GIURISPRUDENZA

LE CYBER POLICIES SI AMPLIANO

LA TUTELA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

L'intensificarsi dello scambio di dati di qualsiasi genere mediante la rete ha reso sempre più importante proteggere il traffico di informazioni sensibili mediante la implementazione di procedure che possano garantire un maggior grado possibile di controllo sui flussi informativi. Il bisogno di protezione si intensifica naturalmente con l'aumentare del traffico dati, poiché all'aumento del volume di dati in termini di massa corrisponde chiaramente anche un maggior valore delle informazioni stesse scambiate attraverso la rete.

La necessità di attivare meccanismi di protezione a tutela dei soggetti a cui i dati fanno riferimento è stata progressivamente avvertita con crescente attenzione negli anni sia a livello pubblico che privato.

Gli attori del settore privato, e cioè da un lato i soggetti che raccolgono e fanno circolare le informazioni attraverso la rete e dall'altro le compagnie assicurative, hanno proficuamente avviato da più di un decennio un rapporto collaborativo al fine di individuare ed applicare i meccanismi più adeguati per evitare il verificarsi dei cybercrime e fronteggiare i c.d. cyber risk, ovvero quei rischi connessi alla manipolazione ed al trattamento dei dati sensibili attraverso la rete.

Gli sforzi del settore privato in tal senso si sono concretizzati nella creazione di polizze assicurative che, rispetto alle polizze per così dire "tradizionali", prevedono sia un ambito di copertura focalizzato sulle circostanze di rischio che interessano i soggetti che entrano in contatto con la rete internet, sia l'adozione di meccanismi di assistenza in seguito ai sinistri che possono verificarsi a seguito di un attacco informatico o di un negligente trattamento dei dati altrui.

Ad esempio, molte polizze cyber offrono ai soggetti assicurati garanzia per la copertura dei costi relativi a: (i) consulente di reazione per i servizi legali, (ii) servizi di pronto intervento da parte di un esperto informatico, (iii) consulente di crisi che interviene per la tutela della reputazione, (iv) servizi di ripristino dei dati, (v) comunicazioni rivolte a qualsiasi Autorità Amministrativa competente in caso violazione di dati personali o violazione di dati Societari e (vi) monitoraggio del profilo creditizio e dell'identità.

L'evoluzione della normativa concernente i *cyber risk*, ed in generale l'intero mondo del *world wide web*, ha vissuto una fase di stallo in cui l'evoluzione normativa stentava a tenere il passo di quella digitale.

A tal proposito basti considerare che la maggior parte della normativa europea in materia è stata emanata tra il 2014 ed il 2016, in particolare ci si riferisce a:

- Regolamento n. 910/2014, regolamento EIDAS, che ha lo scopo di introdurre un quadro normativo armonizzato per i servizi fiduciari ed i mezzi di identificazione elettronica utilizzati all'interno del territorio UE, al fine di fornire certezza e sicurezza alle transazioni elettroniche sia tra soggetti privati che nel rapporto pubblico-privato.

- Direttiva NIS (Network and Information Security), n. 1148/2016, che stabilisce i requisiti minimi di sicurezza informatica, per quelle

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

imprese che forniscono servizi essenziali e gestiscono le infrastrutture in settori critici. Per tali categorie di imprese è necessario il rispetto di una serie di standard minimi di sicurezza contro i cyber risk.

- Direttiva n. 680/2016, sul trattamento dei dati personali da parte delle autorità competenti.

- Regolamento n. 679/2016, regolamento generale sulla protezione dei dati (GDPR), che, insieme alla direttiva 2016/680, è stato definito il "Pacchetto europeo protezione dati". Il regolamento è indirizzato a quelle aziende che, avendo uno stabilimento all'interno dell'UE, trattano dati personali. Tali aziende hanno l'obbligo di adottare misure di tipo tecnico-organizzativo per prevenire e gestire il rischio informatico e hanno altresì l'onere di dotarsi della figura del responsabile della protezione dei dati.

Con riferimento al regolamento n. 679/2016 è interessante sottolineare che le aziende dovranno adeguarsi a detta normativa entro e non oltre il prossimo 24 maggio 2018.

In questa sede è opportuno prendere in considerazione i possibili risvolti che l'introduzione di nuove norme in materia di rischi informatici potrà avere sulle polizze cyber attualmente presenti sul mercato. Questo focalizzandoci in particolare sulla previsione della necessaria presenza, all'interno delle imprese soggette a tale obbligo, del "responsabile della protezione dei dati".

Innanzitutto, delineando brevemente tale figura, in una nota dello scorso settembre, il Garante per la protezione dei dati personali ha chiarito che i responsabili della protezione dei dati personali (RPS) o data protection officer (DPO) – dovranno avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.
Per ciò che riguarda i compiti affidati al RPD, l'articolo 39, paragrafo 1, lettera b) del reg. 679/2016, gli affida, fra gli altri, il compito di sorvegliare l'osservanza del GDPR. Nel considerando 97 si specifica che il titolare del trattamento o il responsabile del trattamento dovrebbe essere *"assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento"*.

Il controllo sul rispetto del regolamento non significa però che il RPD sia personalmente responsabile in caso di inosservanza delle norme da parte del titolare del trattamento. Il GDPR chiarisce infatti che spetta al titolare, e non al RPD, *"mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento"* (articolo 24, paragrafo 1).

Sulla base delle considerazioni sopra esposte, sebbene il Regolamento escluda una diretta responsabilità del RPD circa il rispetto delle norme in materia di protezione dati, che compete invece all'impresa responsabile del trattamento, non è certamente da escludersi che questi soggetti possano essere chiamati a rispondere in caso di negligenza nel proprio operato.

La figura del RPD sarà certamente esposta a giudizi di responsabilità professionale e tale fattore imporrà l'adeguamento delle polizze cyber al fine di tutelare da un lato l'impresa titolare del trattamento da azioni promosse dai terzi danneggiati e dall'altro il RPD stesso.

Per tale motivo alcune compagnie assicurative hanno recentemente provveduto a predisporre Polizze di RC professionale per quei soggetti, sia singoli professionisti che società, che svolgono il ruolo di RPD "esterni". Tali polizze mirano a coprire i danni causati a terzi a seguito di inadempienza ai doveri professionali commessi appunto nell'esercizio dell'attività di vigilanza sul trattamento dei dati.
Il concetto di attività professionale ricomprende chiaramente tutte le attività affidate al RPD dal regolamento UE 679/2016.

Si tratta dunque di un ulteriore ampliamento del mercato delle polizze cyber, divenuto uno strumento sempre più necessario per tutelare le imprese e i professionisti da rischi che, in caso di sinistro, possono avere conseguenze devastanti per l'attività imprenditoriale, soprattutto in alcuni settori industriali (si pensi ad esempio alle banche ed istituzioni finanziarie).

Avv. ***Laura Opilio*** *- Partner CMS*
Dott. ***Roberto Plutino*** *- Junior Associate CMS*

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato