitamente le certificazioni, ma sicuramente prima o poi verrebbe richiesto il pagamento di una cifra (magari anche *una tantum*) per ottenerle. È evidente che un'eventualità siffatta significherebbe impedire lo sviluppo individuale del *software*, poiché il singolo programmatore, oltre alle proprie energie lavorative, dovrebbe investire anche del denaro per fornire un programma alla collettività oppure per il semplice piacere di programmare: chi mai lo farebbe? E, soprattutto, perchè il TCG dovrebbe avere simili poteri? C'è il rischio che si crei una nuova entità che tutela solo chi ha già raggiunto un posizione di potere, senza concedere spazi per l'affermazione di altri soggetti e senza garantire, ma anzi calpestando, la libertà dell'uomo nonché dell'iniziativa economica privata.

È palese che i fini che si dichiarano volersi perseguire mediante l'implementazione del TC possano ben raggiungersi in altri modi, mentre i fini occulti realmente perseguiti, che siano la repressione della pirateria o il consolidamento di situazioni di monopolio, non possono consentire una limitazione della libertà individuale. Basti pensare che ci sono scopi molto più nobili, come la repressione dei delitti, che tuttavia non possono essere perseguiti limitando o eliminando la libertà dei singoli in via generale. In caso contrario le potenzialità astrattamente negative dell'agire dell'uomo comporterebbero una restrizione della sua libertà operata da altri soggetti, di pari grado in via astratta, i quali avrebbero la forza concreta di tutelare i propri diritti (economici) mediante l'assoggettamento di altri e la limitazione dei diritti (umani) di quest'ultimi.

Ancor più grave appare, tuttavia, che il TC rappresenti la nuova frontiera del controllo globale, in quanto consente non solo di svolgere un mero controllo passivo sull'operato altrui, che si concretizza nell'acquisizione di dati personali, ma addirittura di decidere cosa gli altri possono fare. È, quindi, un controllo attivo, perché restringe la sfera cognitiva e di azione dell'uomo entro confini predeterminati aprioristicamente. Indipendentemente dalla chiara antigiuridicità ivi ravvisabile, è legittimo chiedersi come possa la società umana evolversi se gli individui non hanno la libertà di fare alcunché al di fuori degli ambiti determinati da una moderna oligarchia che ha trovato la propria legittimazione in sé stessa e nella sua forza economica.

Il diritto non può restare indifferente dinanzi a simili fattispecie, chiaramente idonee a violare diritti fondamentali della persona, come la libertà e la *privacy* (non solo informatica), la cui tutela ed il cui rispetto consente a ciascun individuo di autodeterminare la propria esistenza. Gli stati dovrebbero recepire non solo le istanze avanzate dai soggetti forti, ma anche quelle provenienti dai propri cittadini, anche se oggi le normative in materia sembrano tutelare con eccessiva veemenza i primi a scapito dei secondi. Ad ogni buon conto, nelle diverse fattispecie il cui *trait d'union* è costituito dalla presenza di tecnologie informatiche, la considerazione delle loro peculiarità ben può

[29] Tale programma è stato creato nel 1999 dall'allora quindicenne Jon Johansen, il quale aveva scritto questo *software* per poter visionare i film registrati su DVD (legittimamente acquistati) anche su computer dotati di sistema operativo "Linux", per il quale non esistevano appositi programmi per la visione dei DVD. Il giovane programmatore è stato però citato in un giudizio penale dal Governo norvegese dietro pressione delle aziende discografiche. Fortunatamente il giovane *hacker* è stato assolto da tutte le accuse.

giustificare una regolamentazione differenziata rispetto ai casi in cui esse non sono presenti; anzi, talvolta, un siffatto *modus operandi* si palesa necessario, purché il legislatore si ispiri al criterio della ragionevolezza e del rispetto della dignità e della libertà dell'uomo.