

Breve analisi dei rapporti tra sicurezza dei dati e legge 675/96

1. Sicurezza informatica e diritto

Una premessa assolutamente indispensabile, anche per chiarire quanto scriverò in seguito; questo breve saggio è la versione ridotta ed adattata dei primi due capitoli del “Manuale di Infosecurity Management”^[1], recente fatica del sottoscritto del M.o.S. Dario Forte.

Quindi, prima di tutto un ringraziamento al co – autore ed all’editore per il permesso di utilizzare il materiale; chi volesse approfondire alcuni aspetti è pregato di fare riferimento alla versione integrale del testo richiamato.

La regola – come tutti i giuristi ben sanno - per la commissione dei reati è quella che essi devono essere compiuti con il c.d. “dolo”, in altre parole ancora con la volontà di compiere tale reato; solamente alcune sono le eccezioni, tra le quali – purtroppo – proprio quelle legate alla Legge 675/96 e derivate.

Inoltre ricordiamo che molti reati sono perseguibili soltanto a querela; spesso anche il giurista non pone attenzione alla circostanza che si compiono atti – magari ogni giorno - che possono costituire degli illeciti, di tipo civile, amministrativo o – in alcuni casi – penale. Non è detto che si debba sempre incorrere nelle sanzioni di legge.

Questo sia perché anche il diritto (come anche in questo caso ben sanno i giuristi) deve essere sempre applicato da uomini, che hanno una loro capacità di discernimento e di valutazione, sia perché – oggettivamente – ritenere che qualunque sistema giuridico possa essere in grado di sancire tutte le attività illecite in ogni modo compiute è pura utopia sia perché, da ultimo, esistono sicuramente dei validi professionisti in grado di “salvare” alcune situazioni oggettivamente complicate.

Ciò non vuol certo significare un invito all’illegalità, ma solamente un’iniezione di tranquillità.

Forse non è inutile ricordare a noi stessi che – con tutta probabilità - non esiste situazione nella quale un avvocato, un magistrato, un pubblico ministero, non possa scorgere dei potenziali o possibili illeciti, così come non è assolutamente detto che – ammesso che tali illeciti siano configurabili – si arrivi ad una condanna.

Quest’argomento assume particolare rilevanza laddove si voglia parlare della c.d.”difesa attiva”, in altre parole della possibilità di compiere azioni che, a volte, possono essere illecite, per difendere la propria posizione.

"Solo un esempio: si sostiene, in genere, che dei sistemi d’armi automatiche collegate a dei sensori possono essere utilizzati a difesa d’apparati militari, ma che l’utilizzazione degli stessi per difendere la proprietà privata costituisce – di norma – un eccesso non consentito. Al contrario, sono leciti i c.d.

“offendicola”, in altre parole le punte dei cancelli ovvero i pezzi di vetro su di un muro, al fine di rendere più difficile al delinquente penetrare nella nostra proprietà. Nella materia trattata questi concetti diventano la liceità di utilizzare un firewall, la liceità di cancellare un messaggio di posta contenente un virus, la liceità di controllare ed eventualmente fermare un attacco di tipo DoS, ma in linea di massima, per restare in tema, non comprendono la liceità di controbattere l’attacco “attaccando” a nostra volta. In altre parole, per usare un concetto che probabilmente molto conoscono, di definire l’ambito della “legittima difesa” in questo campo.” [2]

2. Una breve disamina del problema

Cercherò di indicare alcuni elementi che mi hanno spinto ad accettare l’invito del Curatore.

Innanzitutto voglio chiarire che ho cercato di usare un linguaggio scarno, cercando il più possibile di non scadere nel “legalese” puro, perché ritengo che farsi capire dovrebbe essere l’obiettivo principale di chiunque si accinga a scrivere un libro, ed in particolar modo tale esigenza debba essere tenuta presente laddove si scriva ad un pubblico che, probabilmente, conosce ben poco della materia da un punto di vista “tecnico – informatico”.

Ritengo poi che cercare di pensare e scrivere i concetti con i quali i giuristi sono abituati ad avere a che fare secondo una diversa prospettiva non possa che far bene all’analisi dei problemi, in special modo in questa materia, che si presenta assolutamente “trasversale”.

Se si vuole avere una chiave di lettura di questo breve saggio, in linea di massima, sia nella materia civile sia nella materia penale, ho cercato di pormi su un piano quanto più possibile asettico, dimenticando l’attività d’avvocato e cercando di ragionare in maniera astratta, magari secondo un “gioco delle parti” che spero possa aver dato i suoi frutti. Pertanto in molti casi non mi sono lasciato invischiare dalle sottigliezze tipiche del diritto, ma ho cercato di inquadrare i fenomeni tecnico – informatici in una prospettiva quanto più ampia possibile, anche perché il compito di qualsiasi professionista serio dovrebbe essere quello di conoscere i problemi, affrontarli e quindi cercare di risolverli, non certamente quello di cercare la soluzione più tecnicamente elegante da un punto di vista giuridico.

Chiarisco ancora che la materia (che – come già scritto - ho affrontato di recente ed ampiamente insieme al caro amico Dario Forte[3]) – comprendendo comportamenti, apparecchiature, persone, hardware, software e chi più ne ha più ne metta – appare per propria natura assolutamente non confinabile entro limiti specifici di una sola branca del diritto, ed è trasversale alla classica tripartizione tra diritto civile, penale ed amministrativo, andando a toccare (nella parte in cui si tratta dell’incident handling e della ricerca delle prove) anche la problematica del giudizio che si basi su quelle che in gergo si chiamano “evidenze informatiche”.

3. Cosa vuol dire “sicurezza informatica”

“La sicurezza informatica (o information security) è un concetto che esiste da diversi anni, ma solo

recentemente sta investendo trasversalmente tutto il mondo della “new” economy. L'esplosione di Internet e delle grandi reti aziendali ha infatti costretto imprese e privati non solo a riflettere sulla necessità di proteggere le informazioni, e i dati che circolano quotidianamente da un computer all'altro, ma a dover fronteggiare attacchi sporadici o organizzati che, in molti casi, creano danni ingenti sia di immagine sia economici. Lo scenario che si presenta oggi a chi opera nel mondo dell'informatica, sia da "addetto ai lavori", sia da "utente", è sempre più complesso: la microinformatica ha favorito la diffusione dell'utilizzo di piccoli elaboratori a livelli che fino a qualche anno fa erano impensabili, gli stessi personal computer ora lavorano sempre più spesso collegati tra loro in reti, che possono essere "locali", in altre parole limitate all'ambiente (ad esempio ufficio) nel quale sono attivi (LAN), oppure definite in un ambito territoriale comprendente, in genere, la città nella quale si opera (MAN), oppure reti "geografiche" (WAN) che consentono di collegare utenti situati in nazioni e/o continenti diversi.

La più nota delle reti geografiche è appunto Internet che consente non solo una connettività globale, tra ogni utente dotato di modem, ma sempre più frequentemente anche transazioni economiche per via telematica, con vere e proprie vendite "on line" di prodotti e servizi.

Con la decentralizzazione delle risorse informatiche, l'uso di desktop sempre più potenti ed infine con Internet, la Sicurezza Informatica è divenuta materia d'ordinaria discussione.”[4]

Una delle cose che molti non addetti lavori non sanno, ovvero conoscono solamente di sfuggita, è l'esatto significato dell'acronimo CIA, ovvero *Confidentiality, Integrity, Availability*, in altre parole confidenzialità, integrità e disponibilità delle informazioni.

Confidenzialità.

Un sistema raggiunge gli obiettivi di sicurezza prefissati quando i dati non sono accessibili o comunque interpretabili dai non aventi diritto. Ciò significa che, anche se i dati dovessero essere intercettati, la loro lettura deve risultare impossibile o, per essere più realisti, eccessivamente complessa.

Integrità.

In un'ottica generale di sicurezza non deve essere possibile alterare i dati oggetto di una qualsivoglia transazione. Dette informazioni devono rimanere appunto integre. Questo fattore riveste particolare importanza, soprattutto se si fa riferimento ad operazioni come la contrattualistica digitale, l'e-procurement e le altre manifestazioni d'e-business, in qualsiasi accezione.

Disponibilità.

I dati, gli accessi e i servizi fruibili per via infotelematica devono essere disponibili sempre agli aventi diritto. Aggredire questa terza componente, soprattutto nei processi d'e-business, significa una sola cosa: no business.[5]

4. La definizione legale di sicurezza informatica

Ritengo che l'immagine sopra riportata possa essere sufficientemente esplicativa, ma per ribadire alcuni concetti:

La "sicurezza" dei dati e delle informazioni è un insieme più ampio della sola "sicurezza" informatica, comprendendo anche la c.d. "sicurezza fisica" dei luoghi, delle persone e della c.d. "logistica". Attuare la c.d. "sicurezza dei dati" non è possibile se non ricorrendo a strumenti di tipo legale, oltre che ad - ovvi -accorgimenti tecnici , e - cosa probabilmente ancora più importante - attraverso accorgimenti organizzativi, intendendo tale termine come l'insieme delle risorse disponibili atte e necessarie alla protezione dei dati e delle informazioni.

5. Sicurezza informatica, dei dati e delle informazioni.

Occorre prestare attenzione alla circostanza che qualunque azione compiuta attraverso mezzi informatici e telematici ha **sempre** un "riflesso" in campo giuridico. Infatti, rendere non disponibile un servizio può costituire un illecito contrattuale (se magari non abbiamo a disposizione la banca dati on-line), un illecito civile anche non contrattuale, o, addirittura, un illecito penale (nel caso in cui, per esempio, dei dati siano alterati e/o modificati).

Questa situazione può significare, inoltre, possibilità di avere richieste di risarcimento danni tali da fare desistere dalla voglia di continuare a svolgere l'attività, in alcuni casi. Ricordo, ove fosse necessario, che la legge organicamente intervenuta nella materia è la n.547 del 23 dicembre 1993, n. 547. Ad essa segue la legge 31 dicembre 1996, n. 675 in tema di dati personali (meglio nota come "legge sulla privacy", concetto compreso nella legge stessa ma più ristretto rispetto a quello di "dato

personale”) cui vanno allegati i provvedimenti applicativi e “satelliti” (in particolare il regolamento di cui al DPR 28 luglio 1999, n. 318 sulle misure di sicurezza minime). Vi sono poi varie norme concernenti la c.d. “pedopornografia”, nonché le modifiche operate sulla legge n.633/1941 [6] sul c.d. “diritto d’autore”, (sono state modificate le sanzioni penali connesse alla riproduzione illegale di software).

6. Affrontare il problema

Nel corso dei prossimi capitoli cercherò di spiegare com’è possibile il raggiungimento del livello necessario a garantire ad un’azienda oppure ad un privato una certa “tranquillità operativa”, ma sin d’ora è importante introdurre alcuni concetti base indispensabile a garantire un corretto approccio al problema. Che la sicurezza debba considerarsi un vero e proprio processo lo abbia già detto ma forse è utile precisare alcune semplici, ma basilari, modalità operative.

Prima di tutto è importante affermare che un approccio al problema “a compartimenti stagni” può rivelarsi determinante in senso negativo.

Le soluzioni di sicurezza sono, infatti, sempre multi livello, cioè affidate a più componenti collegati tra loro. E quell’umana, come vedrete, gioca un ruolo molto importante. Ad attacchi distribuiti vanno contrapposte difese dello stesso tipo. È necessario a questo punto prendere confidenza con tre delle leggi fondamentali della sicurezza informatica:

***Mai dire mai**: il dichiarare un sistema, un approccio, una soluzione, una metodica definitivamente sicuri e inattaccabili significa, a prescindere dalla scaramanzia, peccare di superficialità.*

***La sicurezza totale non esiste**: è evidentemente un postulato, ma è indispensabile ribadirlo, specie se si guarda al problema da una prospettiva d’alto livello.*

***Non si possono risolvere i problemi di sicurezza con il solo software**. Conosciuta anche come la legge di Ranum, quest’affermazione è un chiaro messaggio: il malicious hacking si affronta su più livelli.*

I concetti sono esattamente gli stessi da un punto di vista legale, sia dal lato attivo (ovvero di chi debba prendere delle misure atte a scongiurare eventuali conseguenze nefaste) sia dal lato passivo (ovvero di chi debba semplicemente applicare alcune norme “tecniche” che spesso sono divenute espressamente norme giuridiche).[7]

Prima di esaminare le problematiche strettamente legate all'utilizzo di un particolare Sistema Operativo ovvero di questo o quell’applicativo, sarebbe opportuno cercare di comprendere, teoricamente, di cosa esattamente stiamo parlando e quali siano i mezzi a disposizione per raggiungere il nostro scopo. Laddove si faccia riferimento ai sistemi informatici, spesso si è portati a limitare quello che è il reale campo d'applicazione della parola “bene”, associandola esclusivamente a tre categorie:

- L’hardware: l’apparecchiatura;

- *Il software: i programmi necessari al funzionamento dell'apparecchiatura e utilizzati per l'elaborazione delle informazioni;*
- *I dati: le informazioni gestite dai programmi.*

Oltre a questi, infatti, non occorre aggiungere:

- *I supporti di memorizzazione: possono contenere il software ed i dati;*
- *Reti: permettono l'interconnessione dei vari sistemi consentendo quindi lo scambio d'informazioni;*
- *Gli accessi: la possibilità che è data ai soggetti di utilizzare il bene.*
- *Gli individui chiave: solo un attimo di attenzione per pensare a quanto tempo e quante risorse economiche occorrono per preparare adeguatamente un valido amministratore di sistema oppure un operatore specializzato nell'uso di un determinato programma.[8]*

La sicurezza informatica ha – conseguentemente - come obiettivo principale, quello di garantire, riducendo i rischi[9], un adeguato grado di protezione dei beni, mediante l'attuazione di un progetto di sicurezza globale che, partendo dalla definizione di una politica di sicurezza, tenga conto di tutti gli aspetti del problema e pervenga ad un livello di protezione, organizzativo ed informatico, che possa essere monitorato nel tempo.

Per raggiungere quello che è l'obiettivo principale, occorre garantire che il “bene” (nella accezione sopra specificata) mantenga inalterate nel tempo le seguenti proprietà:

- Disponibilità;
- Integrità;
- Sicurezza.

Tutte quelle circostanze potenziali che possono causare un danno rappresentano un rischio, così come occorre notare che un progetto o un programma di sicurezza non azzerano mai il relativo rischio: **la sicurezza totale è sicuramente un'astrazione e non esiste nella realtà.**

A maggior ragione anche quella giuridica; conseguentemente, se si vuole perseguire una strategia orientata alla sicurezza, vengono richiesti più livelli di vigilanza.

Oltre una certa “dimensione” dell'ente (dove i danni potrebbero essere più letali) da tempo sono state attivate procedure e sistemi basati in genere sulla separazione tra l'intranet interna e il web sulla rete pubblica, attraverso i firewall, sistemi d'identificazione fisici o logici.

Attualmente sistemi di questo tipo, su scala ridotta, incominciano ad essere utilizzati da singoli utenti,

per il semplice motivo che aumenta il rischio d'attacchi; da tempo sostengo che sistemi "always on" come l'Adsl, la fibra ottica e in prospettiva anche le reti mobili di nuovo tipo, offrono maggiormente il verso ad attacchi indesiderati.

Per questo si comincia a parlare anche di personal firewall, software o fisici da installare anche su un singolo Pc usato in casa.

Anche per questi esistono le leggi; soltanto ultimamente è stata eliminata la necessità di predisporre **per legge** misure di sicurezza adeguate su pc utilizzati a mero scopo personale (il che, attenzione, non è la stessa cosa di utilizzare a casa il pc per lavoro).

Scopo personale deve essere inteso nel senso di "scopo non avente finalità economiche".

Uno degli errori che sono comunemente effettuati quando ci si avvicina alla sicurezza informatica è costituito dalla mancanza di background sugli argomenti. In pratica si dà per scontato che il lettore conosca le tematiche. Esattamente la stessa cosa avviene quando si comincia a parlare degli aspetti strettamente legali legati alla sicurezza informatica; anche da un punto di vista giuridico il problema si presenta complesso, coinvolgendo diversi rami del diritto (civile, penale, amministrativo, internazionale, processuale, ecc.) con intrecci che a volte possono apparire non chiari, ma che – in realtà – ad un attento esame, possono essere ricondotti a fenomeni di più immediata comprensione e percezione.^[10]

7. I soggetti attivi dei possibili illeciti, ovvero le c.d. "figure Attive".

Per figura attiva intendo, in questa sede, l'artefice delle violazioni, che non è solamente l'hacker di turno. Da tenere presente che – tecnicamente - non è poi così facile parametrizzare le varie figure legate al mondo c.d. "hacker", per il semplice motivo che le motivazioni che spingono a compiere determinate azioni non sono comuni a tutti. Giuridicamente il discorso è molto semplice; come ho già scritto tempo fa ^[11], nel nostro diritto la tradizionale (e giornalistica) distinzione "hacker" (buono) e "cracker" (cattivo) non può esistere, in quanto i comportamenti tipicamente posti in essere da tali soggetti sono **sempre**, per il diritto italiano, dei reati, almeno allo stato attuale della legislazione. L'hacker buono, per il diritto, non può esistere. *Non potendo far altro, quindi, prenderò in prestito dalla letteratura le definizioni di base, condendole con alcune esperienze personali. Nel capitolo tre alcune indicazioni pratiche sulla nuova tendenza dell'hiring hackers^[12]. Parto dalla figura più conosciuta, quella dell'Hacker propriamente detto. Personalmente o definire hacker qualsiasi tecnico che applichi positivamente il proprio skill in materia di programmazione e utilizzo avanzato delle tecnologie. Gli hacker "puri", diventano Uber Hacker dopo un certo periodo di esperienza, quantificato, più che temporalmente (come si fa in alcune arti marziali) in attività scientifiche universalmente riconosciute^[13]. Per applicazione positiva intendo correzioni di eventuali errori di programmazione (debugging), miglioramento del design architettonico dei sistemi, scoperta, segnalazione e proposte di soluzione di security flaw^[14]. Ma l'opera dell'hacker deve fermarsi alla segnalazione e alla sperimentazione di laboratorio. Qualsiasi azione che vada oltre questo fa*

"sconfinare" il soggetto in un'altra categoria. Un esempio di questo sconfinamento è nei cosiddetti *White Hat Hacker* ^[15]. Si tratta di soggetti dall'elevato skill tecnico i quali sono stati coinvolti, almeno una volta, in episodi di violazione di sistemi altrui. Successivamente a questo loro "pentimento" hanno deciso di convertirsi all'hacking costruttivo. Non tutti credono in questi ravvedimenti, anche di questo parlerò tra poco. Andando oltre abbiamo i *Black Hat Hacker*. Sono personaggi che agiscono in una schiera molto ristretta di persone, cercano di operare nel modo più anonimo possibile, alcuni sono mossi da motivazioni filosofico/politico/sociali, altri invece sono soltanto dei criminali. Come la maggior parte dei criminali compone la categoria dei *Cracker*. I *Criminal Hackers* sono abbastanza e compiono le loro azioni a fini distruttivi, di lucro (mercenari) frodi, spionaggio industriale e via dicendo. Sono gli attori che i security manager aziendali dovranno combattere maggiormente durante la loro attività. Ricordio che la maggior parte degli atti di hacking, a prescindere dalle loro motivazioni sono da considerare illegali. ^[16]

Il che, comunque, vuol dire che possa rischiare vari anni di soggiorno nelle patrie galere, in quanto la pena prevista per un DoS ^[17] può andare – come minimo, senza considerare eventuali aggravanti e “salvo che il fatto non costituisca più grave reato – da sei mesi a quattro anni di reclusione. Va aggiunto solo che tale comportamento costituisce un preciso obbligo di legge imposto sia sul titolare di qualsiasi azienda, sia, in maniera specifica, sul soggetto che possa in qualche modo rivestire la funzione di “manager della sicurezza”, a prescindere da come questi sia “chiamato” nell’ambito dell’organigramma aziendale, dovendosi fare riferimento alle funzioni effettivamente svolte e non a quelle soltanto scritte sulla carta. ^[18]

8. Le figure "Passive".

Per figura passiva si intende in questo caso la figura specifica e specializzata dell’operatore della c. d. “*defensive infowarfare*”. Esistono, nel nostro paese, una serie di norme impositive che determinano la necessità della redazione di un "Piano per la sicurezza" (DPCM 8/2/99 e circolare 22/99 dell'AIPA ^[19]). Questo è fondamentalmente relativo a questioni inerenti alla firma digitale; tuttavia si tratta di concetti che non si ritarderanno a trasporre in altri settori. A tal proposito ricordio l'intervento normativo del DPR 318/99, il quale, partendo dalle misure minime di sicurezza per i dati personali, stabilisce una serie di parametri per:

- Analizzare e definire le misure minime di sicurezza, vale a dire implementare una serie di misure minime studiate in base ai diversi *contesti*, in altre parole le varie architetture.
- Le metodiche d’analisi dello scenario, in altre parole dei contesti sopra indicati;
- la pianificazione di un *Documento Programmatico per la Sicurezza*, che, in realtà, interagisce concettualmente con il piano per la sicurezza di cui al punto uno.
- la procedura attuativa del piano, anche in relazione alle misure di sicurezza implementate.

A dire il vero le normative sopra citate ^[20] parlano (specialmente nel caso del DPR 318/99) di amministratore della sicurezza. Nell’ambito delle organizzazioni imprenditoriali “moderne” esiste, in

linea di massima, una organizzazione dei ruoli e delle risorse umane. Ognuna di tali figure sarà investita per la parte di propria competenza delle responsabilità inerenti la protezione dei dati e delle informazioni. Questo significa due cose: assumersi le proprie responsabilità senza nascondersi dietro un dito e, per questo, farsi corrispondere un adeguato compenso.[21] Infatti ricordo che da qualche tempo non è più valido in modo “assoluto” il vecchio principio della c.d. “personalità” della responsabilità penale. Proprio di recente è stata approvata la legge che stabilisce la c.d. “responsabilità amministrativa” [22] delle società e degli organismi complessi, responsabilità che è stata chiamata “amministrativa” proprio perché non poteva essere chiamata “penale” stante il dettato costituzionale, ma che prevede una responsabilità per fatto altrui, come vedrò in seguito, che può arrivare alla c.d. “pena di morte” per la società che lasci “delinquere” un soggetto [23] sul quale deve esercitare il proprio controllo, essendo prevista l’interdizione allo svolgimento dell’attività della società stessa. A prescindere da quanto definito nelle normative appena citate, appare importante definire ruoli e responsabilità nella gestione delle informazioni.

9. Uno schema gerarchico.

Ecco un possibile schema gerarchico:

Come potete vedere dal grafico[24], in cima alla linea gerarchica c'è il “proprietario delle informazioni”.

Ai fini della legge 675/96, spesso chiamata “legge sulla privacy”, ma che in realtà più esattamente è denominata “legge sul trattamento dei dati personali” [25], questo soggetto è individuato nel “titolare del trattamento” [26]. Sempre ai fini della medesima legge, il vero “proprietario” dei dati è in realtà il soggetto al quale i dati si riferiscono, in altre parole il c.d. “interessato” [27]. Altra figura che potrebbe essere assimilata a quella del c.d. “amministratore di sistema”, previsto specificatamente dal D.P.R. n.318/99, applicativo del secondo comma dell’art.15 della legge 675/96, anche se, in prima battuta, occorre rilevare come non vengano previsti compiti e doveri specifici per tale figura, genericamente sottoposta al titolare ed al responsabile, e gerarchicamente sopra ordinata al solo “incaricato del trattamento”. Quest’ultimo, nella struttura della legge 675, costituisce il punto finale della scala, probabilmente l’end user, in altre parole l’impiegato o figura simile esistente in azienda.

10. Breve analisi dei soggetti che possano utilizzare illecitamente i mezzi informatici e telematici

Se si esaminano, da questo punto di vista, i soggetti che possano utilizzare illecitamente i mezzi informatici e telematici, ovvero la stessa rete Internet, ritengo che possano essere individuate alcune macro - categorie come quelle sotto elencate:

- *Dipendenti*

- *Collaboratori*
- *Clienti*
- *Utenti*

Ovviamente la tipologia di controllo che l'azienda può operare nei confronti delle sopra citate categorie varia sostanzialmente laddove la prima, quella dei dipendenti, riceve una tutela specifica fornita in particolare dall'art. 4 [28] della Legge n.300/1970 (Statuto dei Lavoratori), oltre naturalmente a quella fornita dalle altre leggi, che si applicano a tutte le categorie menzionate.[29]

A mio personale parere occorre chiarire nell'ipotesi di "controllo" di soggetti che NON SIANO dipendenti con tutta probabilità l'azienda ha minori restrizioni per quanto concerne la possibilità di poter tutelare i propri interessi.

Appare alquanto ovvio il concetto secondo il quale da una parte l'azienda abbia la possibilità – in base al c.d. "potere direzionale" dell'imprenditore – di emanare direttive cogenti nei confronti dei propri dipendenti, mentre dall'altra nei confronti di tutti i soggetti che *non siano* dipendenti l'azienda non ha altro strumento che quello contrattuale, con tutte le conseguenze del caso. E' appena il caso di notare come le c.d. "*policies*", termine di derivazione anglosassone, nel nostro ordinamento giuridico non possano che rientrare in una delle due categorie sopra specificate, direttive aziendali ovvero clausole contrattuali. La "sicurezza" in termini legali va intesa come la possibilità di conservare e proteggere valori, economici e non; conseguentemente, non può che essere un argomento con ampie intersezioni ed aspetti legali, tutte le volte che i valori appena menzionati siano riconosciuti e/o in qualche modo presi in considerazione dall'ordinamento giuridico. Forse non è inutile ricordare ancora una volta che– direi quasi ovviamente - il diritto si occupa da molto tempo di circostanze, attività ed informazioni che attualmente trovano come principale "luogo" di diffusione e svolgimento la rete Internet ovvero il c.d. "mondo informatico e telematico".

11. Scopo di lucro e scopo di profitto

In via preliminare va inoltre chiarito un aspetto fondamentale del dettato specifico di alcune delle norme sopra menzionate, ovvero la distinzione tra "fine di lucro" e "fine di profitto", rilevante anch'essa per molte delle fattispecie appena elencate.

Orbene, "...Nel lessico comune (cfr. dizionari della lingua italiana) il lucro è indicato, anzitutto e soprattutto, come sinonimo di guadagno, è qui preminente stabilire con quale significato e portata venga usato il vocabolo lucro nell'ordinamento giuridico e, in particolare, nella materia specifica. E' pacifico che nel nostro ordinamento penale il concetto di lucro è più ristretto di quello di profitto. Per tutte, vedasi Cass., sez. II, 9.6.1981 (in Cass. pen. 1983, 316): "La nozione di profitto prevista dall'art. 648 c.p. comprende non solo il lucro, ma qualsiasi utilità, anche non patrimoniale, che l'agente si proponga di conseguire". Viceversa, il fine di lucro "deve necessariamente essere interpretato come fine di trarre un guadagno economicamente apprezzabile" (così - in tema di gioco d'azzardo art. 721 c.p. - Cass. pen. sez. III, 6.5.1998, n. 7144, in Giust. pen. 1999, II, 79).

Nell'art.62 n. 4 c.p. (come modif con L. 7 2.90 n. 19) il termine "lucro" è collegato al verbo "conseguire". Insegna la S.C. che i "motivi di lucro", cui si riferisce detta norma, vanno intesi "in termini di volontà di acquisire, quale risultato delittuosa, un vantaggio patrimoniale" (v. Cass., sez. V, 14.11.90, in Giust. pen. 1991, II, 457). Pare corretto ritenere che "conseguire" o "acquisire" siano verbi congrui al raggiungimento di un risultato "in positivo" (cioè un accrescimento patrimoniale), piuttosto che ad evitare una conseguenza "negativa". Quanto alla specifica materia in esame, esorbita dall'ambito della presente pronuncia, in quanto riguardante fatti realizzati vigente l'art. 171-bis L.633/41 nella formulazione anteriore alla modifica apportata con L.248/00, stabilire se nello scopo di "trame profitto", di cui all'attuale testo della norma, rientri una condotta come quella oggetto del presente processo. Peraltro, la modifica introdotta da quest'ultima Legge non è priva di rilevanza, in quanto conferma una consapevole distinzione, da parte del legislatore, tra i concetti di "lucro" e di "profitto". [30] *Quindi, sintetizzando quanto - molto chiaramente - ha esposto la Corte d'Appello di Torino, "lucro" – in senso penalistico - è espressione e concetto meno ampio di "profitto", che contiene, per così dire, al proprio interno, anche il mero risparmio, concetto – al contrario – non compreso in quello di "lucro". Ancora prima di analizzare nello specifico i diversi illeciti di tipo penale (gli illeciti di matrice civilistica saranno analizzati separatamente nel prosieguo), ritengo che sia importante chiarire la posizione del c.d. "operatore di sistema", figura chiave della legge 547/93. Varie norme, tra quelle introdotte dalla l. 547/1993, fanno riferimento (prevedendo aggravanti speciali) alla figura dell'operatore di sistema[31]. A mero titolo esemplificativo, gli articoli 615-ter, 617-quater, 635-bis, 640-ter c.p., prevedono come ipotesi aggravata specifica le azioni compiute dal c.d. "operatore di sistema". Va chiarito che la nozione d'operatore di sistema - non fornita dal legislatore [32] - risulta peraltro molto ampia. Secondo i più, non può ritenersi circoscritta a figure poste ai vertici del settore informatico (esempio: responsabile della sicurezza, amministratore di sistema, information security manager, aggiungerei responsabile ex art.8 legge 675/96, ecc.), ma effettua un riferimento implicito al rapporto esistente tra operatore e sistema informatico o telematico.[33]*

12. La definizione "minima" di "sistema informatico" o "telematico" in senso giuridico.

A parere di chi scrive, la nozione di "sistema informatico o telematico" appare assai ampia, poiché si deve ricondurre lo schema giuridico ad un preesistente schema logico – tecnico. Per tale motivo un "sistema informatico" esiste laddove possa essere dimostrata l'esistenza dei seguenti elementi base:

- **un input (di qualunque genere, non necessariamente "multi purpose")**
- **un insieme di hardware e software che "processi" tale input**
- **un output, anch'esso di qualunque genere.**

Inoltre, anche se la legge parla praticamente sempre di "sistema informatico o telematico", ritengo che le differenze siano minime, nel senso che un sistema "telematico" differisce ben poco, da un

punto di vista giuridico, da un sistema “informatico”, se non per il fatto che sia raggiungibile attraverso qualunque un mezzo di comunicazione. In buona sostanza, un “sistema telematico” è un sistema informatico connesso, attraverso una rete non locale (tipicamente una W.A.N., da contrapporsi ad una L.A.N., rete locale) ad altri sistemi consimili; come vedrò nel prosieguo, la differenza tra L.A.N. e W.A.N. ha rilevanza ai fini dell’applicazione del sistema delle c.d. “misure minime di sicurezza” previste dal DPR n.318/99. Per la norma penale – la quale, evidentemente, intende sanzionare con maggior rigore le infedeltà di coloro che, dotati di particolari privilegi, dovrebbero proteggere il sistema e che, al contrario, approfittino di tale loro particolare posizione – sarebbero, quindi, “operatori di sistema” tutti i soggetti che, per un qualche motivo, potrebbero ritenersi agevolati nella commissione del reato[34]. Ne consegue che anche i semplici “terminalisti”, indipendentemente dal possesso di cognizioni tecniche, potrebbero rientrare nella categoria di cui si tratta, a condizione però, che essi, come detto sopra, godano di un insieme – per così dire – “minimo” di privilegi. La giurisprudenza – infatti - ha ritenuto operatore di sistema un tecnico software (esterno) che era autorizzato ad accedere alle macchine.[35] La posizione del c.d. “operatore di sistema” (con tutte le conseguenze che comporta per quanto concerne la posizione dei soggetti che operino all’interno dell’azienda) si applica sia ai dipendenti sia ai collaboratori, occasionali e non, esterni ed interni, purché in possesso dei requisiti “minimi” di cui sopra), e pertanto è lecito affermare che il mancato rispetto delle norme relative alla sicurezza, comportamento sicuramente lesivo della fiducia che comunque contraddistingue i rapporti tra datore di lavoro e dipendente, potrà trovare necessaria ed ulteriore collocazione nel mancato rispetto delle norme contrattuali di lavoro.

13. Brevi conclusioni

Quali conclusioni possono essere tratte da quanto scritto in precedenza?

A parere di chi scrive, principalmente, la presa di coscienza della circostanza che sicuramente situazioni come quelle descritte esistono nel nostro paese, che tali situazioni andranno ad aumentare con il corso degli anni e, conseguentemente, il giurista e l’avvocato in particolare dovrebbe essere in grado di comprendere appieno alcuni aspetti “tecnici” al fine di poter correttamente impostare i problemi da un punto di vista giuridico.

Avv. Luca-M. de Grazia

[1] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, , capitolo primo, www.internos.it/security.html

[2] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Luca-M. de Grazia, capitolo primo.

[3] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de

Grazia, capitolo primo, www.internos.it/security.html

[4] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[5] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[6] Legge 18 agosto 2000, n. 248

[7] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[8] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[9] Si tratta di una tendenza a ridurre I rischi assolutamente dovuta e richiesta dalla legge.

[10] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[11] L'hacker "buono" in Italia non può esistere - 26/08/1999 in www.degrazia.it/infodirnet/rubriche/articoli/articoli/p1.html

[12] Con Hiring Hackers intendiamo la politica, posta in essere da alcune aziende, di "arruolare" hackers o sedicenti tali per la verifica delle vulnerabilità.

[13] Un esempio di queste attività può essere costituito da posting su mailing list riconosciute quali BugTRaq, ovviamente riscontrati e confermati dall'intervento del vendor citato e dai partecipanti al gruppo.

[14] Security flaw: bug della sicurezza, lacuna, dovuta solitamente ad un difetto di programmazione e/o impostazione architetturale di un determinato prodotto o infrastruttura.

[15] Hacker dal cappello bianco.

[16] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[17] Vedi nota precedente per riferimenti specifici.

[18] Norme di riferimento: art. 1 legge 675/96, art.8 legge 675/96; art.35 e 36 legge 675/96; art.6

DPR n.318/99; art. 5 DPR n.231/2001.

[19] Per ulteriori informazioni invitiamo il lettore a consultare il sito www.aipa.it

[20] Per un approfondimento di tipo normativo consiglio la consultazione del libro.

[21] In Italia, parte del top management" fa "orecchie da mercante" su questo argomento.

[22] DECRETO LEGISLATIVO 8 giugno 2001, n. 231 (in Gazz. Uff., 19 giugno, n. 140). - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.

[23] **Articolo 5 - DECRETO LEGISLATIVO 8 giugno 2001, n. 231 Responsabilità dell'ente**

1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi

[24] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[25] Nella lingua italiana il significato esatto di “privacy” è riservatezza, che costituisce un insieme più ristretto rispetto al trattamento dei dati personali al quale fa riferimento la legge, all’art. 1 comma 1: *“La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, **con particolare riferimento alla riservatezza e all'identità personale**; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione”*

[26] Legge 675/96, art.1 2 comma lettera “d) per "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;”

[27] Legge 675/96, art.1 2 comma lettera f) per "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

[28] Art. 4 Legge n.300/1970 - Impianti audiovisivi.

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede la Direzione regionale del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, la Direzione regionale del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti della Direzione regionale del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

[29] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[30] Corte di Appello di Torino, Sezione IV Penale, Sentenza 13 dicembre 2000 - 15 gennaio 2001, in http://www.penale.it/giuris/meri_100.htm

[31] Nel commercio elettronico la figura dell'operatore di sistema si dimostra assai critica in quanto si ritiene comunemente, anche su base statistica, che una percentuale considerevole di illeciti commessi su o mediante sistemi informatici o telematici faccia capo a personale interno all'impresa colpita (c.d. insiders).

[32] L'art. 1, lett. c) DPR 318/1999 fissa, in verità, una definizione che potrebbe fare il nostro caso. Secondo il regolamento, gli "amministratori di sistema" sono coloro "cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione". Ma è evidente che quella dell'amministratore di sistema, pur collocata al vertice "tecnico" del sistema, è soltanto una delle ipotesi di "operatore di sistema".

[33] Manuale di Infosecurity Management, Angelo Verde Editore S.r.l., Dario Forte e Luca-M. de Grazia, capitolo primo, www.internos.it/security.html

[34] Qualcuno ha parlato di "violazione del dovere di fedeltà sia nei confronti del titolare del sistema, sia delle persone i cui interessi sono gestiti dal medesimo sistema". C. Pecorella, Il diritto penale

dell'informatica, Padova, 2000, pag. 121.

[35] La sentenza citata (Cassazione, Sezione V Penale, 7 novembre - 6 dicembre 2000, n. 1675) è pubblicata sul sito Penale.it all'indirizzo www.penale.it/giuris/cass_011.htm.