media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 17/2016

ANNALISA REGI*

Crimini informatici: fino a che punto le PMI ne sono davvero consapevoli?

INDICE: 1. Premessa. – 2. La scarsa consapevolezza e percezione del fenomeno del *cyber crime* nelle PMI, "bersaglio" degli aggressori informatici. 3. Il vasto universo del *cyber crime*: le diverse tipologie di minacce, di attacco e di attaccanti. 4. Le vulnerabilità tecniche e umane che le PMI devono fronteggiare. 5. I rischi e i costi per le PMI derivanti dal fenomeno del *cyber crime*. 6. Considerazioni conclusive.

1. *Premessa.*

Come noto, negli ultimi anni si è assistito alla costante ascesa e alla rapida diffusione del fenomeno dei crimini informatici, che, rispetto al passato, si è notevolmente evoluto fino a diventare un'attività molto proficua per le organizzazioni criminali.

* Avvocato presso Jannuzzi & Regi, Milano

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

Occorre preliminarmente rappresentare che non esiste – a livello internazionale – una definizione giuridicamente condivisa dei predetti crimini; esemplificando, potremmo definire il *cyber crime* «*come l'insieme delle operazioni illegali che avvengono su internet*», atteso che la criminalità informatica «*non è da considerarsi un fenomeno alieno o differente dalla criminalità che siamo abituati ad affrontare, ma semplicemente il crimine perpetrato con altri mezzi, attraverso il cyber space*»[1].

Si tratta di una tipologia di atto criminoso molto più pericolosa di quella tradizionale, che amplifica le potenzialità e la pericolosità del soggetto criminale, non avendo la stessa confini fisici e potendo essere perpetrata da qualsiasi parte del mondo e senza alcun tipo di contatto umano[2].

È bene mettere in evidenza che il fenomeno del *cyber crime* riguarda non solo le grandi imprese, ma anche e soprattutto quelle di piccole e medie dimensioni, ragion per cui lo stesso costituisce un notevole rischio per l'Europa e per l'Italia, *in primis*, essendo le piccole e medie imprese (di seguito anche solo "PMI") il fulcro del tessuto economico e sociale europeo ed italiano[3].

Al fine di poter meglio comprendere siffatta ultima affermazione, basti pensare che le PMI rappresentano il 99,8% della totalità delle imprese nel territorio europeo, impiegando 86,8 milioni di persone (66,5% della forza lavoro) e producendo più della metà del fatturato totale delle imprese europee; occorre inoltre specificare che, delle oltre 20 milioni delle PMI

[1] F. ZAPPA, *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2014, 27 ottobre 2016, p. 19, http://www.unicri.it/.

[2] Per essere ancora più precisi, occorre mettere in evidenza che i criminali, diversamente da quello che è lo spazio *internet* per i normali utenti, sfruttano il c.d. *deep web*, ossia spazi che non risultano facilmente accessibili e che non si possono rintracciare attraverso i motori di ricerca (si tratta del *web* sommerso).

[3] EISAS – European Information Sharing and Alert System, A Feasibility Study 2006/2007, 27 ottobre 2016, www.enisa.europa.eu; F. ZAPPA, *op. cit.*, p. 13.

europee, il 92,1 % è costituito da micro-imprese che, sommate alle piccole, rappresentano oltre il 50% dei posti di lavoro per i cittadini europei[4].

Il nostro Paese, con il 99,9% della totalità delle imprese costituito da quelle di piccole e medie dimensioni, non è altro che la "patria" delle PMI, atteso che il 68% della ricchezza italiana è prodotto da quei 12 milioni di persone impiegate in una PMI (più in particolare, le micro-imprese italiane, che rappresentano il 94,4% del totale, hanno un peso del 46,1% in termini di occupazione).

Siffatte aziende sono per lo più familiari e risultano specializzate nel settore manifatturiero, tipico del Made in Italy, «*con oltre 200 distretti industriali, che spesso rappresentano l'eccellenza a livello mondiale*»[5].

2. *La scarsa consapevolezza e percezione del fenomeno del cyber crime nelle PMI, "bersaglio" degli aggressori informatici.*

Occorre sin da subito rilevare che il dilagare del fenomeno del *cyber crime* nell'ambito delle piccole e medie imprese si manifesta in un momento – quale quello attuale - particolarmente delicato, contraddistinto da una notevole tensione economica e finanziaria.

Siffatta situazione fa sì che le aziende siano costrette a fronteggiare misure di austerità e profitti non soddisfacenti, che non consentono loro di avere una disponibilità economica tale da consentirgli di poter investire in una politica di sicurezza informatica.

Nonostante il verificarsi dei crimini informatici implichi danni e perdite di gran lunga maggiori rispetto all'investimento iniziale necessario per contrastarli, spesso le imprese non sono in grado di sostenere i costi per la sicurezza informatica.

[4] *A recovery on the horizon? Annual Report on European SMEs 2012/2013*, European Commission, 27 ottobre 2016, www.ec.europa.eu; F. ZAPPA, *op. cit.*, p. 14.
[5] F. ZAPPA, *op. cit.*, p. 15.

È inoltre opportuno rilevare che l'attenzione in ambito di *cyber crime* è solitamente rivolta nei confronti di quei crimini che colpiscono le grandi aziende, che, a siffatto proposito, destinano consistenti budget nelle policy di difesa e tutela.

Ora, dal fatto che la predetta attenzione nei confronti delle PMI sia pressoché minima, ne deriva che nelle stesse si abbassino sia la percezione del rischio che «*il livello di guardia*»[6].

La scarsa consapevolezza della minaccia informatica nelle piccole e medie imprese comporta, a sua volta, che queste ultime siano diventate «*un bersaglio appetibile per gli aggressori informatici a causa delle loro protezioni deboli e insufficienti*»[7]; i predetti aggressori spostano infatti «*i loro tentativi di attacco verso le PMI come veicolo per colpire imprese più grandi e meglio difese*»[8].

Alla luce di quanto appena esposto, una PMI non deve commettere l'errore di considerarsi immune dal fenomeno del *cyber crime*[9], atteso che le dimensioni di un'azienda non rilevano assolutamente ai fini dell'appetibilità o meno della stessa per i criminali informatici[10].

---

[6] *Id.*, p. 16.
[7] *Ibid.*
[8] *Id.*, p. 17.
[9] Del resto, qualsiasi azienda è un bersaglio molto attraente per i *cyber* criminali; non importa infatti quale sia il *business* o il servizio offerto: informazioni, dati personali, indirizzi *e-mail*, *know-how*, dati sanitari sono vendibili al mercato nero per commettere frodi, per diffondere *malware* e per mettere in atto altri crimini. Ciò che i criminali informatici valutano prima di commettere un attacco è meramente la presenza di denaro o di dati importanti da rubare, come anche la facilità nel violare la sicurezza; F. BOSCO, *Ecco perché la* cybersecurity *è una leva potente per svecchiare le nostre PA e PMI*, Nazioni Unite per la Ricerca sul Crimine e la Giustizia, 27 ottobre 2016, www.forumpa.it.
[10] Al riguardo, è stato anche osservato che «*gli attacchi alle imprese di piccole e medie dimensioni sono estremamente ricorrenti poiché le loro protezioni tendono a essere meno sofisticate, rendendole facili prede*"; le stesse "*sono spesso prese di mira da coloro che vogliono rubare le informazioni bancarie dei clienti per poi ricattarli o usarli come "porta di servizio" per infiltrarsi in organizzazioni più grandi*»: così, W. ROSSI, Gruppo Daisy di consulenza IT, 27 ottobre 2016, https://h30657.www3.hp.com/t5/BusinessNow-it/PMI-italiane-e-sicurezza-informatica-a-che-punto-siamo/ba-p/6198.

3. *Il vasto universo del cyber crime: le diverse tipologie di minacce, di attacco e di attaccanti.*

L'universo del *cyber crime* è abbastanza vasto e comprende diverse tipologie di minacce, di attacco e di attaccanti.

Quanto alle minacce cui le PMI sono esposte, tra le più gravi vi è sicuramente il furto di dati sensibili e di proprietà intellettuale. È un dato incontrovertibile che per le aziende il know-how e la proprietà intellettuale costituiscono il bene più prezioso, un bene la cui perdita può avere un impatto fortissimo, per non dire determinante, sul business aziendale; si pensi a tutti quei beni immateriali (a titolo esemplificativo, le invenzioni industriali e i modelli di utilità, il design dei vari beni, i marchi, i progetti di architettura….) che sono il frutto e il risultato dell'inventiva dell'imprenditore e che risultano essenziali per la stessa esistenza dell'azienda; per quanto concerne poi il furto di dati sensibili, lo stesso riguarda sia i dati interni all'azienda, sia i dati dei clienti e dei fornitori.

Tra le minacce in cui le PMI possono incorrere vi sono inoltre: a) il furto di identità, posto in essere dal criminale che ruba l'identità di un soggetto interno all'azienda (al fine di ottenere informazioni da un ignaro collega) o dell'intera azienda (al fine di utilizzare queste risorse in maniera illecita in un paese straniero, producendo gli stessi beni commercializzati dall'impresa vittima e immettendoli sul mercato come merce contraffatta); b) la frode, ossia l'accesso, senza permesso, a sistemi informatici con il solo obiettivo di ottenere gratuitamente e in maniera illecita i servizi erogati dall'azienda vittima; c) il sabotaggio, avente lo scopo di rallentare o bloccare le attività della vittima tramite l'intralcio delle normali operazioni; d) lo spionaggio, al cui fondamento vi è la finalità di ottenere in maniera illecita informazioni aziendali e commerciali; e) gli attacchi dimostrativi, causati da singoli o gruppi di persone, quali atti di protesta nei confronti dell'azienda vittima, cui viene imputata una condotta scorretta nei confronti degli utenti finali o dei privati cittadini; f) l'estorsione, nel momento in cui il criminale installa illegalmente sul computer della vittima – senza ovviamente

l'autorizzazione di quest'ultima – un software (tale installazione si perfeziona di solito tramite il click su link fraudolenti, trasmessi tramite posta elettronica, o sui social network, a causa di una navigazione non prudente). Attraverso il predetto software, il computer della vittima viene bloccato da remoto o ne vengono criptati i dati, non consentendone l'utilizzo e la vittima deve corrispondere una somma di denaro per sbloccare il computer o decriptarne i dati[11].

Per quanto concerne invece i diversi tipi di cyber attacco che le PMI possono subire, è opportuno rammentare: a) il *phishing*, «*un tentativo di truffa via internet attraverso il quale il malintenzionato cerca di convincere con l'inganno la vittima del raggiro a fornire dati personali sensibili, spesso attraverso l'invio di e-mail che simulano la grafica di siti postali o bancari, richiedendo le credenziali di accesso o il numero della carta di credito, per evitare l'incorrere in possibili problemi o sanzioni*». All'interno della predetta e-mail, è presente un link che la vittima, per risolvere il problema, dovrebbe cliccare; peccato che la vittima acceda purtroppo a un sito falso, in cui inserisce i propri dati personali, consegnandoli così - inconsapevolmente – al criminale; b) lo *spear phishing*, il quale si differenzia dal *phishing* solo per il fatto di non inviare mail casualmente, ma di selezionare in maniera oculata le proprie vittime; c) il *pharming*, che differisce dal *phishing* soltanto perché non richiede una condotta posta in essere dalla vittima, riuscendo – tramite tecniche di intrusione ai danni dell'utente o dell'*internet service provider* – a indirizzarla su un sito controllato dal criminale stesso; d) *l'hacking*, cioè la condotta consistente nell'accesso illecito ad un sistema, al fine di entrare in possesso di informazioni sullo stesso e sul suo funzionamento, nonché dei dati contenuti; e) lo *spam*, vale a dire l'invio tramite e-mail di messaggi indesiderati, a scopo di pubblicità e vendita di materiale illecito/illegale, fino ad arrivare a tentativi di truffa; f) il *malware* ("software dannoso"), espressione utilizzata per ricomprendere l'insieme di tutte le minacce software che possono colpire un computer (a titolo esemplificativo e non esaustivo: *virus*, *trojan*, *worm*…); g) il c.d. attacco *Denial of Service*, ossia un attacco effettuato da un soggetto

[11] F. ZAPPA, *op. cit.*, pp. 25-27.

criminale nei confronti di un sistema informatico o di un sito web, al fine di negare il servizio fornito dal sistema o dal sito attaccato[12].

Quanto agli attaccanti, occorre mettere in evidenza che il gruppo criminale organizzato e gli insider (singoli dipendenti o ex dipendenti) rappresentano per le piccole e medie imprese italiane i profili più minacciosi, soprattutto in considerazione del fatto che il furto della proprietà intellettuale può sicuramente mettere in pericolo il Made in Italy e la produzione di prodotti per eccellenza.

4. *Le vulnerabilità tecniche e umane che le PMI devono fronteggiare.*

È opportuno poi rilevare come ciascuna impresa debba fare i conti con una serie di vulnerabilità, sia tecniche, che umane, che potrebbero essere fronteggiate con un'adeguata preparazione dei responsabili tecnici e una buona conoscenza delle best practices da parte dei vari utenti.

Tra le vulnerabilità tecniche, il primo fattore di rischio è costituito «*dall'esposizione dei dispositivi on-line, dalla tipologia di connessione utilizzata e dalle connessioni in generale*»[13]; del resto, la disponibilità pressoché costante di internet, attraverso reti wireless spesso non protette o protette non adeguatamente, con password di default, senza un'opportuna configurazione degli apparecchi e della rete interna e con l'utilizzo di protocolli non sicuri, rappresenta sicuramente un elemento di notevole pericolosità.

Per non parlare poi della pratica del c.d. *cloud computing*, che consente mediante la connessione a internet sia di avere a disposizione i propri dati e i propri file e di condividerli attraverso più piattaforme, sia di sfruttare applicazioni basate su linguaggi web in condivisione con altre persone.

[12] *Id.*, pp. 30-35.
[13] *Id.*, p. 38.

Altro fattore di rischio è rappresentato dall'incremento dell'utilizzo di dispositivi mobili, quali smartphone e tablet, Smart TV, le cui vendite hanno ampiamente superato quelle dei computer fissi e dei classici portatili. L'uso di siffatti dispositivi mobili, sia aziendali che personali, richiederebbe l'imposizione di alcune "regole", volte a scongiurare che i dati sensibili vengano memorizzati su di essi con estrema superficialità e senza alcun sistema di protezione e sicurezza, che non vengano effettuati aggiornamenti, che non vengano installati antivirus e anti *malware* e che non venga attivato un collegamento a una rete wireless libera e gratuita (messa a disposizione dalle attività commerciali).

Per quanto attiene alle vulnerabilità umane, le stesse potrebbero essere arginate grazie a un uso adeguato e consapevole dei social network e dei dispositivi mobili; questi ultimi, in particolare, vengono utilizzati con superficialità tutte le volte in cui si aprono e-mail da mittenti sconosciuti o si scarica un software "pirata" non sicuro. Occorre poi rilevare che il rischio più elevato che deriva dai social network non è frutto di errori di programmazione delle piattaforme usate, bensì dell'erroneo uso di siffatti strumenti e di «*applicazioni malevole e plug-in esterni collegati ad essi e realizzati da cyber criminali, che reindirizzano gli utenti su siti malevoli o link fraudolenti, ingannandoli pubblicizzando e invitando a cliccare su false applicazioni che riguardano giochi o video virali, piuttosto che la possibilità di sapere chi ha visitato il proprio profilo o di cambiare il colore del template*»[14].

Non si può non comprendere come i criminali informatici "approfittino" delle predette vulnerabilità, sia tecniche, che umane, "sfruttando" le carenze presenti nell'ambito della sicurezza informatica aziendale e della sicurezza dei sistemi e delle reti informatiche in genere[15].

5. *I rischi e i costi per le PMI derivanti dal fenomeno del cyber crime*

[14] *Id.*, pp. 44-45.

[15] Cyber crime *e* security*: i costi del crimine informatico per le aziende*, 27 ottobre 2016, https://www.maticmind.it/.

Dal vasto universo di minacce, di attacco e di attaccanti in ambito di *cyber crime* derivano per le PMI numerosi rischi, che sono anche dovuti alle predette vulnerabilità tecniche e umane.

Siffatti rischi possono incidere su diversi aspetti della "vita aziendale", relativi sia ai profili strettamente connessi agli strumenti informatici, sia ai profili connessi al business e ai beni aziendali più importanti, ossia «*i dati, le persone e i servizi*»[16].

In primis, occorre rilevare che la perdita dei dati o della loro integrità può tradursi sia in una mera perdita economica diretta (mediante furto di denaro da conto corrente o carta di credito, «*perdita di credenziali, spam, o estorsione e truffa*»), sia nella perdita della proprietà intellettuale (a titolo esemplificativo, brevetti) e del know-how, sia in un danno di immagine e reputazionale, che implica, a sua volta, la perdita di credibilità sul mercato.

Del resto, nel contesto attuale l'informazione ha spesso il medesimo valore economico del denaro e può tradursi in «*database clienti, dati finanziari aziendali, dettagli finanziari di clienti e fornitori, informazioni sui prezzi, progetti di prodotti o processi di produzione*».

Ora siffatto rischio non è assolutamente da sottovalutare per le PMI, potendo creare danni difficilmente risanabili, danni che possono avere un considerevole impatto in termini di posti di lavoro ed economia locale e che possono "mettere in ginocchio" l'impresa medesima. In particolare, la perdita dei dati o il furto della proprietà intellettuale possono risultare fatali per aziende che fondano il proprio core-business sulla qualità e sulla segretezza della propria produzione, spesso di un unico bene, essendo l'appetibilità del Made in Italy tale grazie ai modelli, ai brevetti, ai progetti, alle invenzioni, al know-how stessi.

La seconda tipologia di danni in ambito di *cyber crime* che le piccole e medie imprese possono subire concerne i c.d. "danni ad impatto fisico", ossia quei crimini che colpiscono l'integrità della rete aziendale, dei macchinari, dei sistemi e degli strumenti di controllo,

[16] F. ZAPPA, *op. cit.*, p. 37.

«rallentando o bloccando di fatto la produzione e danneggiando il business aziendale o impedendo l'accesso al web e a tutti i sistemi informatici aziendali».

La terza e ultima tipologia di danni concerne i c.d. "danni ad impatto sui servizi forniti o utilizzati da un'azienda", che possono incidere sulla qualità del bene prodotto o sulla sicurezza dei dipendenti o degli utenti[17].

A fronte delle predette tre tipologie di rischi, occorre mettere in evidenza che, a causa del verificarsi degli stessi, le imprese devono sostenere numerosi costi, che vanno dagli indennizzi da corrispondere ai clienti in caso di violazione dei dati ad essi relativi, «*ai costi in contromisure e assicurazioni*[18]*, ai costi per l'implementazione di strategie di mitigazione dei rischi e di recovery in caso d'incidente*»[19].

Per non parlare poi dell'investimento economico e di tempo per ripristinare la rete aziendale, i macchinari, gli strumenti di controllo, i sistemi e i servizi e dei costi inerenti la pulizia del *malware*, la ricerca investigativa e la gestione post-incidente[20].

Quanto alle assicurazioni, è opportuno rappresentare che le stesse costituiscono "uno scudo efficace" contro gli attacchi informatici.

Le compagnie assicurative propongono polizze che, oltre a coprire eventi criminali pressoché comuni, quali la violazione di dati aziendali e personali, prevedono coperture sul furto di proprietà intellettuale, sulle estorsioni e sulle interruzioni di attività.

Considerata la difficoltà di poter beneficiare di una protezione assoluta, risultano assolutamente interessanti quelle soluzioni assicurative che proteggono dalle conseguenze

---

[17] In relazione alle tre tipologie di danni, F. ZAPPA, *op. cit.*, p. 37

[18] In riferimento alle assicurazioni, si precisa che la tendenza delle piccole e medie imprese a dotarsi di polizze assicurative contro il crimine informatico è aumentata notevolmente nel corso del 2015, salendo di 9 punti percentuali rispetto all'anno precedente e del 26% rispetto al 2011: sul punto, si vedano le considerazioni di A. ARGENTIERI, *Le piccole e medie imprese e i rischi del* cybercrime, 27 ottobre 2016, http://www.europeanpensions.net/it/Le-piccole-e-medie-imprese-e-i-rischi-del-cybercrime.php.

[19] Cfr. F. ZAPPA, *op. cit.*, p. 17.

[20] Cyber crime *e* security*: i costi del crimine informatico per le aziende*, 27 ottobre 2016, https://www.maticmind.it/.

economiche e riorganizzative dell'avvenuto attacco informatico, dalle perdite di introito alla perdita di reputazione, garantendo un'assistenza post-attacco, al fine di consentire all'azienda di fronteggiare tale attacco[21].

Tanto premesso e rappresentato, è opportuno riflettere sui risultati emersi nel mese di settembre 2016 dalla quarta edizione dell'indagine internazionale effettuata da GfK Eurisko, su commissione di Zurich Insurance Group, sui rischi derivanti dai crimini informatici su un campione di oltre 2.600 PMI[22] in tredici Paesi del mondo[23].

Dalla predetta ricerca risulta che le piccole e medie imprese italiane hanno mostrato una consapevolezza crescente del fenomeno del *cyber crime* negli ultimi quattro anni. In particolare, la percezione del rischio legato a siffatti crimini è cresciuta sensibilmente, passando dallo 0,8% al 10%, mentre il timore di attacchi alle reti informatiche è aumentato dal 3,2% al 14%.

Ne deriva che il numero assoluto di PMI che teme gli attacchi informatici, pur in forte crescita, rimane ancora molto basso[24].

---

[21] In particolare, tra le soluzioni proposte dalle compagnie assicurative possiamo annoverare: i) il servizio c.d. di "*flooding*", che prevede l'intervento della compagnia nell'ipotesi di un'illegittima lesione della reputazione dell'assicurato (via *web*); tale servizio offre la messa in circolazione nel *web* di contenuti, messaggi e notizie che riportino le informazioni corrette e veritiere sul conto del soggetto leso alle prime pagine dei motori di ricerca; ii) per i servizi in *cloud* sono stati sviluppati prodotti specifici, rivolti sia agli utenti del servizio *cloud*, sia agli stessi fornitori; tali polizze coprono i danni da incendio, l'interruzione di esercizio, i danni alla proprietà intellettuale, alla *privacy* e alla reputazione; iii) soluzioni ibride, che coprono l'esposizione verso i terzi e verso la controparte contrattuale, in termini di costi per monitoraggio e interruzione del servizio, tutela legale specialistica, spese perizie tecniche e supporto IT: M. DETTORI, *I crimini informatici e la risposta delle assicurazioni*, 27 ottobre 2016, www.filodiritto.com.

[22] E' importante rilevare che, delle oltre 2.600 PMI, oltre 250 sono PMI italiane; *PMI, non sottovalutate i pericoli del* Cybercrime!, 27 ottobre 2016, http://www.igsconnect.com/pmi-non-sottovalutate-pericoli-del-cybercrime/.

[23] Risultati della quarta edizione del sondaggio internazionale di Zurich Insurance Group, 27 settembre 2016, http://www.zurich.it/stampa-media/comunicati-stampa/SMEsurvey2016.htm.

[24] Sul punto, si vedano: Cybercrime *e attacchi informatici, solo una PMI italiana su dieci è consapevole dei rischi*, 27 ottobre 2016, https://www.digital4.biz/pmi/approfondimenti/cybercrime-e-attacchi-informatici-solo-una-pmi-italiana-su-10-e-consapevole-dei-rischi_43672159128.htm; Cybercrime *in*

Tali dati riflettono lo scenario registrato dal Clusit, secondo cui il *cyber crime* è cresciuto del 30% nell'ultimo anno e sono aumentati del 39% gli attacchi con finalità di spionaggio informatico; il numero di attacchi registrato è infatti il più alto dell'ultimo quinquennio, con circa 1.012 nel 2015 (contro gli 873 del 2014)[25].

Sulla base di siffatti dati, è stato osservato che «*ogni azienda, indipendentemente dalle dimensioni, è soggetta al rischio cyber*[26] *- qualsiasi processo produttivo è gestito e controllato attraverso sistemi informatici - e un attacco potrebbe determinare un'interruzione dell'attività, con gravi conseguenze in termini di perdita di profitto. E anche se negli ultimi anni le imprese stanno diventando più attente ai rischi informatici e più consapevoli degli impatti negativi di una cattiva gestione della sicurezza informatica, la strada è ancora lunga. Con il recepimento del Regolamento Europeo sulla protezione dei dati (…) da parte degli Stati UE entro il 2018 ed uno scenario caratterizzato da un forte aumento di minacce cyber in Italia nell'ultimo anno, la grande sfida con cui le aziende dovranno confrontarsi riguarderà innanzitutto l'implementazione di piani sempre più efficienti ed efficaci per la sicurezza delle reti e la salvaguardia dei dati*»[27].

6. *Considerazioni conclusive.*

Alla luce di quanto sopra esposto e rappresentato, emerge come nel momento attuale, contraddistinto da una notevole tensione finanziaria e economica, le piccole e medie imprese

---

Italia: le PMI non lo temono ancora abbastanza, 27 ottobre 2016, http://blog.comunicaredigitale.com/cybercrime-italia-pmi/.

[25] Dati Clusit 2015.

[26] A proposito del fatto che ogni azienda, indipendentemente dalle dimensioni, sia soggetta al rischio cyber, è stato osservato che: «è l*a convinzione, manifestata da molte pmi, che le dimensioni ridotte le mettano al riparo da potenziali minacce digitali e dai rischi di subire un* cyber attack *manca di fondamento e può indurre a concezioni e assunzioni sbagliate*»: L. BAILEY, 27 ottobre 2016, http://www.europeanpensions.net/it/Le-piccole-e-medie-imprese-e-i-rischi-del-cybercrime.php.

[27] Così, A. ZAMPINI, 27 ottobre 2016, http://www.zurich.it/stampa-media/comunicati-stampa/SMEsurvey2016.htm.

non abbiano una disponibilità economica tale da consentirgli di poter investire in una politica di sicurezza informatica.

Ora, poiché le PMI italiane possono rivestire un ruolo chiave per la ripresa economica del nostro Paese, è indispensabile che le stesse – con il supporto e l'ausilio sia degli organi interni che europei – definiscano delle politiche volte a migliorare le proprie condizioni di crescita e a supportare la predetta ripresa.

In siffatto contesto, non vi è chi non comprenda come, accanto alle tradizionali politiche di sostegno, riguardanti, tra l'altro, le condizioni di acceso ai finanziamenti e il mercato del lavoro, assuma un ruolo primario lo sviluppo di determinati progetti in ambito tecnologico, sviluppo che richiede, a sua volta, la definizione di una politica di difesa e di tutela nei confronti del *cyber crime*.

In altri termini, è importante investire «*nell'opera di digitalizzazione delle PMI italiane per sostenerne l'internalizzazione*" [28] *e promuovere l'e-commerce; del resto, un'azienda dotata di infrastrutture moderne e di settori tecnologicamente avanzati risulta maggiormente competitiva e in grado di recuperare in maniera nettamente più rapida i rendimenti precedenti al periodo di recessione.*

Al fine di poter attuare siffatta digitalizzazione, occorre tuttavia proteggere le PMI dalle minacce, dagli attacchi e dai rischi connessi al vasto universo di internet, mettendo a punto una strategia di difesa efficace e efficiente, una policy che promuova una cultura della sicurezza su vari livelli, atteso che "la consapevolezza del rischio è la migliore arma di prevenzione»[29].

La sicurezza non deve essere concepita solo come un costo, quanto come un valore e un investimento[30], posto che la lotta al *cyber crime* assicura alle aziende un vantaggio in termini di competitività, considerato che un attacco a danno di una PMI non è altro che un attacco alla nostra economia.

---

[28] F. ZAPPA, *op. cit.*, p. 70.
[29] *PMI, non sottovalutate i pericoli del* Cybercrime!, 27 ottobre 2016, http://www.igsconnect.com/pmi-non-sottovalutate-pericoli-del-cybercrime/.
[30] F. ZAPPA, *op. cit.*, p. 109.

Alla base di un'efficace ed efficiente strategia di difesa e di contrasto ai crimini informatici, vi è senza dubbio la necessità di investire nella prevenzione e nella formazione, accanto all'esigenza di superare tutte quelle "barriere culturali" che non consentono un approccio consapevole nei confronti dei rischi e dei danni dei predetti crimini[31].

Occorre cioè sviluppare una buona policy interna all'azienda, finalizzata ad "informare" del pericolo rappresentato dal fenomeno del *cyber crime* e a "formare" non solo i reparti IT, ma anche i titolari di aziende, il Consiglio di Amministrazione, i dirigenti/i responsabili, i consulenti e tutti i dipendenti, per poter attuare contromisure e strategie concertate[32].

Essendo da un lato la formazione del management delle PMI la prima arma di difesa nei confronti dei crimini informatici ed essendo dall'altro «*il livello di maturità del risk management di una industria (…) direttamente proporzionale alle sue dimensioni*», emerge come – con particolare riferimento alle PMI – sia assolutamente «*necessaria ed urgente l'implementazione di piani di formazione sulle minacce cyber*»[33].

Ciò risulta ancora più necessario se solo si consideri che «*più è piccola la dimensione dell'impresa, minore è anche la sua capacità di identificare un attacco subito rispetto ad una impresa di maggiori dimensioni, per mancanza di reparti tecnici specializzati o semplicemente perché meno abituata a considerare la minaccia*»[34].

Insomma, è auspicale promuovere una corretta informazione, atteso che la migliore difesa inizia proprio con l'educazione del personale; linee guida di sicurezza[35] definite chiaramente

---

[31] F. BOSCO, *La criminalità informatica e le PMI*, 27 ottobre 2016, http://www.tecnaeditrice.com/articoli/ict_security/la_criminalit_informatica_e_le_pmi.

[32] Al riguardo, è stato osservato che «*il mantenimento della sicurezza di base non è più sufficiente a proteggere l'attività delle PMI. Avere soltanto un programma* antivirus *in esecuzione senza crittografare i dati sensibili è come chiudere a chiave la porta d'ingresso lasciando spalancata la finestra al piano terra*»: C. SISTO, *PMI italiane e sicurezza informatica: a che punto siamo?*, 27 ottobre 2016, https://h30657.www3.hp.com/t5/BusinessNow-it/PMI-italiane-e-sicurezza-informatica-a-che-punto-siamo/ba-p/6198.

[33] F. ZAPPA, *op. cit.*, p. 29.

[34] *Id.*, p. 30.

[35] In relazione alle modalità di realizzazione delle linee guida, F. BOSCO, *op. cit.*

e di immediata comprensione «*non trasformeranno tutti i dipendenti in esperti IT, ma potranno fare la differenza tra qualcuno che risponde a un attacco di phishing e qualcuno che ignora l'e-mail*»[36].

In particolare, «*i leader aziendali devono farsi avanti ed essere pronti a sostenere reti e dispositivi contro la minaccia della criminalità informatica, dall'istituzione di team di risposta agli attacchi informatici all'assicurazione che i sistemi IT e le reti siano sempre dotati di patch e protezione. Tutto ciò deve rappresentare la nuova normalità*»[37].

E' inoltre auspicale che tra imprese affini per settore o per dimensione si instauri un dialogo, un rapporto di collaborazione e di condivisione, volto a diffondere contromisure, politiche concertate e best practices messe a punto nella lotta e nel contrasto al fenomeno dei crimini informatici.

Da ultimo, occorre mettere in evidenza come nel 2013 l'Unione Europea abbia adottato una strategia cibernetica, invitando gli Stati membri a fare altrettanto e come nel 2014 anche l'Italia si sia a sua volta dotata di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico. La lotta e il contrasto ai crimini informatici necessita, tuttavia, non solo di azioni legislative incisive, ma anche di azioni da parte delle forze dell'ordine, delle associazioni di categoria, delle università, degli esperti legali e delle aziende.

Sulla base di quanto appena esposto, al fine di contrastare i predetti crimini, è stato suggerito un percorso basato sullo sviluppo di due progetti complementari, volti a creare network promotori di una cultura della sicurezza e garanti del costante aggiornamento delle buone prassi, delle contromisure e delle politiche concertate[38]. Nello specifico, il primo si prefigge di incrementare la conoscenza e la condivisione di informazioni su diversi livelli aziendali e concerne l'organizzazione di seminari, workshop e corsi di formazione differenziati per tutti gli attori diversamente coinvolti nel sistema produttivo; il secondo prevede la realizzazione di tavole rotonde tra figure professionali differenti, quali i

[36] C. SISTO, *op. cit.*
[37] *Ibid*.
[38] 27 ottobre 2016, http://www.pmi.it/tecnologia/infrastrutture-it/approfondimenti/96670/cybercrime-nele-pmi-rischi-soluzioni.html.

rappresentanti delle piccole e medie imprese nel settore merceologico, le forze dell'ordine, le associazioni di categoria, le università e gli esperti legali[39].

In estrema sintesi: la sicurezza aziendale può progredire e "offrire" una difesa nella lotta al *cyber crime* soltanto attraverso la promozione di una cultura della sicurezza su vari livelli, l'educazione del personale, una tecnologia innovativa, la cooperazione e la libera condivisione delle conoscenze; è dunque necessaria una «*combinazione di persone, tecnologia e criteri per erigere un fronte comune, contro i crimini informatici*»[40].

[39] F. BOSCO, *op. cit*.
[40] C. SISTO, *op. cit.*