



L'informatica ci renderà liberi?

A cura di: Roberto Iannarelli*

Il tema della *security* in campo informatico sta prepotentemente conquistando gli onori della cronaca a causa della preoccupante crescita di crimini afferenti questa materia. La frequenza e la gravità delle violazioni vanno naturalmente di pari passo con lo sviluppo tecnologico delle nazioni e tanto più queste si affidano all'*Information Technology*, tanto più si espongono a rilevanti perdite economiche ma anche di sicurezza nazionale ovvero di dati strategicamente rilevanti a carattere militare, politico ed industriale.

Il reato informatico che viene tuttavia oggi percepito maggiormente dai cittadini che hanno accesso a queste tecnologie, è quello relativo alla violazione della *privacy* e pertanto si discuterà congiuntamente di *security* e *privacy*. In realtà, un confronto diretto è eterogeneo. Scardinando la prima si ha modo di accedere a varie tipologie di dati sensibili tra i quali anche quelli relativi alla *privacy* del singolo cittadino. Potremmo quindi affermare che il primo è il mezzo, il secondo un possibile effetto.

Va a questo punto ricordato che il cittadino può accedere alle tecnologie informatiche in maniera indiretta ovvero senza necessariamente l'atto volontario di sedersi davanti ad un computer e, magari, collegarsi ad Internet. Quando si prelevano i soldi da un Bancomat, si scatena una sequenza di attività informatiche di complessità inimmaginabile all'ignaro utente. L'operazione coinvolge gran parte delle tecnologie informatiche e telematiche disponibili sul mercato: trasmissione dati, database a distribuzione geografica, crittografia e molte, molte altre. Ognuna di queste tecnologie ha i suoi punti di vulnerabilità e si presta quindi ad essere violata.

La violazione della sicurezza di un sistema informatico è configurabile come un'attività avente carattere tecnico, più o meno rilevante a seconda del modello di sicurezza adottato dai creatori e dai responsabili del sistema stesso.

È quindi un'attività che viene associata alla figura dell'*hacker* personaggio che, nell'immaginario collettivo, specie grazie a certa filmografia, viene spesso associato all'imberbe ragazzino un po' stralunato ed un po' geniale che con tecniche misteriose



riesce a violare sistemi progettati da intere *equipés* di scienziati con una pletera di specializzazioni quali l'informatica, l'ingegneria di sistema, la matematica e, talvolta, la fisica.

Eppure nulla ferma il nostro *teenager* che con pochi efficaci colpi sulla tastiera, viola, in meno che non si dica, il Pentagono, la Casa Bianca oppure la National Bank. Certamente viene da domandarsi quanto sia realistico tutto ciò e se si siano realmente verificati casi simili.

Quando si vanno a discriminare le violazioni della sicurezza informatica, un primo dato emerge in modo preponderante: molti dei cosiddetti *hackers*, sarebbero meglio definibili come "spie in erba", a volte dotate di acume psicologico nonché di ottima vista ed udito piuttosto che di particolari doti informatiche.

Tutti i normali operatori di computer, compreso l'impiegato della banca o della posta, avevano la pessima abitudine di lasciare incustodite le proprie password, scrivendole su coloratissimi "post-it" appesi normalmente al monitor o alla tastiera. Non contenti, durante le operazioni di sportello, magari in base ad una malevola richiesta del *hacker-spia*, si allontanavano dalla loro postazione lasciando agio alla, magari non molto tecnica ma efficacissima, trafugazione del codice.

Altra situazione, ad un livello di complessità "superiore", è quella legata al fenomeno delle password non-casuali.

Tutti noi quando dobbiamo creare una password abbiamo la tendenza, per pigrizia e per paura di dimenticarla, a comporre un'associazione facilmente memorizzabile di termini legati alla nostra vita. Le persone non immaginano neppure la quantità di password violate semplicemente ricavandole dai dati anagrafici del malcapitato.

Altra modalità, consiste nel far girare appositi programmi che provano a ricomporre casualmente la password. La maggior parte dei software di *password-cracking* non contengono, però, alcuna intelligenza elaborativa ma si limitano all'uso della "forza bruta" computazionale delle macchine che accostano, permutandole, tutte le parole contenute in un vocabolario redatto tenendo conto delle reali o presunte maggiori frequenze utilizzate dagli utenti nella scelta delle password.

Certo i tecnici dell'informatica e i responsabili dei sistemi, non sono stati certo a guardare e sono state elaborate un certo numero di strategie per porre rimedio a questa prima serie di inconvenienti.



Una volta compreso come gli operatori non possedessero una cultura della “sicurezza informatica”, i datori di lavoro, privati e pubblici, hanno promosso corsi di formazione, hanno sensibilizzato il personale in ogni modo ed hanno infine previsto sanzioni, anche pesanti, a chi non si attiene alle regole aziendali. Una delle prime misure fu quelle di impedire ai sistemi di accettare password “banali”, obbligando all’uso di chiavi non brevi, formate da caratteri maiuscoli e minuscoli nonché numeri.

L’uso di password così complesse comportava tuttavia una maggior tendenza degli utenti ad appuntarle ovunque.

Per eliminare alla radice il problema si sono introdotte delle interfacce di autenticazione che fossero meno “umane” e quindi meno passibili di violazione.

Vi è stata una prima ed una seconda generazione di carte magnetiche, senza e con microchip, da inserire in un apposito lettore. Sono oggi commercialmente accessibili, le prime generazioni di interfacce “biometriche” che legano l’autenticazione a caratteristiche fisiche imprescindibilmente legate all’individuo come l’impronta digitale o quella della retina.

A favorire il criterio ingegneristico del calcolo *ad abundantiam*, ci vengono fortunatamente incontro i sempre più ridotti costi dell’elettronica peraltro associati a sempre più accurate prestazioni delle interfacce di sicurezza il che permette di non lesinare sui sistemi di sicurezza *hardware*.

Vanno poi messi in conto tutti gli errori ed omissioni di cui sono responsabili gli amministratori di sistema nel configurare le proprie reti. In particolare è necessario prestare maggiore attenzione nel considerare il corretto “raggio” della rete cui la macchina è collegata. La maggior interconnessione delle reti attuali e ancor più di quelle future, obbliga a riflettere accuratamente su quali nodi potrà raggiungere l’utente con il suo profilo di autorizzazioni e configurare la sicurezza d’accesso in base al dato più delicato presente sulla rete potenzialmente accessibile.

Con la sola eliminazione di queste forme semplici ed “improprie” di violazione della sicurezza, si ottiene una rilevante diminuzione del fenomeno. A questo punto rimangono da esaminare quei casi che, effettivamente, destano maggiore interesse e preoccupazione.

Un fenomeno sicuramente più sofisticato, è quello delle così dette “*backdoors*”.

Cosa sono queste “porte posteriori di accesso” è presto detto. Sono parti di programma, non documentate, inserite dai programmatori nel software commerciale di comune acquisto sul



mercato. Il fenomeno è particolarmente preoccupante quando il software interessato è il sistema operativo ma oggi sono molto devastanti anche gli inserimenti all'interno dei *browser* internet e sui *client* di posta elettronica.

Le motivazioni che inducono i programmatori ad inserire questo codice "maligno" di cui solo loro conoscono le modalità d'accesso e le funzionalità, vanno dal mero narcisismo, dall'ossessione del potere e del controllo, fino a vere e proprie forme, anche preventivamente escogitate, di rivalsa sul proprio datore di lavoro in caso di licenziamento o di semplici ostilità quali mancate promozioni od altre presunte ingiustizie. Anche la semplice infedeltà, legata magari a fini di lucro, può essere una possibile motivazione.

Tramite queste porzioni di codice, il programmatore ha la possibilità di realizzare qualsiasi tipo di intrusione e di danno anche se deve imporsi dei limiti tecnici specie sulla lunghezza del codice aggiunto per evitare di essere scoperto dai sistemi automatici di rilevamento della casa produttrice.

Talmente grande è la pericolosità del fenomeno, che le *software house* adottano varie strategie per combatterlo.

Bisogna preliminarmente considerare che quando si parla di un moderno, complesso sistema operativo dotato di metafora di interfaccia di tipo grafico, si parla di un oggetto con svariati milioni di righe di codice.

Questo rende l'idea di quanto sia complesso rilevare la presenza di qualche centinaio di righe al di fuori di quelle richieste dai progettisti del sistema.

Assieme a software "di controllo automatico del software", vengono adottate altre strategie come quella di compartimentare i vari sotto-assiemi del progetto in tante *black boxes* di cui i programmatori conoscono solo *input* forniti ed *output* richiesti ma non conoscono, perlomeno nei dettagli, gli altri sotto processi del sistema. Questo indubbiamente rende più difficoltoso, ma non certo impossibile, l'inserimento di frammenti di codice estraneo.

In realtà quando sopra si parlava di case produttrici, si diceva un'inesattezza in quanto, in questa "fase storica" dell'informatica gestionale, vi è una sola realtà colpita in maniera preponderante: Microsoft.

Questo accanimento può essere dovuto a vari motivi di cui alcuni, forse, sopravvalutati quali il sabotaggio industriale tramite le famose *backdoors* vendute da personale infedele alla concorrenza, oppure a lotte anti-capitaliste o anti-americane anche a sfondo destabilizzante o terroristico.



Molto più semplicemente, la massiccia diffusione di attacchi al software Microsoft è legata alla sua distribuzione ubiquitaria sul pianeta nonché ad una ingegnerizzazione che, per certi versi ha lasciato un po' a desiderare anche sotto l'aspetto della sicurezza sia per ragioni commerciali legate talvolta ad una eccessiva urgenza di apparire sul mercato col nuovo prodotto, sia per una oggettiva innovatività dei prodotti legata indissolubilmente ad un aumento esponenziale della loro complessità e quindi alla progressiva difficoltà di effettuare un completo ed accurato collaudo complessivo.

Nei sistemi complessi è impossibile testare ogni possibilità teorica di malfunzionamento in quanto è matematicamente dimostrabile come ciò richiederebbe una tempistica assolutamente incompatibile col mercato e questo in termini di vari ordini di grandezza.

Depurando il numero totale delle violazioni della sicurezza informatica anche del fenomeno delle backdoors, il numero dei casi superstiti si fa sempre più piccolo e sempre più interessante.

Solo ora è lecito ragionare su un certo numero di "ragazzi prodigio" che sembrano effettivamente rispondere agli stereotipi cui siamo abituati. In primo luogo non si tratta di adolescenti ma di ragazzi decisamente più grandi, a volte con percorsi accademici variamente interrotti alle spalle. Molti, pur essendo effettivamente degli *outsider* dell'informatica tanto che, dopo scoperti, vengono assunti da importanti organizzazioni private o governative, hanno creato la loro fama anche grazie a "furti" di informazioni nei modi classici discussi precedentemente.

La loro abilità tecnica consiste principalmente nello scovare i "buchi" nella sicurezza delle porte di accesso del computer quando questo si affaccia su Internet. In altre parole nello scovare gli errori umani di cui sono disseminati i software che, come già detto, nella loro complessità, non possono essere testati completamente dal produttore.

Altra fonte di errori umani, piuttosto facile da scoprire, sono i già accennati errori di configurazione dei sistemi da parte degli amministratori che lasciano aperti veri e propri "portoni" d'ingresso.

Il profilo tipico del *hacker* risponde ad una mentalità abbastanza tipica: grande abilità, pazienza, aspetti maniacali del carattere o altre devianze psicologiche e, a volte, convinzioni socio-politiche antisistema. Con appositi software spesso scritti da loro stessi e molta fortuna, riescono a "sfondare" e a costruirsi una fama. Il fatto che alcuni fra loro provengono da



solenni insuccessi nelle facoltà informatiche, la dice lunga tra le differenti qualità richieste nei due campi.

Il mondo di Internet è poi popolato da una infinità di sciacalli ovvero di programmatori non particolarmente abili ma che, una volta diffusasi su Internet l'idea originale scovata dagli *outsider*, la studiano e la utilizzano per creare una serie infinita di cloni varianti.

L'utente di Internet certo non si consola sapendo che il proprio computer è fuori uso grazie all'invenzione di un *outsider* piuttosto che di un *free rider* informatico; anzi la quantità di danni provocata da quest'ultimo è percentualmente assai più rilevante.

Non si può, per ultimo, non accennare ai virus come strumenti di violazione della *privacy*. Tecnicamente non si dovrebbe parlare di "virus". I virus informatici sono programmi che, con varie tecniche, entrano nel nostro sistema, si staccano dal software "portatore sano" ed inconsapevole e si "riproducono" nel senso che fanno copie di sé stessi sulla stessa macchina o su altre macchine collegate in rete. Lo scopo classico di un virus era e resta, quello di provocare dei danni al computer mediante la corruzione dei dati e dei programmi contenuti nei supporti fissi di memorizzazione. I virus, in altre parole, non si proponevano inizialmente di violare la *security*.

Ora le cose sono cambiate. I virus viaggiano prevalentemente su Internet: è più sicuro, più rapido e, soprattutto, dà accesso a una sterminata rete di computer. Sono stati quindi battezzati con nomi più confacenti ai loro scopi: *worms*, *trojan*, *spyware*, *malware*.

Particolarmente interessanti nell'ambito della *security*, sono quei virus, *latu sensu*, che non provocano danni ma "spiano" le azioni dell'utente sulla macchina collegata in rete. Questi *spyware* sono in grado di catturare la digitazione di password e di inviarle, via Internet, agli estensori del programma. L'uso di Internet, sempre più popolare e quindi sempre meno frequentato da "esperti", alimenta fruttuosamente questa attività di "spionaggio". Scrivere *spyware*, è relativamente più facile rispetto alle competenze necessarie per violare la *security* alla vecchia maniera quando erano necessari i famosi e rari *outsider* di cui sopra. Pertanto, è cresciuto il numero di programmatori in grado di realizzarli e la loro devastante presenza su Internet nonostante le contromisure consistenti nei software antivirus.

Se togliendo dal conto anche i nostri (pochi) ragazzi prodigio, non abbiamo ancora esaminato tutti i casi è perché esiste un numero di situazioni che ancora non si adattano ai profili "criminali" fin qua delineati.



Se la diffusione dei sistemi operativi Microsoft con i loro problemi e le loro vulnerabilità, è predominante, è pur vero che le banche dati più importanti risiedono ancora oggi su sistemi della famiglia Unix e discendenti o su sistemi ancor meno diffusi e conosciuti se non, addirittura, su sistemi proprietari.

Tutti questi sistemi operativi sono più robusti, più complessi e anche poco standardizzati, al contrario di Windows. Per questi sistemi, ad esempio, non si conosce praticamente l'esistenza di virus informatici.

Ancora, ci sono sistemi che, per la loro configurazione e per la preparazione degli operatori abilitati ad accedervi, non sono oggettivamente sensibili ai fenomeni sopra descritti in termini di smarrimento di password o di incuranza.

Eppure tutti questi sistemi sono stati almeno una volta violati magari laddove uno non se lo aspetterebbe ovvero decrittando codici cifrati con algoritmi che sono stati testati in ambiti militari e accademici assolutamente affidabili.

È ragionevole pensare che ci siano dei singoli individui così geniali e dotati di risorse computazionali - parliamo di super computer da milioni di dollari, sebbene oggi esiste qualche alternativa meno costosa - da arrivare a risultati di simile rilevanza?

Possibile, forse, ma molto improbabile. Si aprono, invece, altri scenari: dai servizi segreti, allo spionaggio industriale. Dalle organizzazioni terroristiche con alle spalle interi stati o comunque risorse economiche importanti. Possiamo, in taluni casi, pensare anche a ricatti, estorsioni (ma anche collusioni) nei confronti di chi detiene le chiavi dei sistemi da parte della criminalità organizzata.

Tornando alla distinzione iniziale, fin qua è stata descritta la violazione della *security*, ovvero la violazione del blocco di accesso ad un sistema da parte di un soggetto non abilitato a tale operazione.

Rimane però da esaminare il caso di coloro che, *strictu sensu*, il sistema non lo violano in quanto autorizzati ad accedervi ma che abusano di tale autorizzazione per usi impropri. Anche in questo caso non è detto che l'abuso commesso sia quello della violazione della *privacy*. Colui che abusa potrebbe, per esempio, carpire e diffondere un segreto industriale o d'ufficio non specificatamente legato ai dati personali di una o più persone.

Anche se le cronache più recenti ci hanno bombardato di abusi relativi alla privacy, bisogna sempre tener presente che dietro alla volontà di acquisire un qualsivoglia dato personale, a



meno di comportamenti infantili di semplice curiosità – che pur sempre esistono in ciascuno di noi –, esiste e deve essere individuato, tramite le opportune indagini investigative, l'esatto movente.

Tornando però all'aspetto più prettamente tecnico, vanno esaminate le peculiarità di questo tipo di azione indebita.

Nel caso degli abusi, infatti, è necessario non tanto mettere in atto sistemi di prevenzione dell'intrusione, quanto realizzare una qualche forma di registrazione degli accessi e delle attività svolte durante la permanenza nel sistema.

Ancor prima di far questo, deve essere risolto il primo fondamentale aspetto: assicurarsi che chi è penetrato nel sistema sia effettivamente colui che dichiara di essere.

Nel caso di una semplice password, questo requisito non è ovviamente garantito. Otteniamo un notevole incremento di sicurezza se associamo l'uso della password ad una *card* a microprocessore o, ancora meglio, con un interfaccia biometrica.

Una volta che ci siamo assicurati della reale identità di chi si è introdotto nel sistema, resta da effettuare il *tracking*, il *logging* delle attività svolte. Questa attività, per dirla in breve, ha dei costi legati in maniera non lineare alla quantità di utenti che accedono al sistema e alla loro attività media. Se il numero di accessi è elevato così come l'attività media nel sistema, la memorizzazione e la conservazione dei dati accumulati può in breve tempo assumere dimensioni imponenti tali da rendere inaccessibile il sistema.

Ancora più costoso e disarmante della conservazione delle tracce, è il loro esame al fine di verificare abusi. Se è vero che tale attività può essere, almeno in parte, automatizzata tramite sistemi (informatici) di controllo, questo implica un ulteriore aumento dei costi senza dimenticare che il problema dell'abuso (o violazione) si potrebbe applicare anche ai sistemi di controllo medesimi.

Sembrerebbe, pertanto, un problema circolare, senza soluzione. In realtà non è così.

Sicuramente si può e si deve effettuare, in base alla delicatezza delle informazioni, un accurato bilanciamento costi/benefici ovvero tener conto della reale qualità e quantità di controlli da effettuare ovvero il livello di dettaglio, in quanto questo è un parametro fondamentale per calcolare l'impatto economico dell'archiviazione.

Si valuterà, inoltre, la quantità di persone che è effettivamente necessario autorizzare specialmente ai livelli con i maggiori privilegi.



Mettendo insieme tutta una varietà di strategie, sebbene ciascuna di esse in linea teorica non sia assolutamente inviolabile e, per motivi di costo, neppure attuata al massimo delle sue potenzialità di protezione, si ottiene, nel complesso, un sistema che presenterà altrettanto forti problemi di “costi” anche per il malintenzionato. Costi che non saranno necessariamente di tipo economico ma anche, per esempio, di natura temporale.

L’abuso dei dati da parte del personale autorizzato ad accedervi presenta un altro, consistente, inconveniente. Il problema è quello di limitare, da una parte, l’accesso ai dati al minor numero di persone, ma, nel contempo, permettere lo svolgimento regolare delle attività istituzionalmente previste senza perdite di efficienza dovute alla natura eccessivamente restrittiva delle regole. Anche per questa difficoltà per risolvere la quale l’informatica può dare un aiuto ma non una soluzione esaustiva, andranno trovati adeguati punti di equilibrio in termini di efficaci compromessi.

Rimane da esaminare un’ultima, ancora più subdola, forma di violazione della privacy.

In questo caso, non si configurano reati relativi alla violazione della sicurezza informatica. Anzi, alla luce dell’attuale legislazione, in buona parte dei casi, non sono neppure configurabili reati di violazione della privacy.

Si vuole alludere alle ormai molteplici occasioni della vita quotidiana di noi cittadini, durante le quali, con un consapevolezza spesso assai bassa, autorizziamo qualcuno ad utilizzare i nostri dati personali.

Certamente questa forma di appropriazione non ci colpisce tutti in ugual misura, ma, in realtà, è solo una questione di tempo e di ricambio generazionale.

L’abitudine a fornire i propri dati è legata ad una molteplicità di fattori: la comodità legata alla tecnologia, la possibilità di accedere a sempre più servizi esclusivamente tramite queste tecnologie nonché una miriade di forme di *battage* pubblicitario (premi, punti, sorteggi ecc.).

Anche le istituzioni governative favoriscono l’uso di tecnologie informatiche e telematiche: le *cards* multiservizio (carte d’identità a microchip) sono state un primo tentativo delle amministrazioni di attenuare l’utilizzo dei supporti cartacei.

Ma sono di questi giorni le iniziative di legge che permettono, al fine di contrastare l’evasione fiscale, la possibilità di controlli fittissimi ed incrociati su tutti i circuiti telematici che imprenditori, ma anche singoli cittadini, incrociano quotidianamente nella loro vita.



Sono però ancora i frequentatori di Internet, i soggetti migliori ai quali carpire informazioni personali. Vi è ormai una moltitudine di siti che richiedono la compilazione di un *form*, per l'accesso a qualche servizio, per l'iscrizione a qualsiasi attività *on line* o anche, semplicemente, per l'accesso alle pagine più interne del sito.

Alcune di queste "interviste" *on line*, rispondono ai criteri della legge italiana, riportando la fraseologia di rito (da sottoscrivere peraltro tramite la semplice spunta di alcune caselle), per l'autorizzazione al trattamento dei dati.

Solo alcuni siti, per lo più istituzionali, richiedono la stampa, la firma e l'invio del documento cartaceo, molti altri non riportano neppure le indicazioni di legge. Per non parlare poi dei siti stranieri.

Se gli utenti leggessero attentamente, ma non lo fa quasi nessuno, si accorgerebbero cosa comporta applicare le spunte che, di solito, sono almeno due.

Con la prima, si autorizza l'uso dei dati per i soli fini "istituzionali del sito. Se ci stiamo, ad esempio, registrando ad un sito di *e-commerce*, è evidente che fornire il proprio indirizzo sarà necessario per la spedizione delle merci o dei servizi da noi acquistati.

La seconda autorizzazione che siamo chiamati a dare, riguarda invece la possibilità dei proprietari del sito di utilizzare per fini non "istituzionali" quei dati nonché la possibilità di cederli a terzi. Spesso la richiesta è accompagnata da giustificazioni inerenti alla possibilità d'inviare materiale informativo, pubblicitario oppure di segnalarci le novità o appuntamenti di rilievo.

Questo sarà probabilmente uno degli utilizzi dei nostri dati, ma la realtà è anche un'altra.

Qualcuno sarà forse rimasto piacevolmente meravigliato nel ricevere nella propria buca delle lettere (cartacee o virtuali), pubblicità che sembrano fatte su misura per lui, che lo informano esattamente su un certo tipo di prodotti o di tecnologie che lo interessano. Altri, invece, avranno ricevuto inviti a mostre, concerti, convegni culturali o politici a cui si accorgono di partecipare volentieri.

Ma il mittente è davvero così fortunato nell'indovinare i gusti del destinatario? Non proprio.

Esiste un mercato ormai florido ed esteso di "fornitori di elenchi". Questi elenchi non contengono solo i recapiti delle persone, ma sono ricchissimi d'informazioni d'ogni genere.

Se potessimo visionare alcuni dei migliori tra questi database, penseremmo di essere spiati notte e giorno per la quantità di notizie personali affiancate al nostro nominativo. E, in effetti, siamo spiati. Ma non da agenti in carne ed ossa. Siamo spiati dal bancomat, dalla carta di



credito, dalla carta multiservizi del Comune, dalle tante carte dei supermercati, delle catene dei distributori di benzina e, se ciascuno guarda nel proprio portafoglio, può sicuramente aggiungere qualche ulteriore indicazione. Certo, non tutte le carte rendono disponibili i dati in ugual misura, ma se abbiamo firmato la “liberatoria”, possono, in linea di principio, farlo legalmente.

Le carte punti degli esercizi commerciali ed in particolare, delle grandi catene di distribuzione, sono tra le più temibili in assoluto. Quando le abbiamo “gratuitamente” ottenute, abbiamo fornito una serie completa di dati anagrafici. Poi abbiamo incominciato a fare la spesa. Ogni volta che passiamo alla cassa e consegniamo la tessera per il caricamento degli ambiti punti, veniamo radiografati dalla testa ai piedi.

Quantità e qualità di tutte le merci acquistate, frequenza degli acquisti, metodi di pagamento sono dati di una ricchezza inusitata per un ricercatore statistico, per lo psicologo ed il sociologo che saranno in grado di disegnare profili di una accuratezza tale da lasciarci a bocca aperta. Probabilmente se la volta successiva ci consegnassero all’entrata un carrello con la spesa già fatta, sentiremmo la necessità di togliere o aggiungere ben pochi articoli.

Lo stesso dicasi di molti siti Internet. Per ogni sessione di collegamento ad un sito, c’è la possibilità di registrare a quali pagine si è acceduto e quali *links* o percorsi, si sono seguiti. Se la sessione è registrata ovvero se l’utente si è dovuto autenticare, anche in questo caso, gli analisti saranno in grado di costruire un profilo delle persone, anche se sicuramente meno accurato di quello del supermercato. Questa tecnica è molto usata dai *bookstores*.

Si potrebbero fare molti altri esempi, ma forse è più utile porsi una domanda basilare: tutto questo è necessariamente un male? Se tutta quest’attività, ha uno scopo preminentemente commerciale, e tendenzialmente tesa a soddisfare in maniera precisa e puntuale i miei bisogni, magari fornendomi un’informazione preziosa su una merce o su un avvenimento che potrei, con dispiacere perdere, non dovrei essere tutto sommato contento del servizio offertomi?

Una prima obiezione potrebbe riferirsi al fatto che qualcuno sta lucrando dalla vendita dei miei dati personali. Si potrebbe facilmente replicare all’osservazione rispondendo che, *in primis*, mi è stata richiesta un’autorizzazione ed io l’ho, in piena libertà, sottoscritta. *In secundis*, il servizio che mi è fornito a fronte della mia autorizzazione, ha un costo che non mi viene addebitato direttamente ma tramite la cessione dei miei dati i quali, *uti singuli*, hanno, tutto sommato, un valore commerciale assai basso.



Ma la contro-obiezione è più forte. Se la libertà del singolo è un valore *sub specie aeternitatis*, indipendente dai mezzi e dalle tecnologie, allora deve essere assicurato l'accesso ai servizi anche se la persona non accetta la cessione dei propri dati. Se questo non avviene, come in realtà in molti casi succede, siamo dinanzi ad un'imposizione quasi ricattatoria: o rinunci a questo servizio oppure cedi i tuoi dati. Già in parte oggi, ma sempre più in futuro, la possibilità di rifiutare i servizi legati alle tecnologie, non necessariamente tramite Internet, sarà sempre più difficile e comunque capace di creare cittadini con differenti possibilità di fruire dei servizi stessi.

Oltretutto non si può far finta di ignorare che l'adesione alla cessione dei dati, è, in molti casi, legata all'ignoranza o alla noncuranza del singolo.

Per attenuare questo fenomeno, bisogna intervenire certamente a livello informativo verso i cittadini, ma bisogna anche creare regole valide ed assicurarsi che vengano rispettate. È questo uno dei compiti per i quali sono state create in molti paesi, le autorità garanti della privacy.

Un altro aspetto preoccupante è l'impossibilità di sapere chi acquisterà i miei dati personali ovvero la perdita di qualsiasi forma di controllo su di essi. Il cittadino può, solo e sempre che - come già detto - ne abbia coscienza, sapere di avere autorizzato una determinata Società. Ma dei successivi passaggi, di chi comprerà e rivenderà un certo numero di volte i suoi dati, non riuscirà mai più a tenerne traccia.

Infine, bisogna pur considerare un uso diverso da quello commerciale, già preoccupante per i vari aspetti testé illustrati.

La tecnologia offre possibilità fino ad oggi inimmaginabili: incrociare le varie banche dati, sommare varie porzioni dei nostri profili psicologici fino ad ottenere una qualità incredibilmente alta da una moltitudine di dati dispersi.

È lecito quindi domandarsi se non esiste la reale possibilità di utilizzare tali informazioni a fini, per esempio, politici, di controllo sociale, ricattatorio.

E se tali considerazioni sono, di massima, valide per tutte le Nazioni, si rivelano particolarmente pregnanti nei paesi in fase di sviluppo, di transizione alla democrazia o di consolidamento democratico.

Questi processi politici richiedono tempi assai più lunghi rispetto allo sviluppo tecnologico - in particolar quello informatico - per cui queste stesse tecnologie, se male utilizzate, potrebbero trasformarsi da potenziali strumenti democratici in ostacoli alla democrazia stessa.



Per non considerare poi, gli usi sovra-nazionali, quelli legati al terrorismo o la possibilità che la criminalità organizzata tragga un qualche vantaggio dal possesso di queste banche dati.

Una sola cosa è certa: le tecnologie informatiche e telematiche sono troppo utili per rinunciarvi e occuperanno fasce sempre più consistenti del nostro spazio sia di quello reale, geografico, mediante la loro diffusione planetaria, sia di quello virtuale attraverso reti sempre più profondamente interconnesse.

È necessario, anzi, vitale che tutti i paesi si dotino di una legislazione efficace per uno sviluppo massivo ma compatibile di tali tecnologie nel rispetto delle libertà individuali.

E soprattutto che lo facciano in tempi non politici ma...telematici.

*Capo Centro Elaborazione Dati, Sistemista, Analista, Programmatore, Network Administrator, Database Administrator, responsabile sicurezza informatica, responsabile acquisti nell'ambito della P.A.