ItaliaOggi Sette

diffusione:88589
tiratura:133263

Affari Legali

*Cyber security, la prevenzione passa dai legali*

da pag. 23

*La sicurezza informatica sta diventando una delle attività più richieste agli studi*

# Le cyber-sfide dei legali

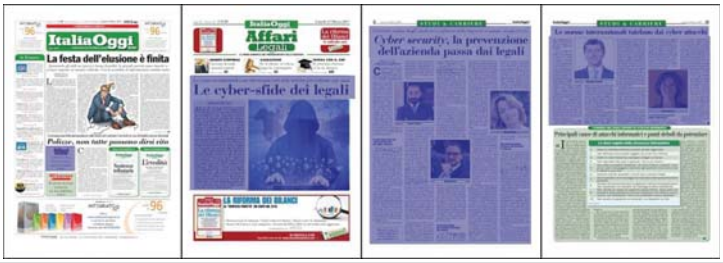
DI ROBERTO MILIACCA

***Allarme cyber-security in Italia. Secondo il Rapporto Clusit 2016, curato dall'Associazione Italiana per la Sicurezza Informatica (tra pochi giorni andrà alle stampe il rapporto 2017), il Belpaese è tra i primi dieci paesi al mondo nella classifica degli obiettivi di cyber-crime. La situazione della sicurezza informatica del paese non è delle migliori, soprattutto perchè sotto attacco non sono solo le grandi imprese o le istituzioni pubbliche, ma anche le aziende di medie e piccole dimensioni. Secondo l'Italian CyberSecurity Report 2016, realizzato dal Cis-Sapienza e dal Laboratorio Nazionale di CyberSecurity, è proprio contro le pmi che si sta concentrando la maggior parte delle aggressioni informatiche illecite di questi ultimi tempi, cioè dove sono più bassi i livelli di consapevolezza del rischio, di capacità di reazione, di aggiornamento e formazione del personale. Questa settimana su Affari Legali abbiamo voluto affrontare il tema, interpellando alcuni tra gli studi che si sono specializzati nella lotta al cyber-crime, forti anche delle normative che, a livello nazionale e internazionale, consentono loro di svolgere, al fianco delle imprese, un'attività di prevenzione dei crimini informatici. Poche settimane fa il governo ha aggiornato il Dpcm sulla sicurezza informatica del paese, cercando di razionalizzare e aggiornare il precedente decreto Monti sulle operatività delle strutture istituzionali predisposte alla vigilanza sul cyber-crime. Il nuovo decreto si integra con le recenti disposizioni comunitarie (la direttiva Network and information security) elaborata proprio per rendere più sicuro lo spazio informatico europeo. Insomma, tempo di nuove sfide, sia per le aziende che per i professionisti.***

Giuseppe Vaciago

Rocco Panetta

Stefano Mele



ItaliaOggi Sette



*L'attività svolta dagli studi nei confronti delle imprese si muove su più fronti*

# *Cyber security*, la prevenzione dell'azienda passa dai legali

*Pagine a cura di* MARIA CHIARA FURLÒ

Crimini che passano per il web, cyber spionaggio e attacchi informatici per sottrarre email, documenti e altri file a personalità più o meno note, imprese e governi. Un tema tornato alla ribalta dopo l'inchiesta della procura di Roma che ha portato all'arresto dei due fratelli, Giulio e Francesca Maria Occhionero, ritenuti responsabili di un'ampia attività di cyber spionaggio a scapito di numerose persone legate alle istituzioni, alla politica e alla finanza. In quest'ambito il lavoro di un avvocato specializzato può essere preziosissimo, soprattutto in fase di prevenzione da possibili attacchi.

## Il ruolo degli avvocati nella prevenzione dei cyber attacchi

È capitato diverse volte a **Rocco Panetta**, partner dello studio legale ***Nctm*** ed esperto di internet e nuove tecnologie, di doversi occupare di consulenze alle aziende in ambito di attacchi informatici, «è il nostro lavoro quotidiano. Noi lavoriamo sia in sede preventiva, aiutando aziende e P.a. a pianificare nel tempo e con calma la compliance sull'uso dei dati (la c.d. privacy) e sulla loro sicurezza, soprattutto, sia in caso di incidenti, di violazioni interne ed esterne di dati (c.d. data breach)».

Come spiega il professionista, in questi casi, il presidio «deve essere senz'altro informatico, ma non si può prescindere dalla piena comprensione della complessità giudico legale del fenomeno, se non altro al fine di evitare, prevenire e rimediare al rischio di sanzioni e di richieste di risarcimento danni. In questo gli avvocati specializzati nell'ambito della privacy possono fare la differenza».

Da quando tutte le comunicazioni e i documenti di una società sono stati completamente digitalizzati, lo spionaggio informatico ha cominciato a rappresentare uno dei principali rischi da affrontare e mitigare ogni giorno.

In quest'ottica, il ruolo di consulenza da parte di un avvocato specializzato in Diritto delle Tecnologie, Privacy e Cyber Security «risulta fondamentale sia a seguito di un attacco informatico subìto, che soprattutto in via preventiva, per evitare a monte che simili comportamenti possano essere messi in atto, oppure per essere pronti da un punto di vista legale e procedurale a reagire in maniera efficace nel caso si verifichino», conferma **Stefano Mele** (nel 2014 inserito dalla Nato nella lista dei suoi «Key Opinion Leaders for Cyberspace Security») di ***Carnelutti Studio Legale Associato***. Secondo l'esperto, peraltro, il rischio non giunge soltanto dall'esterno, attraverso Internet o i malware allegati alle email, ma anche e sempre più spesso dall'interno della struttura, attraverso l'azione, ad esempio, di dipendenti in procinto di cambiare azienda, oppure scontenti, infedeli o addirittura pagati da concorrenti perché capaci di avere un accesso privilegiato e consapevole alle informazioni vitali della società da spiare.

Ecco perché svolgere consulenza legale in questo specifico settore, quindi, «è da tempo un'attività quasi giornaliera, che mira ad affiancare il top management e i responsabili della Corporate Security e dell'IT in queste delicatissime attività pre o post incidente informatico», aggiunge Mele.

*Supplemento a cura di* ROBERTO MILIACCA
*rmiliacca@class.it*
*e* GIANNI MACHEDA
*gmacheda@class.it*

Occupandosi da molti anni di cybercrime, anche a **Caterina Flick** dello studio ***Nunziante Magrone*** è capitato di offrire consulenza in questo ambito. «L'avvocato penalista può aiutare in due modi», spiega la professionista, riferendosi nel primo caso all'intervento riparatorio, dopo che l'attacco è avvenuto, «si interviene con le indagini difensive e con l'attivazione di procedimenti giudiziari per i reati informatici subiti o con la difesa nei procedimenti giudiziari che coinvolgono il cliente».

Il secondo modo «è l'intervento preventivo, con l'individuazione e corretta qualificazione dei rischi che corre il cliente e la predisposizione degli interventi per la messa in sicurezza dei sistemi informatici e dell'organizzazione». Questo tipo di consulenza, continua Flick, è richiesta dalle aziende consapevoli del fatto che la cybersecurity è utile per diversi obiettivi, tutti rilevanti anche economicamente, in particolare: proteggere know how, brevetti, segreti industriali, tutelare i dati personali trattati, prevenire reati informatici che potrebbero comportare gravi conseguenze per l'azienda. «In ogni caso in questo settore questioni tecniche e giuridiche sono strettamente collegate, per cui per offrire una consulenza legale seria è necessario avvalersi del supporto di tecnici competenti», aggiunge l'avvocato.

## Come funzionano gli attacchi informatici più comuni

Anche a **Giuseppe Vaciago**, partner di ***R&P Legal*** è capitato sia di assistere numerose società vittime di attacchi informatici che di fornire consulenza in materia di sicurezza informati-

ItaliaOggi Sette

diffusione:88589
tiratura:133263

ca. «Nel caso degli attacchi, il maggior numero di casi è la cosiddetta Bec (*Business Email Compromise*)» dice Vaciago spiegandone il funzionamento: «i dipendenti di un'azienda ricevono una mail fraudolenta, che finge di essere stata inviata da persone o enti di cui si fidano, e che invece è mandata dai truffatori. Nella mail c'è un link o un allegato, seguendo il primo o aprendo il secondo il destinatario viene infettato. Questa è la prima fase, un attacco detto di *phishing*, in cui si cerca di ingannare un utente con email fasulle per infettarlo o rubargli delle credenziali.

A quel punto inizia la fase due. I truffatori hanno accesso al pc e/o alla mail del dipendente. Iniziano a spiarne le comunicazioni interne ed esterne, individuano i responsabili commerciali, i creditori e debitori. Si fanno un quadro della situazione e quindi arrivano alla fase tre. Simulano, con una finta email, di essere un fornitore dell'azienda cui deve essere fatto un pagamento e spiegano che per qualche motivo hanno cambiato Iban. Il nuovo codice in realtà corrisponde a un conto aperto su una banca estera da un membro dell'organizzazione criminale».

Purtroppo, aggiunge Vaciago, è quasi impossibile identificare il cybercriminale perché sono organizzazioni complesse e sono in grado di rendersi completamente anonime. L'intervento di un avvocato esperto del settore è, quindi, «volto principalmente a chiarire le modalità tecniche utilizzate per commettere l'illecito al fine di predisporre un eventuale esposto o denuncia. Tale attività è utile per gestire l'inevitabile contenzioso che si genera in seguito alla truffa tra le due società». Un altro tipo di attacco che le aziende subiscono spesso è quello del ransonware. Come spiega il partner di R&P Legal, si tratta di un malware – tecnicamente «trojan» – che viene utilizzato dai cyber-criminali per bloccare i documenti contenuti sui sistemi infettati e per chiedere un riscatto, in genere in bitcoin. Dopo essere stato contagiato dal cryptovirus, il computer continua a funzionare ma foto, filmati, musica e scritti della vittima vengono protetti tramite algoritmi di cifratura. Al pagamento del riscatto, i criminali in genere sbloccano la protezione dai documenti e rimuovono il criptovirus.

## Strumenti normativi e tecnici che tutelano le imprese

Questi casi sono infatti sempre più frequenti per via dell'evoluzione tecnologica e del fatto che molte aziende non si preoccupano di tutelarsi contro le intrusioni. La normativa vigente, infatti, spiega **Elena Martini** dello studio ***Martini Manna*** «prevede espressamente la tutela delle informazioni riservate sia nell'ambito del codice della proprietà industriale, sia nel codice civile laddove questo sanziona la concorrenza sleale, sia nel codice penale con le norme a tutela dei segreti.

Tuttavia la tutela - in particolare quella da codice della proprietà industriale - è subordinata al fatto che il soggetto che la richiede abbia per primo protetto le proprie informazioni riservate con misure sia tecniche che giuridiche adeguate». Si tratta quindi innanzitutto, da un punto di vista tecnico, continua la professionista, di porre in essere misure in linea con il progresso tecnologico, per bloccare intrusioni e copie non autorizzate.

Dal punto di vista giuridico, invece, è necessario adottare «strumenti che indichino chiaramente la titolarità e la riservatezza delle informazioni: *non-disclosure agreement* («*Nda*»), policy interne, disclai-

Caterina Flick

Elena Manna

ItaliaOggi Sette



# Le norme internazionali tutelano dai cyber attacchi

mer sui documenti e sulle email con cui questi vengono trasmessi», aggiunge Martini.

Gli strumenti normativi per tutelare le imprese e i privati in caso di cyber attacchi «esistono e derivano principalmente dall'attuazione di norme internazionali». A farlo notare è Caterina Flick che prende ad esempio la Convenzione sul cybercrime, firmata a Budapest nel 2001, «che in Italia è stata attuata con la legge 48/2008, e che è stata ratificata ed entrata in vigore in quasi tutti i paesi membri del Consiglio d'Europa e in importanti paesi terzi (tra gli altri: Usa, Australia, Israele ...)», spiega la professionista che cita poi anche il recente regolamento europeo sulla protezione dei dati personali, che – «pur essendo focalizzato su altri aspetti – interviene comunque anche sul trattamento dati che avviene online e impone l'adozione di misure di sicurezza».

Secondo Flick però le difficoltà maggiori nel perseguire legalmente crimini informatici stanno però nel fatto che spesso gli attacchi partono da paesi «pirata», che non hanno adottato le regole condivise dagli altri paesi, e nei quali è difficile agire. «La difesa migliore rimane quindi l'adozione di misure di sicurezza informatica adeguate e il loro continuo aggiornamento», conclude l'avvocato di Nunziante Magrone.

La strumentazione giuridica che tutela da questi episodi «c'è ed esiste sin dal 1996, anno in cui è entrata in vigore la prima legge sulla privacy», afferma Rocco Panetta spiegando poi che negli anni le leggi si sono evolute e aggiornate e hanno via via introdotto fattispecie che regolano proprio il data breach, ossia la violazione di dati personali, soprattutto attraverso l'uso di strumenti tecnologicamente avanzati. «E ora a partire dal 25 maggio 2018, data di entrata in vigore del c.d. GDPR, regolamento UE n. 679/2016, il data breach diventerà un elemento pivotale nel sistema di protezione dei dati, con obbligo di notifica al Garante e agli interessati nelle 72 ore successive alla conoscenza dell'evento e le sanzioni sull'illecito trattamento dei dati raggiungeranno il livello massimo del 4% del fatturato annuo globale di gruppo del trasgressore.

Il rischio sanzione sarà talmente alto che si spera possa innescare processi virtuosi di compliance per aziende e pubbliche amministrazioni. Ma occorre fare presto, perché il 2018 è domani e occorre adeguare i processi ed i sistemi delle aziende per tempo», conclude Panetta.

C'è però anche da considerare che le tecnologie e la rete Internet sono alla base e interconnettono ogni ambito della vita dei cittadini, delle imprese, delle pubbliche amministrazioni e dei governi. «A seconda delle azioni intraprese dai soggetti terzi, sono numerose, quindi, le norme che intervengono a sostegno e tutela dei diritti lesi: da quelle previste dal codice penale e relative ai crimini informatici, passando anche per il nuovo dettato dell'art. 4 dello Statuto dei Lavoratori, oppure per l'impianto normativo previsto a tutela della proprietà intellettuale o della reputazione online», fa notare Stefano Mele.

## Le assicurazioni contro i rischi informatici

Esistono anche delle assicurazioni per proteggersi dai rischi informatici, in particolare quelli legati alla violazione delle misure di sicurezza e alla sottrazione dei dati personali (occorre ricordalo, sono dati personali anche quelli dei dipendenti e non solo quelli dei clienti). «Si tratta di un mercato ben conosciuto e solido Oltreoceano, ma nuovo per l'Italia e in forte ascesa. Il problema attuale, però, è soprattutto legato alla difficoltà di comprendere appieno cosa si debba assicurare all'interno di un'azienda e il perché occorra assicurare un asset aziendale piuttosto che un altro», spiega Mele aggiungendo che «ancora una volta, farsi affiancare in queste situazioni da un avvocato che sappia coniugare la parte strettamente tecnico-informatica alle norme in vigore, risulta fondamentale per non trovarsi completamente disorientati e soprattutto scoperti a livello assicurativo in caso di incidenti informatici».

ItaliaOggi Sette

diffusione:88589
tiratura:133263

Affari Legali

*Cyber security, la prevenzione passa dai legali*

da pag. 23

*La sicurezza informatica sta diventando una delle attività più richieste agli studi*

# Le cyber-sfide dei legali

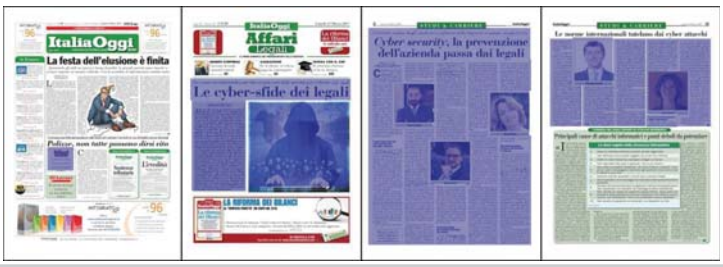
DI ROBERTO MILIACCA

***Allarme cyber-security in Italia. Secondo il Rapporto Clusit 2016, curato dall'Associazione Italiana per la Sicurezza Informatica (tra pochi giorni andrà alle stampe il rapporto 2017), il Belpaese è tra i primi dieci paesi al mondo nella classifica degli obiettivi di cybercrime. La situazione della sicurezza informatica del paese non è delle migliori, soprattutto perchè sotto attacco non sono solo le grandi imprese o le istituzioni pubbliche, ma anche le aziende di medie e piccole dimensioni. Secondo l'Italian CyberSecurity Report 2016, realizzato dal Cis-Sapienza e dal Laboratorio Nazionale di CyberSecurity, è proprio contro le pmi che si sta concentrando la maggior parte delle aggressioni informatiche illecite di questi ultimi tempi, cioè dove sono più bassi i livelli di consapevolezza del rischio, di capacità di reazione, di aggiornamento e formazione del personale. Questa settimana su Affari Legali abbiamo voluto affrontare il tema, interpellando alcuni tra gli studi che si sono specializzati nella lotta al cyber-crime, forti anche delle normative che, a livello nazionale e internazionale, consentono loro di svolgere, al fianco delle imprese, un'attività di prevenzione dei crimini informatici. Poche settimane fa il governo ha aggiornato il Dpcm sulla sicurezza informatica del paese, cercando di razionalizzare e aggiornare il precedente decreto Monti sulle operatività delle strutture istituzionali predisposte alla vigilanza sul cyber-crime. Il nuovo decreto si integra con le recenti disposizioni comunitarie (la direttiva Network and information security) elaborata proprio per rendere più sicuro lo spazio informatico europeo. Insomma, tempo di nuove sfide, sia per le aziende che per i professionisti.***

Caterina Flick

Giuseppe Vaciago

Stefano Mele



ItaliaOggi Sette

diffusione:88589
tiratura:133263

*L'attività svolta dagli studi nei confronti delle imprese si muove su più fronti*

# *Cyber security*, la prevenzione dell'azienda passa dai legali

*Pagine a cura di* **Maria Chiara Furlò**

*Supplemento a cura di* **Roberto Miliacca** ***rmiliacca@class.it*** *e* **Gianni Macheda** ***gmacheda@class.it***

Crimini che passano per il web, cyber spionaggio e attacchi informatici per sottrarre email, documenti e altri file a personalità più o meno note, imprese e governi. Un tema tornato alla ribalta dopo l'inchiesta della procura di Roma che ha portato all'arresto dei due fratelli, Giulio e Francesca Maria Occhionero, ritenuti responsabili di un'ampia attività di cyber spionaggio a scapito di numerose persone legate alle istituzioni, alla politica e alla finanza. In quest'ambito il lavoro di un avvocato specializzato può essere preziosissimo, soprattutto in fase di prevenzione da possibili attacchi.

## Il ruolo degli avvocati nella prevenzione dei cyber attacchi

È capitato diverse volte a **Rocco Panetta**, partner dello studio legale ***Nctm*** ed esperto di internet e nuove tecnologie, di doversi occupare di consulenze alle aziende in ambito di attacchi informatici, «è il nostro lavoro quotidiano. Noi lavoriamo sia in sede preventiva, aiutando aziende e P.a. a pianificare nel tempo e con calma la compliance sull'uso dei dati (la c.d. privacy) e sulla loro sicurezza, soprattutto, sia in caso di incidenti, di violazioni interne ed esterne di dati (c.d. data breach)».

Come spiega il professionista, in questi casi, il presidio «deve essere senz'altro informatico, ma non si può prescindere dalla piena comprensione della complessità giudico legale del fenomeno, se non altro al fine di evitare, prevenire e rimediare al rischio di sanzioni e di richieste di risarcimento danni. In questo gli avvocati specializzati nell'ambito della privacy possono fare la differenza».

Da quando tutte le comunicazioni e i documenti di una società sono stati completamente digitalizzati, lo spionaggio informatico ha cominciato a rappresentare uno dei principali rischi da affrontare e mitigare ogni giorno.

In quest'ottica, il ruolo di consulenza da parte di un avvocato specializzato in Diritto delle Tecnologie, Privacy e Cyber Security «risulta fondamentale sia a seguito di un attacco informatico subìto, che soprattutto in via preventiva, per evitare a monte che simili comportamenti possano essere messi in atto, oppure per essere pronti da un punto di vista legale e procedurale a reagire in maniera efficace nel caso si verifichino», conferma **Stefano Mele** (nel 2014 inserito dalla Nato nella lista dei suoi «Key Opinion Leaders for Cyberspace Security») di ***Carnelutti Studio Legale Associato***. Secondo l'esperto, peraltro, il rischio non giunge soltanto dall'esterno, attraverso Internet o i malware allegati alle email, ma anche e sempre più spesso dall'interno della struttura, attraverso l'azione, ad esempio, di dipendenti in procinto di cambiare azienda, oppure scontenti, infedeli o addirittura pagati da concorrenti perché capaci di avere un accesso privilegiato e consapevole alle informazioni vitali della società da spiare.

Ecco perché svolgere consulenza legale in questo specifico settore, quindi, «è da tempo un'attività quasi giornaliera, che mira ad affiancare il top management e i responsabili della Corporate Security e dell'IT in queste delicatissime attività pre o post incidente informatico», aggiunge Mele.

Occupandosi da molti anni di cybercrime, anche a **Caterina Flick** dello studio ***Nunziante Magrone*** è capitato di offrire consulenza in questo ambito. «L'avvocato penalista può aiutare in due modi», spiega la professionista, riferendosi nel primo caso all'intervento riparatorio, dopo che l'attacco è avvenuto, «si interviene con le indagini difensive e con l'attivazione di procedimenti giudiziari per i reati informatici subiti o con la difesa nei procedimenti giudiziari che coinvolgono il cliente».

Il secondo modo «è l'intervento preventivo, con l'individuazione e corretta qualificazione dei rischi che corre il cliente e la predisposizione degli interventi per la messa in sicurezza dei sistemi informatici e dell'organizzazione». Questo tipo di consulenza, continua Flick, è richiesta dalle aziende consapevoli del fatto che la cybersecurity è utile per diversi obiettivi, tutti rilevanti anche economicamente, in particolare: proteggere know how, brevetti, segreti industriali, tutelare i dati personali trattati, prevenire reati informatici che potrebbero comportare gravi conseguenze per l'azienda. «In ogni caso in questo settore questioni tecniche e giuridiche sono strettamente collegate, per cui per offrire una consulenza legale seria è necessario avvalersi del supporto di tecnici competenti», aggiunge l'avvocato.

## Come funzionano gli attacchi informatici più comuni

Anche a **Giuseppe Vaciago**, partner di ***R&P Legal*** è capitato sia di assistere numerose società vittime di attacchi informatici che di fornire consulenza in materia di sicurezza informatica. «Nel caso degli attacchi, il maggior numero di casi è la cosiddetta Bec (*Busi-*

ItaliaOggi Sette

diffusione:88589
tiratura:133263

*ness Email Compromise*)» dice Vaciago spiegandone il funzionamento: «i dipendenti di un'azienda ricevono una mail fraudolenta, che finge di essere stata inviata da persone o enti di cui si fidano, e che invece è mandata dai truffatori. Nella mail c'è un link o un allegato, seguendo il primo o aprendo il secondo il destinatario viene infettato. Questa è la prima fase, un attacco detto di *phishing*, in cui si cerca di ingannare un utente con email fasulle per infettarlo o rubargli delle credenziali.

A quel punto inizia la fase due. I truffatori hanno accesso al pc e/o alla mail del dipendente. Iniziano a spiarne le comunicazioni interne ed esterne, individuano i responsabili commerciali, i creditori e debitori. Si fanno un quadro della situazione e quindi arrivano alla fase tre. Simulano, con una finta email, di essere un fornitore dell'azienda cui deve essere fatto un pagamento e spiegano che per qualche motivo hanno cambiato Iban. Il nuovo codice in realtà corrisponde a un conto aperto su una banca estera da un membro dell'organizzazione criminale».

Purtroppo, aggiunge Vaciago, è quasi impossibile identificare il cybercriminale perché sono organizzazioni complesse e sono in grado di rendersi completamente anonime. L'intervento di un avvocato esperto del settore è, quindi, «volto principalmente a chiarire le modalità tecniche utilizzate per commettere l'illecito al fine di predisporre un eventuale esposto o denuncia. Tale attività è utile per gestire l'inevitabile contenzioso che si genera in seguito alla truffa tra le due società». Un altro tipo di attacco che le aziende subiscono spesso è quello del ransonware. Come spiega il partner di R&P Legal, si tratta di un malware – tecnicamente «trojan» – che viene utilizzato dai cyber-criminali per bloccare i documenti contenuti sui sistemi infettati e per chiedere un riscatto, in genere in bitcoin. Dopo essere stato contagiato dal cryptovirus, il computer continua a funzionare ma foto, filmati, musica e scritti della vittima vengono protetti tramite algoritmi di cifratura. Al pagamento del riscatto, i criminali in genere sbloccano la protezione dai documenti e rimuovono il criptovirus.

## Strumenti normativi e tecnici che tutelano le imprese

Questi casi sono infatti sempre più frequenti per via dell'evoluzione tecnologica e del fatto che molte aziende non si preoccupano di tutelarsi contro le intrusioni. La normativa vigente, infatti, spiega **Elena Martini** dello studio ***Martini Manna*** «prevede espressamente la tutela delle informazioni riservate sia nell'ambito del codice della proprietà industriale, sia nel codice civile laddove questo sanziona la concorrenza sleale, sia nel codice penale con le norme a tutela dei segreti.

Tuttavia la tutela - in particolare quella da codice della proprietà industriale - è subordinata al fatto che il soggetto che la richiede abbia per primo protetto le proprie informazioni riservate con misure sia tecniche che giuridiche adeguate». Si tratta quindi innanzitutto, da un punto di vista tecnico, continua la professionista, di porre in essere misure in linea con il progresso tecnologico, per bloccare intrusioni e copie non autorizzate.

Dal punto di vista giuridico, invece, è necessario adottare «strumenti che indichino chiaramente la titolarità e la riservatezza delle informazioni: *non-disclosure agreement* («*Nda*»), policy interne, disclaimer sui documenti e sulle email con cui questi vengono trasmessi», aggiunge Martini.

Gli strumenti normativi per tutelare le imprese e i privati in caso di cyber attacchi «esistono e derivano principalmente dall'attuazione di norme internazionali». A farlo notare è Caterina Flick che prende ad esempio la Convenzione sul cybercrime, firmata a Budapest nel 2001, «che in Italia è stata attuata con la legge 48/2008, e che è stata ratificata ed entrata in vigore in quasi tutti i paesi membri del Consiglio d'Europa e in importanti paesi terzi (tra gli altri: Usa, Australia, Israele ...)», spiega la professionista che cita poi anche il recente regolamento europeo sulla protezione dei dati personali, che – «pur essendo focalizzato su altri aspetti – interviene comunque anche sul trattamento dati che avviene online e impone l'adozione di misure di sicurezza».

Secondo Flick però le difficoltà maggiori nel perseguire legalmente crimini informatici stanno però nel fatto che spesso gli attacchi partono da paesi «pirata», che non hanno adottato le regole condivise dagli altri paesi, e nei quali è difficile agire. «La difesa migliore rimane quindi l'adozione di misure di sicurezza informatica adeguate e il loro continuo aggiornamento», conclude l'avvocato di Nunziante Magrone.

La strumentazione giuridica che tutela da questi episodi «c'è ed esiste sin dal 1996, anno in cui è entrata in vigore la prima legge sulla privacy», afferma Rocco Panetta spiegando poi che negli anni le leggi si sono evolute e aggiornate e hanno via via introdotto fattispecie che regolano proprio il data breach, ossia la violazione di dati personali, soprattutto attraverso l'uso di strumenti tecnologicamente avanzati. «E ora a partire dal 25 maggio 2018, data di entrata in vigore del c.d. GDPR, regolamento UE n. 679/2016, il data breach diventerà un elemento pivotale nel sistema di protezione dei dati, con obbligo di notifica al Garante e agli interessati nelle 72 ore successive alla conoscenza dell'evento e le sanzioni sull'illecito trattamento dei dati raggiungeranno il livello massimo del 4% del fatturato annuo globale di gruppo del trasgressore.

Il rischio sanzione sarà talmente alto che si spera possa innescare processi virtuosi di compliance per aziende e pubbliche amministrazioni. Ma occorre fare presto, perché il 2018 è domani e occorre adeguare i processi ed i sistemi delle aziende per tempo», conclude Panetta.

C'è però anche da considerare che le tecnologie e la rete Internet sono alla base e interconnettono ogni ambito della vita dei cittadini, delle imprese, delle pubbliche amministrazioni e dei governi. «A seconda delle azioni intraprese dai soggetti terzi, sono numerose, quindi, le norme che intervengono a sostegno e tutela dei diritti lesi: da quelle previste dal codice penale e relative ai crimini informatici, passando anche per il nuovo dettato dell'art. 4 dello Statuto dei Lavoratori, oppure per l'impianto normativo previsto a tutela della proprietà intellettuale o della reputazione online», fa notare Stefano Mele.

ItaliaOggi Sette

diffusione:88589
tiratura:133263

## Le assicurazioni contro i rischi informatici

Esistono anche delle assicurazioni per proteggersi dai rischi informatici, in particolare quelli legati alla violazione delle misure di sicurezza e alla sottrazione dei dati personali (occorre ricordalo, sono dati personali anche quelli dei dipendenti e non solo quelli dei clienti). «Si tratta di un mercato ben conosciuto e solido Oltreoceano, ma nuovo per l'Italia e in forte ascesa. Il problema attuale, però, è soprattutto legato alla difficoltà di comprendere appieno cosa si debba assicurare all'interno di un'azienda e il perché occorra assicurare un asset aziendale piuttosto che un altro», spiega Mele aggiungendo che «ancora una volta, farsi affiancare in queste situazioni da un avvocato che sappia coniugare la parte strettamente tecnico-informatica alle norme in vigore, risulta fondamentale per non trovarsi completamente disorientati e soprattutto scoperti a livello assicurativo in caso di incidenti informatici».



Elena Manna

Rocco Panetta