LE LEVE E LE SFIDE PER IL RILANCIO DEL PAESE

LE FRONTIERE DELLA SICUREZZA
SICUREZZA INFORMATICA E PREVENZIONE DEL CYBERCRIME
CERNOBBIO 3 SETTEMBRE 2017

Prof.ssa Paola Severino

SOMMARIO: 1. Premessa. 2. L'ampliamento delle competenze per il Tribunale delle imprese. – 3. La sicurezza informatica: un valore da tutelare. – 4. La criminalità informatica: nuovi rischi da affrontare – 5. Segue: la duttilità delle tecniche di reazione. – 6. L'importanza della prevenzione. – 7. L'intervento della sanzione penale. – 8. Uno sguardo al futuro: le sfide e le opportunità.

1. Premessa

Ringrazio gli organizzatori per l'invito a intervenire in questo prestigioso consesso e a prendere parte a dibattiti sempre stimolanti e costruttivi. Forse qualcuno si stupirà nel vedere un giurista parlare di sfide per il futuro del Paese, ma io credo che la crescita, economica e non solo, di un Paese, passi anche attraverso un sistema di giustizia adeguato e funzionale agli scopi di evoluzione che si selezionano come primari.

A questo proposito vorrei ricordare l'ultima occasione in cui ho avuto l'onore di prendere qui la parola, nell'ambito di un confronto al tempo dedicato al tema del contrasto alla corruzione, e ricordo come la discussione

sui costi del fenomeno corruttivo abbia poi rappresentato il volano per la riforma del settore, attuata nel nostro Paese sulla scia degli *input* sovranazionali.

Anche in quest'occasione mi occuperò – ancorché sotto un profilo completamente diverso – degli interventi da proporre affinchè la giustizia non rappresenti più il vagone di coda che rallenta l'evoluzione dell'Italia, ma divenga invece spinta sinergica allo sviluppo socio-economico della nostra collettività.

Vorrei occuparmi in particolare di due aspetti, auspicando che il Forum Ambrosetti possa nuovamente rappresentare un volano per stimolare il legislatore ad intervenire.

2. L'ampliamento delle competenze del Tribunale per le imprese.

Il primo aspetto riguarda l'ampliamento delle competenze ora attribuite al Tribunale delle imprese. Come forse qualcuno sa, l'introduzione del Tribunale delle imprese per alcune limitate materie civilistiche di particolare rilievo nel mondo dell'economia ha rappresentato il primo, timido tentativo di testare il funzionamento di una giustizia specializzata in settori che richiedono un elevato tecnicismo. Ora possiamo dire che il test è riuscito, perchè quella sia pur parziale riforma ha portato ad una riduzione della durata dei processi, ad una rilevante crescita della prevedibilità degli esiti, ad una diminuzione del numero delle impugnazioni. In altre parole ha dimostrato che un giudice "specializzato" pronuncia sentenze più rapide, più solide, tendenti all'omogeneità.

Sorge allora spontanea la domanda: perchè non estendere l'esperimento al settore del diritto penale d'impresa? Un settore nel quale la complessità delle tematiche societarie (si pensi all'aggiotaggio o all'*insider trading*), delle

tematiche di bilancio (false comunicazioni sociali), delle tematiche fiscali (risparmio, elusione ed evasione fiscale), delle tematiche di responsabilità delle persone giuridiche (D.L.vo n. 231/2001) esige la presenza di un giudice penale particolarmente esperto non solo del sistema sanzionatorio, ma anche degli aspetti più tecnici della materia societaria.

Non è certamente questa la sede per affrontare analiticamente una proposta complessa, ma è questa la sede più idonea per lanciare e condividere con la folta e qualificata comunità finanziaria qui presente un'idea volta a ribadire l'assoluta necessità di una giustizia efficiente per la crescita economica del Paese.

3. La sicurezza informatica: un valore da tutelare.

Il secondo aspetto di cui vorrei sinteticamente occuparmi oggi è relativo alla sicurezza informatica. Mi occuperò dunque non di frontiere tradizionali e di 'violazioni fisiche' di dette frontiere bensì di confini in certo modo meno definiti ma altrettanto importanti e meritevoli di un serio presidio.

Concentrerò pertanto la mia attenzione sui fenomeni di *cyber attack*, sulle strategie di *cyber security* e sulle tecniche più adeguate per sanzionare il *cyber crime*.

Non sarò certo originale se sottolineo come l'utilizzo di internet rappresenti da un lato un fenomeno imprescindibile per lo sviluppo economico di un Paese, del suo sistema imprenditoriale, dei suoi apparati di sicurezza, delle sue istituzioni ed anche per la vita di noi tutti singolarmente presi. Esso inoltre consente di accelerare lo sviluppo di fattori alternativi rispetto a quelli di un'economia tradizionale, sostituendo ad esempio gli impiegati di banca addetti agli sportelli con impiegati di banca esperti di *home banking*, oppure i venditori al dettaglio con gli addetti al deposito, al

trasporto ed alla consegna dei prodotti venduti su piattaforma *e-commerce*. Esso infine impone anche alla luce dei dati citati venerdì da Valerio De Molli (3,2 milioni di lavoratori sostituiti nei prossimi 5 anni a causa dell'automazione) di formare nuove generazioni di esperti e di addetti, capaci di confrontarsi con prospettive multidisciplinari e con nuovi orizzonti di sviluppo sociale ed economico (v. *startup*).

Sotto tutti questi aspetti il fenomeno della comunicazione via internet non può e non deve spaventare, ma anzi può rappresentare per un Paese, come l'Italia, certamente capace di svilupparne le potenzialità e di consolidare le eccellenze che già emergono nel settore, una nuova strada di crescita. Se i nostri giovani vorranno affrontare questa sfida, noi, le nostre Università, le nostre imprese saranno e sono già pronte ad affrontarla e vincerla.

D'altra parte, non vi è dubbio che internet sia già diventato non più uno strumento "da regolare", ma uno strumento a supporto della regolazione per i pubblici poteri. Si pensi all'impego delle nuove tecnologie per la indicizzazione e il controllo incrociato di dati in materia fiscale, all'utilizzo di algoritmi intelligenti per il calcolo degli ammortamenti previdenziali e degli oneri contributivi, alla prenotazione o erogazione di servizi essenziali, all'impiego a livello investigativo e di *intelligence*, di sistema di monitoraggio e filtraggio delle comunicazioni per prevenire atti di terrorismo.

Né vi è dubbio che internet abbia rappresentato la fonte di nuovi e diversi modelli d'impresa, creando attraverso la cosiddetta *sharing economy* nuovi mercati, nuove utilità, nuovo e più distribuito benessere, nuovi mezzi di esplorazione o addirittura di condizionamento delle scelte del consumatore.

4. La criminalità informatica: nuovi rischi da affrontare.

È però altrettanto evidente che l'uso di strumenti digitali rappresenta anche la fonte di nuovi e diffusi rischi, implementati dalle dimensioni che può con essi assumere la violazione della *privacy* dei singoli, la captazione di dati sensibili per le imprese e per il mondo della finanza, l'aggressione a segreti nazionali relativi alla sicurezza ed alla difesa. Rischi molto più difficili da contenere rispetto al passato, considerando che l'anonimato garantito dal mezzo informatico non solo rappresenta un incentivo al *cyber attack*, ma ne può moltiplicare le possibilità di riuscita, contemporaneamente indebolendo enormemente le possibilità di reazione efficace attraverso i sistemi sanzionatori tradizionali. Si pensi all'uso di *bitcoin* a fini di riciclaggio oppure a fini di estorsione in danno di aziende costrette a pagare per ottenere la restituzione di dati cancellati attraverso la intromissione di un virus. Si pensi all'apertura e chiusura nel giro di poche ore di caselle di posta elettronica, al fine di perpetrare attraverso di esse truffe o altri reati contro il patrimonio. Si pensi alla possibilità di intromettersi nelle comunicazioni commerciali acquisendo l'identità di un altro soggetto ed ottenendo indebiti benefici.

In altri termini, la *duttilità delle tecniche d'attacco*, richiede il costante adeguamento della reazione rispetto alle nuove forme di aggressione. Il contrasto della criminalità informatica è infatti reso particolarmente arduo dalla continua "metamorfosi" degli attacchi informatici sulla base dei nuovi ritrovati tecnologici.

Si è già detto del crescente utilizzo delle *criptovalute* e delle nuove frontiere del *cyber-laundering*, incentivato da una moneta virtuale che sembra sfuggire ad ogni forma di controllo e di regolazione da parte dei pubblici poteri benché il suo utilizzo sia in rapida crescita. Il fenomeno è

assai difficile da controllare. Spesso, le transazioni vengono effettuate nella parte oscura della rete (c.d. *dark web*) e, in linea di principio, potrebbero essere legate ad operazioni economiche tanto lecite quanto illecite.

Un esempio emblematico dell'evoluzione delle forme di attacco è dato altresì dalla diffusione di *ransomware* e dall'affinamento delle tecniche di criptazione di sistemi informatici mediante l'invio di *virus-esca*. Assai di frequente la cronaca quotidiana riporta notizie di attacchi informatici perpetrati al fine di ottenere il pagamento di un riscatto, spesso in criptovaluta, quale prezzo per il ripristino del sistema "infettato". Anche qui l'attività di contrasto è resa particolarmente complessa dalla creazione di *malware* sempre più evoluti (*CriptoLocker, WannaCry Locker*, per ricordarne alcuni), nonostante l'apparente semplicità del loro funzionamento sulla base della crittografia asimmetrica (che è la stessa utilizzata per le transazioni commerciali e i dispositivi di firma digitale).

5. Segue: la duttilità delle tecniche di reazione.

Tutto ciò spiega perché, se si vuole sviluppare una sana economia informatica, così come l'Italia e l'Europa, in quanto leader mondiale in ricerca e innovazione, sa e può certamente fare, occorre pensare ad un approccio alla regolazione molto diverso rispetto ad altri fenomeni di indebito utilizzo del sistema finanziario.

In primo luogo, così come la *sharing economy* apre ad una latitudine sconfinata di commerci, la prevenzione e la repressione del fenomeno devono avere una dimensione assolutamente transnazionale. L'insediamento di *provider* in luoghi che ne favoriscono l'anonimato e ne coprono la responsabilità, ad esempio, può rendere inefficace anche la migliore normativa nazionale di prevenzione.

L’apertura consentita di siti opachi in luoghi che non ne disciplinano la registrazione comporta la possibilità di utilizzarli per la diffusione di fenomeni di *deep web*, contenitori di inimmaginabili nefandezze, senza che il sistema legale possa intervenire.

In altri e più generali termini, la rete di prevenzione e controllo, per essere efficace non dovrebbe presentare smagliature, per evitare che in esse si inseriscano i fenomeni illeciti, sfruttandone le carenze.

Accordi internazionali, dunque, per regolamentare un sistema di comunicazioni internazionali.

A questi principi si ispira la recente direttiva europea (n. 1148/2016) la quale nel “considerando” 43 recita testualmente che “data la dimensione planetaria dei problemi relativi alla sicurezza delle reti e dei sistemi informatici, è necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti della sicurezza”.

In secondo luogo, occorrerà attrezzare dei veri e propri osservatori dotati delle complesse e multidisciplinari conoscenze necessarie al fine di segnalare i rapidissimi mutamenti delle tecniche di attacco, studiare le possibilità di prevenirle e diffondere al massimo le informazioni necessarie ad evitare l’aggressione.

Così, ad esempio, per combattere efficacemente il fenomeno, di cui parlavo prima, delle creazioni di *malware* sempre più evoluti nell’ambito del fenomeno dei *virus-esca*, gli utenti dovrebbero essere costantemente informati sull’evoluzione delle tecniche di *social engineering* che inducono la cooperazione artificiosa della vittima dell’attacco (ad es. apertura di una email sospetta, inserimento dei dati della propria carta di credito su un sito costruito *ad hoc* etc).

Così pure, sempre a titolo di esempio, per prevenire il fenomeno, cui ho fatto cenno, del *cyberlaundering*, appare utile concentrarsi sulla necessaria esistenza di una *block chain*, sulla quale vengono registrate, in modo accessibile, tutte le transazioni di ogni singolo *bitcoin*.

Con la conseguenza che ogni operazione di conversione, così come ogni ordine di pagamento da un "portafoglio" all'altro è, in linea di principio, perfettamente tracciabile. Tenuto conto di queste caratteristiche tecniche e del fatto che il lato oscuro del fenomeno sta nell'anonimato dei soggetti coinvolti nello scambio, occorrerebbe puntare, per la prevenzione, su un sistema di *block chain* che interdica operazioni provenienti da indirizzi criptati.

6. L'importanza della prevenzione.

Se si vuole fare il punto della situazione della prevenzione in Italia si potrebbe dire che da ultimo gli interventi più recenti hanno manifestato un approccio regolatorio serio e profondo, evidenziando la necessità dell'adozione di strategie nazionali e misure di sicurezza minime nell'ambito della Pubblica Amministrazione. Sul punto un importante traguardo è stato segnato nel dicembre 2013 con l'adozione da parte del Consiglio dei Ministri del *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*, documento che, concepito con intento eminentemente programmatico, ha visto una primaria attuazione con la successiva *Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015* in base alla quale sono state varate le *Misure minime di sicurezza ICT per le pubbliche amministrazioni* pubblicate in Gazzetta Ufficiale lo scorso 4 aprile. Tali fonti secondarie appaiono ispirate dall'intento di promuovere una cultura della prevenzione del *cyber-risk*, sulla base di un approccio innovativo di valutazione e gestione del

rischio medesimo. Un approccio che, più in generale, si palesa estremamente utile per il contrasto della criminalità informatica.

Quanto al settore privato e delle imprese, ancora molto c'è da fare sul piano della prevenzione, anche se i recenti interventi volti alla creazione di figure di *Data protection manager* anche in quel settore rappresentano un primo passo avanti.

Molto interessanti appaiono inoltre alcune recenti iniziative volte a creare un *framework* nazionale di *cyber security* il cui scopo è quello di offrire alle piccole e medie imprese un approccio omogeneo su base volontaristica che consenta di misurare il proprio profilo di rischio, configurare una strategia aziendale *cyber* ad esso adeguata, avvalersi dell'esperienza nel frattempo maturata tra aziende iscritte ad un circuito ed innovare tempestivamente i propri sistemi di difesa (v. *Italian Cyber Security Report* curato dal CIS e dal CINI).

Ancora una volta, è proprio in ambito europeo (Direttiva n. 1148/2016) che questi principi di autoregolazione vengono enunciati. Nel "considerando" 44 si invitano i Paesi membri a promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura di gestione del rischio, che comprenda tanto una corretta valutazione di esso quanto l'attuazione di misure di sicurezza ad esso adeguate.

Lo strumento preventivo e le fonti di autoregolazione rappresentano dunque l'ossatura su cui basare un approccio europeo di *cybersecurity* qualificando l'UE come istituzione internazionale capace di dare modelli di regolamentazione anche ad altri Paesi e di proseguire in quell'opera di pacificazione sociale e di stabilizzazione finanziaria di cui – come giustamente è stato osservato in molte delle relazioni dei giorni scorsi – noi tutti abbiamo goduto negli ultimi 60 anni.

7. L'intervento della sanzione penale.

Last but not least, occorre dare uno sguardo al tema sanzionatorio. In effetti, in uno scenario così ampio e per certi aspetti inquietante il diritto penale costituisce un presidio irrinunciabile di tutela di fronte alla crescente diffusione della criminalità informatica e di fronte alla molteplicità ed alla rilevanza degli interessi lesi dai comportamenti illeciti.

Si tratta di interessi di indiscusso rilievo come la personalità individuale, la riservatezza delle comunicazioni, la confidenzialità delle informazioni, i dati personali, il diritto d'autore. Si tratta di condotte illecite plurioffensive, che possono cioè ledere più di uno dei beni giuridici tutelati. Si tratta di comportamenti intrusivi o di captazione di dati, produttivi di danni economici molto significativi.

Per convincersene è sufficiente richiamare le statistiche diffuse dal *World Economic Forum* che lo scorso anno hanno stimato il costo globale della criminalità informatica in 445 miliardi di dollari all'anno, e evidenziato come le minacce derivanti dal *cyber space* costituiscano quelle più temute dagli utenti in termini di dannosità e probabilità di verificazione[1]. Al di là delle difficoltà connesse alla identificazione dei colpevoli e alla effettiva "giustiziabilità" degli attacchi informatici, sembra che la repressione del *cybercrime* non sia neppure da sola sufficiente a ridurre le allarmanti prospettive di crescita del fenomeno.

Le medesime statistiche riportate nel *WEF Report* prevedono infatti che, in mancanza di efficaci strategie difensive e preventive, nel 2020 le perdite

[1] Report Global Risks 2014 pubblicato sul sito internet istituzionale *http://www3.weforum.org*

economiche causate dalla criminalità informatica potrebbero arrivare fino a 3.000 miliardi di dollari[2].

Ecco che, a livello di politica criminale, le istanze connesse alla prevenzione degli attacchi e, più in generale, alla sicurezza informatica trovano linfa nella necessità di arginare un incremento statistico davvero preoccupante.

Se ci si chiedesse per quale motivo il fenomeno stia assumendo via via una ampiezza sempre maggiore, la risposta sarebbe evidente: il *cybercrime* ha connotati peculiari rispetto alla criminalità comune e ciò, dal punto di vista degli autori, agevola l'esecuzione delle varie condotte criminose. Alcune di queste caratteristiche, quali la *transnazionalità* e la *desensibilizzazione soggettiva* sono state da tempo individuate e hanno guidato gli Stati nella repressione del fenomeno.

Le violazioni perpetrate tramite il *cyber space* sono infatti, come si è già accennato, prive di confini fisici e di limiti geografici; spesso i criminali informatici agiscono da Paesi lontani, il più delle volte poveri e tecnologicamente arretrati, riuscendo a produrre effetti dannosi su sistemi informatici collocati in Stati economicamente forti. Ciò assicura, al contempo, l'impunità e il conseguimento di ingenti profitti. La spinta criminogena alla commissione di tali reati, peraltro, risulta accresciuta dalle minori remore morali connesse all'assenza di un contatto "fisico" tra il colpevole e la vittima, e alla diffusa consapevolezza da parte degli autori delle obiettive difficoltà di essere identificati.

Del resto, è ormai sotto gli occhi di tutti come gran parte della vita sociale e delle transazioni economiche si svolgano sulla piattaforma digitale. Non può quindi stupire il progressivo incremento, quantitativo e qualitativo, degli

[2] In questo senso anche il Consorzio Interuniversitario per l'informatica (CINI) nel documento *Il futuro della Cybersecurity in Italia*, ottobre 2015, p. 2

attacchi informatici, e che il *cyber* spazio sia divenuto, come da metafora, la "terra di mezzo"[3] della criminalità: dalle classiche truffe via *web*, a forme evolute di estorsione, dal *phishing* al furto di dati sensibili, dallo spionaggio e dal sabotaggio di dati ed informazioni, alla commissione di atti vandalici meramente emulativi.

Sebbene nel panorama globale il diritto penale dell'informatica sia una materia relativamente giovane, essa appare caratterizzata dal suo essere continuamente *in fieri*, di pari passo con l'evoluzione della scienza e della tecnica e con le "sfide" lanciate dal progresso tecnologico.

Un decisivo passo avanti nell'attività di contrasto del *computer crime* è stato compiuto nel 2001 con la stipula della *Convenzione di Budapest sul cybercrime.*

Essa rappresenta il primo accordo internazionale vincolante in materia ed ha il dichiarato obiettivo di realizzare una politica comune fra gli Stati membri mediante l'adozione di una legislazione appropriata che consenta il coordinamento delle attività volte a contrastare il crimine informatico. Sebbene l'ordinamento italiano fosse già per larga parte conforme alle disposizioni pattizie, la legge di ratifica della Convenzione (Legge 18 marzo 2008, n. 48) rinnovò profondamente il sistema prevedendo per i reati informatici la responsabilità dell'ente *ex* D. Lgs. 231/2001 (art. 24-*bis*) e interpolando molte disposizioni procedurali sulla competenza, sui poteri dell'Autorità giudiziaria e di polizia nella repressione dei crimini informatici e sulle modalità di conservazione della prova informatica (disposizioni c.d. di informatica forense).

La cooperazione intergovernativa ha avuto basi ancor più solide grazie al diritto del c.d. terzo pilastro della Comunità Europea. In particolare la Decisione Quadro 2005/222/GAI, adottata con il deliberato intento *"di*

[3] *Il futuro della Cybersecurity in Italia, ibidem*

migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione" (considerando n. 1), aveva gettato le basi per lo *standard* minimo di criminalizzazione in materia di criminalità informatica. Successivamente, abolita la struttura a pilastri con il Trattato di Lisbona, il referente normativo fondamentale della materia è divenuto l'art. 83 del TFUE che consente oggi di stabilire, mediante direttive adottate secondo la procedura legislativa ordinaria, *minimum rules* in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale, fra le quali rientra, appunto, la criminalità informatica.

Da ultimo la Direttiva 2013/40/UE ha modificato e ampliato le disposizioni contenute nella decisione quadro 2005/222/GAI, stabilendo norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione, con l'obiettivo di facilitare la prevenzione di tali reati e migliorare la cooperazione fra autorità giudiziarie e altre autorità competenti, compresi la polizia e i servizi degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e l'Agenzia per la sicurezza delle reti e dell'informazione (ENISA). La Direttiva, mantenendo ferme la maggior parte delle disposizioni contenute nella decisione quadro 2005/222/GAI, detta alcune norme integrative rispetto alla Convenzione di Budapest, che riconosce come *framework* fondamentale di lotta contro la criminalità informatica (considerando n. 15).

8. Uno sguardo al futuro: le sfide e le opportunità.

Credo non esista materia come quella del *cyber* in cui presente e futuro abbiano distanze così ravvicinate.

La velocità con cui i mezzi di comunicazione, le intelligenze artificiali, la robotica, l'*e-commerce* si sviluppano e si modificano è tale da imporre a noi tutti una visione *orwelliana* del mondo e dei modelli di sviluppo economico che verranno introdotti e che dovremo regolamentare.

Fantasia, inventiva e capacità di immaginazione dovranno entrare nel bagaglio culturale del giurista, creando una rivoluzione copernicana, da modello di analisi di ciò che è accaduto, a modello di previsione di ciò che potrà accadere, per essere pronti a regolamentarlo nel migliore dei modi.

Interdisciplinarietà, internazionalizzazione, cultura d'impresa dovranno poi connotare le nuove figure manageriali destinate ad assicurare un corretto uso del mezzo informatico e a tutelare la sicurezza di aziende, di istituzioni, di nazioni intere.

Fondere insieme cultura economica, giuridica, tecnica, ingegneristica, sociologica rappresenterà il compito di chi dovrà costruire una nuova classe dirigente, nel settore pubblico e nel settore privato, adeguata ad affrontare un fenomeno così prismatico.

Questa è la sfida cui dovranno rispondere i nostri imprenditori ma, prima ancora, le nostre Università, dimostrando che la tecnologica, e dunque il progresso, possono anche creare nuove opportunità.