Insurance Daily

LUNEDÌ 16 GENNAIO 2017 N. 1050

PRIMO PIANO

Ue-Usa, accordo prima di Trump

L'accordo siglato venerdì scorso tra Unione Europea e Stati Uniti può valere anche fino a tre miliardi di dollari. Il testo apre ancora di più il mercato per gli assicuratori di Ue e Usa riducendo alcuni ostacoli "legali e patrimoniali", secondo quanto recita un comunicato congiunto. Il deal dovrebbe offrire una regolamentazione più chiara per quei soggetti (tanti) che si occupano di assicurazione e riassicurazione su entrambe le sponde dell'Atlantico. Questo porterà a una semplicità d'investimento maggiore, cosa che potrebbe coinvolgere nel piano europeo per gli investimenti nuovi soggetti. Se da una parte i requisiti regolamentari saranno "più morbidi", dall'altra le Autorità Ue e Usa aumenteranno quelli patrimoniali a fronte dei rischi di riassicurazione.

"Quest'accordo rappresenta un ulteriore successo nella cooperazione tra l'Unione Europea e le Autorità di vigilanza degli Stati Uniti", ha commentato il presidente di Eiopa, Gabriel Bernardino.

Il risultato raggiunto è il frutto di discussioni che duravano da più di vent'anni, ma arriva anche nel peggior momento possibile per questo tipo di patti transnazionali, in un contesto di riflusso e rigurgiti protezionisti, e a una settimana dalla salita al potere di Donald Trump, che si autorappresenta come il presidente Usa più isolazionista degli ultimi 90 anni.

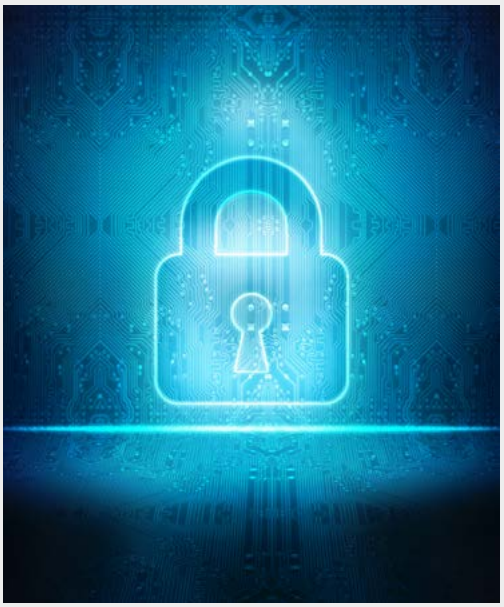
Fabrizio Aurilia

RISK MANAGEMENT

Data Breach: il trasferimento del rischio informatico

Il Regolamento UE sulla conservazione dei dati e le minacce informatiche sempre più consistenti rappresentano un background che meglio definisce i potenziali rischi cyber per imprese e dirigenti: il mercato assicurativo si sta adeguando alle nuove esigenze

(PRIMA PARTE)



La nuova normativa introdotta dal Regolamento Europeo n. 2016/679 impone a tutte le aziende, pubbliche e private, e a tutti gli individui che debbano in qualunque modo gestire, conservare, trasferire o trattare dati personali, di adottare un'articolata politica di *risk management* allo scopo di garantire la propria conformità ai requisiti di sicurezza previsti dal Regolamento stesso.

Per la quasi totalità dei soggetti giuridici che operano nella civiltà digitale in cui viviamo si tratta, quindi, di mettere in atto un approccio integrato, non più basato sul semplice concetto di *compliance*, ma caratterizzato da un'attenta analisi e gestione dei rischi sottesi al trattamento dei dati personali.

La protezione dei dati delle persone fisiche costituisce, infatti, un diritto sancito dall'Articolo 8 della Carta dei diritti fondamentali e dall'Articolo 16 del Trattato sul funzionamento dell'Unione Europea. E poiché i dati personali possono essere violati, danneggiati o distrutti a causa di errori umani o con intenti criminosi, è vitale che i princìpi e le norme che li tutelano siano improntati al pieno rispetto dei diritti di chi li possiede.

Esempi includono gli archivi di società commerciali, nei quali i nomi dei clienti sono associati alle informazioni sulle loro carte di credito o ad altri dati sensibili, oppure le informazioni mediche conservate da assicuratori, medici e ospedali.

Si tratta dunque di assicurare la protezione di tali dati e informazioni personali quando vengano potenzialmente messi a rischio a causa di frodi informatiche, problemi tecnici o errori di qualunque tipo.

(continua a pag. 2)

Insurance Daily

LUNEDÌ 16 GENNAIO 2017 N. 1050

(continua da pag. 1)

GLI OBBLIGHI DEL TITOLARE

Il Regolamento prevede che il Titolare e il Responsabile del trattamento dei dati, figure chiave della nuova normativa, effettuino un'adeguata analisi dei rischi ipotizzabili e la documentino, incorporando i principi della *Privacy by design e Privacy by default* fin dalla progettazione dei processi aziendali e degli applicativi informatici, per garantire il rispetto delle norme introdotte e impedire eventuali abusi nell'utilizzo di tali informazioni.

Oltre all'obbligo di predisporre tale documento di valutazione del rischio, denominato *Privacy Impact Assessment* (PIA), e di garantire con adeguati presidi organizzativi l'*accountability* del soggetto che li tratta, è previsto l'obbligo di definire i tempi di conservazione dei dati e di indicarne la provenienza in caso di utilizzo, nonché quello di comunicare tempestivamente al Garante qualsiasi violazione dei propri database.

NASCE L'ESIGENZA DI TRASFERIRE IL RISCHIO INFORMATICO

Quale che sia l'origine della compromissione dei dati personali, gli effetti che ne derivano per le vittime possono essere assai rilevanti, dalla perdita di profitto ai costi di recupero dei sistemi, al danno reputazionale.

Violazioni e compromissioni dei dati, infatti, possono causare accumulazioni di rischio estese alle società interdipendenti attraverso la catena distributiva globale, danneggiando l'intero sistema produttivo di un'azienda e influendo direttamente sulla sua capacità di condurre l'attività svolta, con serie conseguenze per la sua reputazione e costi ingenti per recuperare i dati perduti e per resistere alle eventuali azioni di risarcimento intraprese da terzi, senza parlare delle multe e ammende previste.

Il nuovo Regolamento europeo, infatti, prescrive sanzioni fino a 20.000.000 di euro per i privati e per le imprese non facenti parte di gruppi e fino al 4% del fatturato consolidato complessivo per i gruppi societari: cifre cospicue, intese come forte deterrente per tutti i soggetti inadempienti.

Data l'ampiezza e l'estrema complessità che caratterizzano il rischio informatico, al di là dell'obbligo di adottare un'adeguata politica di risk management, si impone dunque la necessità di ricorrere, ove possibile, al trasferimento di una parte dei rischi derivanti dal trattamento dei dati altrui e dalla protezione di quelli propri.

I COSTI DEL CYBER CRIME E IL MERCATO DEI RISCHI INFORMATICI

I costi causati dagli attacchi informatici, che rappresentano solo una parte delle compromissioni totali, sono valutati in circa 500 miliardi all'anno dal **Center for Strategic and International Studies**, eppure il mercato dei rischi *cyber* è ancora ai primi stadi del suo sviluppo, nonostante il potenziale premi globale sia stato stimato da **Guy Carpenter** in circa 2 miliardi all'anno.

Sembra che il mercato europeo rappresenti solo una frazione di tale importo, con circa 150 milioni di dollari, ma l'Europa potrebbe facilmente raggiungere i 700-800 milioni di euro entro il 2018, proprio in virtù dell'entrata in vigore della nuova normativa sulla protezione dei dati sensibili e degli obblighi ivi previsti per le aziende.

In Italia si ritiene che i costi per le perdite dirette da attacchi informatici si aggirino tra 800 e 900 milioni di euro, ma i soli danni alla reputazione e da perdita di profitto sono valutati da **McAfee** nell'ordine di 8,5 miliardi di euro, pari a circa lo 0,6% del PIL del nostro paese, e le perdite dovute ad interruzioni operative dei sistemi supererebbero addirittura i 14 miliardi di euro.

Oltre al classico *cybercrime* (furto di dati per trarne vantaggi politici, economici o finanziari), gli attacchi più comuni hanno come obbiettivo:

- la *diffusione* (accesso ai sistemi per propagazione massiva, come accade per lo *spam*);
- l'*hactivism* (diffamazione di organizzazioni o divulgazione di dati riservati);
- il *furto di identità* (sottrazione di informazioni personali di cittadini);
- la *distruzione o cancellazione materiale* dei dati, volta ad ostacolare e danneggiare gli affari di una determinata impresa.

Per alcune di queste esposizioni un adeguato livello di risk management resta probabilmente la soluzione più conveniente, dal momento che i prodotti offerti dal mercato assicurativo non sono ancora in grado di coprire la totalità dei rischi ipotizzati.

Le perdite dirette dovute ad atti criminosi come l'estorsione, ad esempio, sono assicurabili solo in alcuni paesi, mentre è ovunque possibile tutelarsi contro le loro conseguenze, come i costi necessari per il recupero dei dati sottratti e per il ripristino e la decontaminazione dei sistemi danneggiati, fino alla perdita di profitto o all'aumento dei costi di esercizio causati dall'interruzione dell'attività esercitata. (continua a pag. 3)

Insurance Daily

LUNEDÌ 16 GENNAIO 2017 N. 1050

(continua da pag. 2)

Sono queste le garanzie prestate dalle cosiddette "*First Party Cyber Policies*", offerte oggi da compagnie specializzate, che coprono i danni propri dell'assicurato in caso di alterazione, distruzione o sottrazione di dati, nonché l'interruzione parziale o totale dell'attività assicurata che ne dovesse derivare.

NON SI TRATTA SOLO DI AZIONI DOLOSE

Bisogna però considerare che solo il 40% delle violazioni ha origine dolosa: la restante parte dei danni subiti dai dati personali, infatti, resta divisa quasi equamente tra guasti nel funzionamento dei sistemi e semplice errore umano.

In questo caso, soluzioni assicurative per la mitigazione del rischio sono disponibili da tempo nei mercati di tutto il mondo e si sono già diffuse anche in Italia.

Si tratta, ad esempio, delle polizze "Tutti i rischi dell'Elettronica", appartenenti al ramo Rischi Tecnologici, conosciute sin dagli anni Ottanta e originariamente pensate per indennizzare i danni subiti dalle apparecchiature elettroniche, elemento essenziale dell'attività di tutte le società di servizi e delle industrie, con l'affermarsi dei processi produttivi computerizzati.

Questo tipo di polizze, già nate come un prodotto innovativo su base *all risks*, ha dovuto per forza di cose evolversi con grande rapidità, adattandosi al vertiginoso sviluppo dell'elettronica, fino all'avvento dell'era digitale. Oggi è quindi possibile accedere a soluzioni personalizzate a copertura dei danni subiti da apparecchiature quali computer, impianti telefonici, macchine per analisi mediche e scientifiche, strumenti di controllo e misurazione e altri impianti elettronici, in seguito ad eventi accidentali come incendio, furto, sovratensione elettrica ed eventi atmosferici e catastrofali, inclusi guasti e malfunzionamenti in genere. Sono pure comprese le spese sostenute per il riacquisto delle unità di memorizzazione dei dati danneggiate e il ripristino degli stessi, nonché i maggiori costi per il proseguimento dell'attività con apparecchi sostitutivi e/o metodi di lavoro alternativi.

Cinzia Altomare

(*La seconda parte dell'articolo verrà pubbicata su Insurance Daily di domani, martedi 17 gennaio*)

RICERCHE

Ramo vita, trasformazioni in corso

Mercato in evoluzione, le compagnie puntano su maggior attenzione al cliente e sviluppo dell'automazione

Il mercato assicurativo è in continua evoluzione. Aumento della concorrenza, tensione sulla redditività dei canali distributivi, crescita dei costi amministrativi e gestionali: sono solo alcuni dei fattori che stanno spingendo le compagnie ad rivedere i modelli operativi finora utilizzati nel ramo vita. Una trasformazione che è già in corso, come testimoniato dai risultati di una ricerca condotta da **CeTIF**, in collaborazione con **Indra**, sulle politiche di gestione del portafoglio prodotti, il governo dei processi distributivi e la mitigazione del rischio operativo di sette compagnie. "Riteniamo – commenta **Paolo Fantoni**, manager in Italia del mercato assicurativo di Indra – che nel mondo vita l'approccio conservativo è un passo certo verso l'obsolescenza".

Dalla polizza al cliente

"È sempre più urgente – continua Fantoni – l'implementazione di nuovi sistemi più flessibili, veloci, orientati al cliente e in grado di gestire ogni tipo di prodotto e di rischio". E le compagnie appaiono consapevoli delle novità. La ricerca delinea infatti l'immagine di un settore che sembra muoversi lungo alcune linee ben definite. La prima riguarda il cambiamento di paradigma nella considerazione del cliente: non più attenzione alle singola polizza, ma una considerazione generalizzata verso il cliente nell'interezza dei suoi bisogni assicurativi. Si punta innanzitutto su un rinnovamento nelle strategie di fornitura di servizi, in modo da garantire al cliente una fruizione dei prodotti in una logica di omnicanalità. In seconda battuta, secondo la ricerca, le compagnie stanno investendo nell'analisi dei dati relativi al cliente, al fine di giungere a una profilazione delle sue esigenze e all'adozione di strategie di cross selling e up selling.

It: tecnologie e automazione

Il secondo fronte evolutivo riguarda invece l'automazione per la gestione dei prodotti e la parametrazione dei dati: in questo contesto, una più stretta collaborazione fra compagnie e It appare fondamentale. La ricerca rivela come il 70% del campione sfrutti già tecnologie sufficientemente innovative rispetto agli obiettivi prefissati nel ramo vita. Soltanto due compagnie affermano che raggiungeranno un livello di ottimizzazione completo nel 2019: le altre, la maggioranza del campione, hanno già iniziato un percorso evolutivo in questo settore. Segnale evidente che le compagnie reputano il ramo vita di strategica importanza per il proprio business. E si stanno già muovendo per migliorare la propria posizione nel mercato.

Giacomo Corvi

Insurance Daily

LUNEDÌ 16 GENNAIO 2017 N. 1050

RICERCHE

La business interruption preoccupa gli imprenditori

L'interruzione delle attività resta il principale rischio per le aziende, nel mondo e in Italia. Seguono cambiamenti nei mercati, i rischi informatici e le calamità naturali, molto temute nel nostro Paese. Questi i dati salienti dell'Allianz Risk Barometer 2017

L'imprevedibilità del contesto economico è il *leitmotiv* delle paure delle imprese mondiali. Preoccupate da mercati volatili, protezionismo e terrorismo, ma anche dai pericoli che arrivano dalle nuove tecnologie e dalle catastrofi naturali. Tuttavia, secondo il sesto **Allianz Risk Barometer**, il principale timore per le aziende sono le perdite dovute a interruzione delle attività. Che, anche in Italia, si confermano il rischio più temuto (36%), seguito dai cambiamenti nei mercati (30%), le catastrofi naturali (25%) e, a pari merito, i rischi informatici e i timori delle evoluzioni nello scenario macro economico (23%).

La business interruption resta dunque, per il quinto anno consecutivo, al centro delle paure (37% delle risposte a livello globale e 36% in Italia), soprattutto perché può provocare perdite di reddito significative, ma anche perché emergono nuove cause scatenanti, come gli attacchi informatici e l'interruzione delle attività dovuta a instabilità politiche, scioperi o attacchi terroristici. Questa tendenza è guidata, in parte, dalla crescita dell'Internet of Things e dalla sempre maggiore inter-connettività di macchine, aziende e supply chain, ma anche dal continuo mutamento dello scenario politico (Brexit, elezioni Usa, imminenti elezioni in Ue) che genera paure di un maggiore protezionismo e di un processo di anti-globalizzazione.

"Le aziende di tutto il mondo - conferma **Chris Fischer Hirs**, ceo di **Agcs** - si stanno preparando ad un anno di incertezze. Sono preoccupate per i mutamenti imprevedibili nel panorama legale, geopolitico ed economico di tutto il mondo. Stanno emergendo nuovi rischi, oltre a quelli classici di incendio e di catastrofi naturali; per questo è necessario ripensare agli attuali strumenti di monitoraggio e gestione del rischio".

Monitorare le politiche mondiali

Nella classifica dei pericoli, troviamo, al secondo posto, la volatilità del mercato (31% delle risposte a livello globale e 30% in Italia): una preoccupazione non solo per le aziende, ma anche per i settori dell'aviazione/difesa, dei servizi finanziari, del marittimo e dei trasporti. Per anticipare eventuali modifiche normative improvvise, che potrebbero influire sui mercati, le aziende dovranno investire più risorse in un miglior monitoraggio delle politiche mondiali: secondo **Euler Hermes** assicuratore del credito commerciale e società del gruppo **Allianz**, infatti dal 2014 sono state introdotte, nel mondo, 600-700 nuove barriere commerciali all'anno.

Il pericolo che arriva dalla tecnologia

Alta l'attenzione anche per i rischi informatici, che, a livello globale, si posizionano fra le prime tre minacce e che salgono al 2° posto nelle Americhe e in Europa, e al primo in Germania, Regno Unito e nei Paesi Bassi: in Italia sono in 4° posizione.

Il pericolo, che deriva dalla dirompente dipendenza dalla tecnologia e dall'automazione, diventa crescente a causa delle conseguenze degli attacchi indiretti, delle modifiche legislative e degli errori tecnici e umani. In particolare, sono di prossima attuazione le nuove normative sulla protezione dei dati, il cui nuovo Regolamento generale dovrà essere recepito dalle imprese europee, nel 2018, con alti costi sia di adattamento che di sanzioni in caso di inadempienza.

Nell'ambito dell'industria 4.0, poi, l'incapacità di presentare o interpretare correttamente le informazioni potrebbe provocare un'interruzione della produzione e le aziende devono, oggi, imparare a pensare ai dati come ad un bene e a ciò che ne può impedire l'utilizzo: secondo i risultati, le piccole aziende sottovalutano la minaccia informatica, che si posiziona solo al 66° posto, nonostante l'effetto di un incidente grave potrebbe essere molto più dannoso proprio per questo tipo di realtà.

Le calamità, primo rischio per italiani e giapponesi

Infine, al quarto posto, a livello mondiale, si posizionano le catastrofi naturali, i cambiamenti climatici e la crescente variabilità del meteo (rispettivamente il 24% e il 6% delle risposte), che, in Italia, invece troviamo al terzo posto (con il 25% delle risposte) e che rappresentano la preoccupazione principale per Giappone e Hong Kong, così come per le aziende mondiali di ingegneria/costruzioni e servizi/energia.

Laura Servidio

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 16 gennaio di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577