ISSN 2724-1068

CORPORATE GOVERNANCE

Rivista diretta da **Giovanni Barbara**

4/22

G. Giappichelli Editore

Editoriale

ANDREA ZOPPINI *

1. La digitalizzazione della società, oltre a innegabili benefici in termini di semplificazione dei flussi informativi e degli scambi economici, espone gli attori pubblici e privati a nuove minacce di tipo informatico, rendendo irrinunciabile l'adozione di un adeguato apparato di contrasto, tale da assicurare la tutela di un insieme di situazioni soggettive riferibili alla persona fisica, di interessi economici legati all'impresa e di interessi di tipo strategico riconnessi alla sicurezza nazionale.

In tale scenario, il concetto di *cybersecurity*, inteso, in senso lato, come insieme delle misure idonee a garantire la sicurezza dello spazio cibernetico, evoca una pluralità di problematiche per il giurista. Non a caso, la crescente regolazione del settore tradisce l'idea che il legislatore sia ben consapevole dell'insufficienza di un approccio esclusivamente tecnico-informatico. Ciò sul presupposto che soltanto attraverso la definizione di un quadro normativo solido nonché di una prassi comportamentale condivisa è possibile costruire una strategia di protezione improntata all'effettività.

Occorre pertanto acquisire consapevolezza del ruolo assegnato al diritto in materia di *cybersecurity*, verificando (i) quali sono le situazioni soggettive, gli interessi e i beni di cui è necessario preservare la sicurezza e (ii) le modalità mediante le quali tale attività può essere espletata.

(i) Con riferimento al primo quesito, è ragionevole affermare che il diritto debba ambire a promuovere la riservatezza, l'integrità e la disponibilità di dati, infrastrutture e reti. In primo luogo, difatti, la regolazione della *cybersecurity* si intreccia con la normativa in materia di protezione dei dati personali, raccogliendo le istanze proprie di tale branca, essenzialmente volte alla tutela dei diritti e delle libertà delle persone fisiche nello spazio cibernetico. Al contempo, tuttavia, è bene ricordare che l'ambito della *cybersecurity* non è sovrapponibile a quello della *privacy*, posto che le tematiche riconnesse a quest'ultima, pur rappresentando un ele-

* Professore ordinario di Diritto civile presso l'Università degli Studi Roma Tre.

mento irrinunciabile della sicurezza cibernetica, non sono in grado di esaurire completamente il tema.

La maggiore estensione del perimetro della *cybersecurity* è data dalla circostanza per cui nel suo novero rientrano anche tutte le misure a tutela delle infrastrutture dello spazio cibernetico, della resilienza dei sistemi e degli interessi nazionali. Atteso che i dispositivi fisici sono sempre più connessi alla rete, ove il diritto in materia di *cybersecurity* si occupasse soltanto della prevenzione degli attacchi a dati e informazioni, rischierebbe di lasciare prive di regolazione le minacce alle strutture dotate di materialità.

Al contempo, posto che la minaccia informatica può talvolta tramutarsi nella lesione di interessi di rilievo nazionale, il ruolo del diritto risulta cruciale al fine di definire una strategia di prevenzione e contrasto coordinata, tesa a garantire un livello elevato di sicurezza delle reti informative dal cui malfunzionamento o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

(ii) In merito alle modalità mediante le quali l'attività di implementazione della sicurezza cibernetica può essere svolta, le peculiarità del settore impongono un approccio normativo quanto più variegato possibile.

In tale prospettiva, un modello virtuoso potrebbe esser dato dalla coesistenza di (a) norme programmatiche, (b) norme coercitive e (c) norme volte a fornire incentivi e cooperazione agli operatori.

Le prime, fissando i macro-obiettivi da raggiungere nella disciplina del settore, favoriscono l'armonizzazione degli interventi sia a livello nazionale sia a livello europeo. Si consideri, al riguardo, l'elaborazione della Strategia Nazionale di Sicurezza Cibernetica 2022-2026.

Le norme coercitive, di contro, attraverso l'imposizione dell'obbligo e la previsione della sanzione per il caso dell'inadempimento, appaiono irrinunciabili nell'ottica di assicurare l'*enforcement* dell'intero modello regolatorio. Si pensi, ad esempio, alla responsabilità civile del titolare del trattamento in caso di *data breach* e alla responsabilità penale per le ipotesi di *cybercrime*.

Inoltre, la contestuale previsione di disposizioni volte a carpire la cooperazione degli operatori, anche eventualmente attribuendo loro incentivi, come è avvenuto per le certificazioni *cybersecurity*, può rivelarsi utile in un comparto dove la minaccia cibernetica rivolta a un privato può produrre conseguenze anche in capo all'attore pubblico e viceversa.

2. Il presente numero è dunque dedicato all'analisi del rapporto tra diritto e *cybersecurity* entro diverse prospettive.

Il saggio di Giovanni Barbara, attraverso l'esame dei recenti sviluppi normativi, si sofferma sull'importanza di potenziare la cultura *cyber* degli operatori al fine di prevenire e affrontare adeguatamente il *cyber risk*.

Il contributo di Daniele Piva si occupa dell'impatto della *cybersecurity* sulle

strutture di *corporate governance*, constatando il ruolo cruciale delle normative di settore, delle *best practices* e dei sistemi di certificazione per la creazione di un modello efficiente di *Cyber Risk Management* a supporto degli amministratori, in risposta alle sfide derivanti dal cambiamento tecnologico.

Il lavoro di Maddalena Rabitti e Susanna Sandulli tratta il problema dell'assicurabilità del rischio cibernetico, osservando, per un verso, l'assenza allo stato di criteri oggettivi di valutazione della minaccia, e, per l'altro, la necessità di interventi volti a costruire uno schema legale funzionale all'assicurazione dei *cyber risks*.

Il saggio di Giulia Schneider affronta i tratti del rischio cibernetico nel settore finanziario attraverso l'analisi delle novità apportate dal Regolamento Dora e dei possibili nuovi doveri a carico degli amministratori.

Lo studio di Tommaso Sica, dopo la ricognizione delle tipologie di rischi cibernetici e degli strumenti di gestione e prevenzione degli stessi, opera un raffronto tra la disciplina della *cybersecurity* e quella in materia di protezione dei dati personali, con un particolare approfondimento sulle ipotesi di incidente cibernetico e di violazione dei dati personali.

Lo scritto di Chris Thomale si occupa del problema della *cybersecurity*, muovendo dalla necessità per le imprese di proteggere gli *assets* liquidi e di dotarsi di un efficiente sistema aziendale per la gestione dei pagamenti, per poi concentrarsi sulla responsabilità degli amministratori per il caso di malversazioni ai danni dell'impresa.

Nell'Osservatorio, Simone Russo analizza l'impatto dei rischi cibernetici nella c.d. "Quarta rivoluzione industriale", ossia quella data dal crescente ricorso a un modello di business "*cloud centric*".

Nicolò Moschi spiega le ragioni che spingono un numero sempre maggiore di imprese a utilizzare i sistemi cloud.

Riccardo Fabbri riflette sul possibile impatto dei processi di integrazione e dei modelli ibridi di cloud sull'incremento del rischio cibernetico.

Antonio Giannino e Giovanni Artese esplorano l'evoluzione dei rischi informatici, indagando le origini della sicurezza cibernetica e i suoi attuali sviluppi.

Francesca Valenti, Enrico Amarante e Federico Sertori ricordano l'importanza della *compliance* aziendale in vista dell'implementazione della *cybersecurity* delle imprese.

Infine, il contributo di Elisa Zambito Marsala, spostando la riflessione entro il prisma della *corporate social responsibility*, illustra le modalità con cui Intesa San Paolo ha riscritto la sua "*ESG identity*".