Cybersecurity e *corporate governance* tra valutazioni *top-down* e tecniche *bottom-up*

Cybersecurity and corporate governance between top-down assessments and bottom-up techniques

DANIELE PIVA [*]

ABSTRACT

Nella società digitale, la gestione della sicurezza cibernetica dell'impresa impone scelte organizzative e infrastrutturali che rinviano a responsabilità di *corporate governance*, dovendosi adottare ed efficacemente attuare modelli di *risk assessment* e di *risk management* idonei a prevenire attacchi informatici d'impatto economico e reputazionale potenzialmente devastante in quanto, per un verso, conformi agli standard normativi e di certificazione di riferimento nonché alle *best practices* delle autorità di vigilanza e, per altro verso, in linea con le misure adottate per la prevenzione dei *computer facilitated crimes* presupposto della responsabilità amministrativa di cui al d.lgs. n. 231/2001 e per il trattamento di dati personali ai sensi del Regolamento UE 679/2016 (GDPR) che, del resto, definisce la "violazione dei dati personali" proprio come "violazione di sicurezza". L'ennesimo banco di prova per la *governance* che, a prescindere dalla previsione di singoli obblighi di settore diversamente sanzionati, ne può comportare una responsabilità civile verso la società o verso terzi, ad esempio ai sensi degli artt. 2381, 2392 o 2050 c.c., così come persino una responsabilità penale, sia pur eventualmente a titolo di concorso, per omesso impedimento dell'evento ai sensi degli artt. 110 e 40 cpv. c.p.

In the digital society, the management of the company's cyber security imposes organizational and infrastructural choices that refer to corporate governance responsibilities, having to adopt and effectively implement risk assessment and risk management models suitable for preventing IT attacks with an economic and reputational potentially devastating as, on the one hand, compliant with the reference regulatory and certification standards as well as with the best practices of the supervisory authorities and, on the other hand, in line with the measures adopted for the prevention of computer facilitated crimes as a prerequisite for administrative responsibility pursuant to Legislative Decree 231/2001 and for the processing of personal data pursuant to EU Regulation 679/2016 (GDPR) which, moreover, defines the "violation of personal data" precisely as "security breach". Yet another test case for governance which, regardless of the provision of individual sector obligations sanctioned differently, can lead to civil liability towards the company or towards third parties, for example pursuant to articles

[*] Professore associato di Diritto penale presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre.

2381, 2392 or 2050 of the Civil Code, as well as even a criminal liability, albeit possibly by way of complicity, for omitted impediment of the event pursuant to articles 110 and 40 criminal code.

Sommario: 1. Premessa: la trasformazione digitale dal *business* alla *compliance*. – 2. La *cybersecurity* come responsabilità di *governance*. – 3. *Cyber Risk Management Model* e *compliance* integrata: tra normative di settore, *best practices* e sistemi di certificazione. – 4. *Risk assessment* e *Risk Management* nel modello PDCA (*Plan-Do-Check-Act)*. – 5. Il raccordo con la prevenzione dei "reati informatici-fine" e dei "reati informatici-mezzo" nei modelli organizzativi *ex* d.lgs. n. 231/2001. – 6. (in particolare) I protocolli di comportamento sulla *gestione* dell'attacco informatico.

1. Premessa: la trasformazione digitale dal *business* alla *compliance*

Ab origine, secondo la definizione di Norbert Wiener del 1948, la cibernetica indicava lo studio del controllo e della (auto)regolazione della macchina tramite la trasmissione e l'elaborazione di informazioni provenienti dall'esterno, sino a concretizzarsi poi nelle infrastrutture di difesa delle reti dalle interferenze altrui nelle fasi della creazione, conservazione, invio e ricezione di comunicazioni potenzialmente esposte al rischio di furti, danneggiamenti, interruzione o indirizzamento errato secondo i noti standard di disponibilità, confidenzialità e integrità (C.I.A.).

Oggi la sicurezza informatica esprime, per lo più, in modo unitario gli strumenti di tutela (locali, di *hardware* o *software*) dei sistemi di elaborazione dati da possibili violazioni, sottrazioni o modifiche non autorizzate sempre più rilevanti a causa del loro utilizzo massivo, anche sul versante geopolitico ed economico, tramite la diffusione dei dispositivi "intelligenti" (smart, piattaforme o app) che costituiscono il c.d. "*Internet of things* (IoT)" [1] e, non da ultimo, possibili strumenti di aggressione alla stessa sicurezza nazionale come dimostrano gli interventi nel settore dell'*intelligence* e della difesa [2].

A livello aziendale, la trasformazione digitale – accentuata, per un verso, dalla diffusione dell'industria e del web 4.0 in cui vengono continuamente estrapolati dati dalle navigazioni, dalle email o dal *file sharing* di utenti inconsapevoli tramite configura-

[1] Sull'impatto delle nuove tecnologie e della rete sulla società si rinvia, in particolare, ai lavori monografici di CASTELLS, *The Internet Galaxy. Reflections on the Internet, Business, Society*, Oxford, 2001, p. 58; BALDWIN, *La grande convergenza. Tecnologia informatica, Web e nuova globalizzazione*, Bologna, 2018, p. 29 ss.; FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[2] Si pensi, solo per fare un esempio, al *Cybersecurity Maturity Model Certification* (CMMC), rilasciato a gennaio 2021 dal Dipartimento della Difesa degli Stati Uniti (DoD) quale standard unificato per l'implementazione della sicurezza informatica in tutta la base industriale della difesa (DIB).

zioni appositamente finalizzate di servizi o app nel *cyberspace* ovvero praticati attacchi di *social engineering* per captare da dipendenti informazioni utili sulla propria realtà aziendale e, per altro verso, dalla diffusa autorizzazione a utilizzare dispositivi personali nel posto di lavoro (c.d. BYOD – *bring-your-own-device*) o accedere da remoto ai sistemi aziendali (anche in esecuzione di *smart working* emergenziale o consensuale) – ha finito col rivoluzionare il modo di fare *business* sia nella gestione interconnessa e automatizzata dei processi (ad esempio di *automatic strategic learning*, *data analytics*, *robotic Automation, artificial intelligence and machine learning*) sia nell'articolazione dei rapporti interni o esterni affidata a *software* di teleconferenza o sistemi di comunicazione *online* per l'assunzione e condivisione di decisioni operative, per la formazione del personale tramite *Learning Management Systems* (LMS), per l'inoltro delle segnalazioni di *Whistleblowing* [3] o per la stessa offerta tramite soluzioni *user friendly* di beni o servizi, inclusi quelli essenziali [4].

Si è passati, così, dalla semplice elaborazione meccanica di dati all'impiego di programmi capaci di auto-apprendere, correggersi e persino autodeterminarsi in funzione delle finalità per cui sono predisposti, con nuove prospettive di *compliance* [5], ad esempio mediante ricorso alla tecnologia del *blockchain* [6], e contemporaneo dischiudersi di inesplorati orizzonti sul piano della attribuzione delle relative responsabilità [7]; mentre la connettività è divenuta iper-connettività globale grazie alla

---

[3] Cfr. BAFFI, *Il canale informatico per le segnalazioni del whistleblower in ambito 231*, in *La Responsabilità amministrativa delle società e degli enti*, 2, 2020, p. 262 ss. Si pensi ora alla piattaforma ANAC e ai canali di segnalazione interna, anche tramite strumenti di crittografia, ora previsti dall'art. 4 dello schema di decreto legislativo approvato dal Consiglio dei Ministri in data 9 dicembre 2022 recante *Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.*

[4] Stando alla *Strategia Cloud Italia* elaborata nell'ambito del Piano Nazionale di Ripresa e Resilienza per l'implementazione e il controllo del cloud nazionale, il cui obiettivo è la realizzazione del Polo Strategico Nazionale sul quale far migrare dati della Pubblica Amministrazione.

[5] In tema ABRIANI, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni ad uno studio sull'impianto dell'intelligenza artificiale sulla* corporate governance, in *Nuovo dir. soc*., 3, 2020, p. 268 ss.; NISCO, *Riflessi della* compliance *digitale in ambito 231*, in *Sist. pen*., 14 marzo 2022, spec. p. 5 ss.

[6] In tal senso VITELLI, *Blockchain e modelli organizzativi: nuove opportunità di* governance, in *La Responsabilità amministrativa delle società e degli enti*, 2, 2021, p. 342 ss.; PREZIOSI, *Responsabilità da reato degli enti e intelligenza artificiale*, *ivi*, 4, 2020, p. 173 ss.; SALVATORE, *Blockchain e 231*, *ivi*, 254; MINICUCCI, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari*, in *disCrimen*, 29 aprile 2022, p. 21 ss.: trattandosi, infatti, di un *database* per la gestione di transazioni crittografate su una rete decentralizzata di tipo *peer-to-peer* nel quale si registrano tutti i blocchi con i dati di ciascuna operazione, non è possibile modificare, cancellare o sovrascrivere ma solo aggiungere informazioni a garanzia della trasparenza della gestione e della completezza del tracciamento.

[7] Sui possibili modelli di autonoma responsabilizzazione della macchina, divenuta in determinati

crescente velocità di accumulo e scambio di dati [8], incluso quello di codici e *password* di *login* scambiati nei mercati illegali del *deep* o *dark web*.

2. La *cybersecurity* come responsabilità di *governance*

Da tempo e sotto diversi profili la *cybersecurity* rinvia a competenze e responsabilità di *corporate governance,* coinvolgendo scelte strategiche sul versante sia infrastrutturale sia organizzativo.

La valutazione del crescente impatto economico-finanziario e reputazionale di un attacco informatico costituisce, invero, la "ragion pratica" della verticalizzazione delle responsabilità per la sicurezza che non dipende più solo dalla implementazione di soluzioni tecniche ma anche e soprattutto dalla progettazione di *policy* trasversali alle singole *business unit* e richiede scelte precise in termini di gestione dei rapporti con eventuali aggressori interni (dirigenti, dipendenti o consulenti infedeli) o esterni (*hacker* esperti o semplici esploratori), denuncia o meno alle competenti autorità e comunicazione interna alle funzioni operative o di controllo [9].

In un simile contesto, è proprio la pericolosità di *inside* o *outside attacks* a richiedere l'attivazione di garanzie da parte di chi – creando un proprio *metaverso* nell'ambito di un cyberspazio privo di confini, accessibile a tutti, coperto da anonimato e con informazioni circolanti in modo permanente [10] – può finire col danneg-

---

contesti non più strumento bensì titolare della decisione comportamentale, sia consentito il rinvio a PIVA, *«Machina discere, (deinde) delinquere et puniri potest»*, in *Il diritto dell'era digitale e dell'IA*, a cura di GIORDANO-PANZAROLA-POLICE-PREZIOSI-PROTO, Milano, 2022, p. 681 ss. e alla bibliografia ivi citata.

[8] PICOTTI, Cybercrime *e diritto penale*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, a cura di PARODI-SELLAROLI, Milano, 2020, p. 711 s.

[9] Si pensi, solo per fare qualche esempio, al c.d. *dos* (tecnica utilizzata per bersagliare di richieste un determinato servizio al fine di provocarne il collasso), al furto di informazioni riservate (specie nelle imprese operanti nel settore bancario, finanziario, sanitario o farmaceutico o in quelle *multiutilities*) accompagnato o meno da richieste estorsive, al fenomeno del *Whaling* o delle c.d. "*fake CEO mail*" (ossia delle comunicazioni di posta elettronica inviate da un soggetto che si finge l'amministratore e ordina pagamenti ai propri sottoposti da una casella mail che magari si differenzia di un solo carattere da quella ufficiale) sino alla pratica del *ransomware* (o "pizzo elettronico") che con la trasmissione di un'email (di un *sms* o *chat*) e l'apertura di essa (di un allegato, o cliccando su un l*ink* o *banner*) può introdurre *spyware*, *malware*, *worm, virus*, *backdoor*, *keylogger, sniffer* o *trojan horse* per propagarsi da un *computer* a un altro, consentire accessi non autorizzati, infettare il sistema informatico ovvero spiare, captare o registrare i dati ivi custoditi, recapitando la richiesta economica (tendenzialmente da eseguire in *bitcoin* o tramite *voucher* anonimo e prepagato MoneyPak) per rimuovere la limitazione.

[10] Sulla potenzialità offensiva che assume così il *cyberspace* dal punto di vista sia "esterno" ossia

giare l'azienda che gestisce come i suoi stessi "utenti-avatar": il cyber-individuo deve cioè farsi carico, al vertice dell'organizzazione, del controllo sulle tecnologie e sulle loro evoluzioni orientandolo verso un continuo miglioramento degli standard di prevenzione, in rapporto alla possibile metodologia di aggressione dei propri *network* [11].

Se, dunque, ai sensi dell'art. 2381 c.c., il compito di garantire, anche in materia di *cybersecurity*, un assetto organizzativo adeguato alle dimensioni e ai rischi spetta, nell'ambito di strutture societarie, al CEO o amministratore delegato, sull'intero Consiglio di amministrazione [12] incombe quello di "agire in modo informato": obblighi di *compliance* rispetto ai quali – se è pur vero che conta più la predisposizione del mezzo che l'impedimento dell'esito [13] – neppure può escludersi, sul versante penale, qualsiasi rilevanza ai sensi e per gli effetti dell'art. 40 cpv. c.p., nei limiti di cui si dirà in conclusione.

Detto altrimenti, la costruzione *ad hoc* di un efficace sistema di *governance* non determina soltanto un vantaggio competitivo per chi è in grado di comunicarlo ai propri *stakeholders*, ai clienti e al mercato ma esprime il contenuto di un onere di corretta organizzazione, la cui violazione – a prescindere da obblighi settoriali puntualmente sanzionati a livello amministrativo o penale – può esporre a responsabilità apicali di varia natura, in quanto la protezione dei dati dell'azienda è ormai divenuta condizione della sua stessa sopravvivenza [14]. A ciò si aggiunga che, sul piano reputazionale, a fronte di attacchi informatici istintivamente l'attenzione si incentra spesso non tanto sull'*hacker*, il quale può anche perseguire analogo scopo di profit-

---

del funzionamento della rete sia "interno" dell'utente che vi costruisce la sua esperienza v. KERR, *The Problem of Perspective in Internet Law,* in *Georgetown Law Journal,* n. 91, 2003, p. 357 ss., di recente ripreso da BENATTONI, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace,* in *Sist. pen.,* 5, 2020, p. 303 ss. e FIORINELLI, Nomina nuda tenemus? *Lo statuto penalistico del crimine informatico tra mutamenti fenomenici e modificazioni semantiche*, in *disCrimen,* 3 gennaio 2023, p. 9 ss.

[11] Quella c.d. *targeted* (in quanto preceduta dal *footprinting* incentrato sull'analisi del sistema più adeguato per bypassare i dispositivi di protezione) e quella c.d. *opportunistic* (in quanto basata su uno *screening* dei probabili bersagli e sulla successiva scelta di quello con maggiori *chance* di successo).

[12] Eventualmente tramite un comitato appositamente costituito al suo interno o un sottocomitato, ove istituito, del Comitato Controllo e Rischi.

[13] Così, di recente, MONGILLO, *Presente e futuro della compliance penale*, in *Sist. pen.*, 11 gennaio 2022, p. 2.

[14] In generale, sui possibili effetti paralizzanti degli attacchi informatici cfr., volendo, lo studio contenuto in UNITED NATIONS HUMAN RIGHTS COUNCIL, *Ending Internet shutdowns: a path forward*, United Nations, 15 giugno 2021, in *www.undocs.org*; o anche le riflessioni di RYAN-MOSLEY, *Why you should be more concerned about internet shutdowns*, in *MIT Technology Review*, 9 settembre 2021, in *www.technologyreview.com*.

to, bensì sull'inadeguatezza del *management* aziendale a minimizzare rischi per lo più inevitabili [15].

3. *Cyber Risk Management Model* e *compliance* integrata: tra normative di settore, *best practices* e sistemi di certificazione

Per strutturare un adeguato modello di *Cyber Risk Management* a supporto del *board* in risposta alle sfide derivanti dal cambiamento tecnologico e dalla moltiplicazione dei rischi di attacchi informatici è possibile attingere ai diversi standard desumibili dalle normative di settore e dalle *best practices* internazionali.

Si consideri, da un lato, la direttiva NIS n. 1148/2016 o i d.P.C.M. sul perimetro di sicurezza nazionale cibernetica [16] che, anche per le imprese che non rientrano nel relativo campo di applicazione, possono offrire un catalogo di indicazioni circa l'adozione delle misure tecnico/organizzative finalizzate a prevenire e minimizzare l'impatto di incidenti *cyber* ovvero il contenuto dei modelli organizzativi *ex* d.lgs. n. 231/2001 o degli adempimenti imposti dal Regolamento 679/2016 (GDPR) rispetto alle quali la *cybersecurity* costituisce, in effetti, un "presidio comune" [17]. Dall'altro, alla certificazione ISO 27001 relativa all'*Information Security Management System* (ISMS) a garanzia della riservatezza, integrità e disponibilità delle informazioni ovvero alla ISO 22301 sulla continuità operativa.

Di particolare rilievo, come accennato, è il sistema di procedure e controlli introdotto dal d.l. 21 settembre 2019, n. 105 (convertito con la legge 18 novembre 2019, n. 133) sul perimetro di sicurezza nazionale cibernetica "al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato: esso si fonda, infatti, sulla predisposizione e sull'aggiornamento periodico del proprio elenco di reti e sistemi informativi o informatici comprensivo della relativa architettura e componentistica, sulla protezione fisica e logica dei dati, sull'integrità delle reti e dei sistemi informativi, sulla prevenzione e la notifica di inci-

[15] Così anche DE ROBBIO-AGNINO, *I reati informatici in ambito aziendale*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 246.

[16] D.P.C.M. 30 luglio 2020, n. 131, 14 aprile 2021, n. 81, 15 giugno 2021 e infine 18 maggio 2022, n. 92.

[17] ROMOLOTTI, *Cybersecurity: Un ponte tra gdpr e d.lgs. 231/2001 alla luce del d.lgs. 101/2018,* in *La responsabilità amministrativa delle società e degli enti,* 2, 2019, p. 78 s.

denti, sulla comunicazione al Centro di valutazione e certificazione nazionale (CVCN) nel caso di affidamento di forniture di beni, sistemi e servizi ICT destinati a essere ivi impiegati nonché sull'attribuzione di funzioni di ispezione, verifica ed eventuale prescrizione alla Presidenza del Consiglio dei Ministri e al Ministero dello sviluppo economico (peraltro con imputazione all'ente di specifico illecito amministrativo *ex* d.lgs. n. 231/2001 in relazione a condotte di reticenza o mendacio ai sensi dell'art. 1, comma 11, d.l. n. 105/2019) [18].

Più in generale, utili indicazioni possono poi mutuarsi – in attesa di futuribili sviluppi di iniziative già intraprese a livello ONU [19] – dalla più recente normativa nazionale [20] e comunitaria [21] sulla cybersicurezza, così come dalla *practice* dei corrispondenti enti (ENISA, Agenzia per la cybersicurezza nazionale o Comitato interministeriale per la cybersicurezza) volti a promuovere la cooperazione e lo sviluppo di progetti per la realizzazione di un cyberspazio globale sicuro, sotto il coordinamento – specie a seguito delle modifiche introdotte col Regolamento UE 2002/991 dell'8 giugno 2022 – di EUROPOL.

Nondimeno, il modello di *Cyber Risk Management Model* dovrà coordinarsi con le misure di *compliance* a protezione dei dati personali circolanti su reti o sistemi informatici aziendali, adottate in attuazione di quanto previsto dal Regolamento UE 679/2016 (GDPR) e dal d.lgs. n. 196/2003 come riformato *ex* d.lgs. n. 101/2018 – il cui art. 4, n. 12, del resto, definisce la "violazione dei dati personali" proprio come "violazione di sicurezza" [22].

---

[18] Per un commento v. ROMOLOTTI, *Il decreto cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001,* in *La responsabilità amministrativa delle società e degli enti,* 1, 2020, p. 121 ss.

[19] Ci si riferisce alla Risoluzione 74/247 adottata il 27 dicembre 2019 ed intitolata "*Countering the use of information and communications technologies for criminal purposes*", con cui si è istituito un Comitato intergovernativo di esperti (Comitato *ad hoc*), rappresentativo di tutti i paesi, per elaborare una Convenzione globale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione per scopi criminali. In argomento v. MATTARELLA, *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica,* in *Sist. pen.*, 3, 2022, p. 41 ss.

[20] D.l. 14 giugno 2021, n. 82, convertito in legge 4 agosto 2021, n. 10, in combinato disposto col d.lgs. 18 giugno 2018, n. 65, di recepimento della direttiva UE 2016/1148, 6 luglio 2016, c.d. «NIS» – *Network and Information Security.*

[21] *Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019,* relativo *all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione.*

[22] Specie in materia di accesso e utilizzo delle informazioni, tracciabilità di decisioni e operazioni, *screening* aziendale in conformità al *Data Protection Impact Assessment* (DPIA), diversificazione dei processi e formazione del personale.

4. *Risk Assessment* e *Risk Management* nel modello PDCA (*Plan-Do-Check-Act)*

Il punto di partenza è la mappatura dei processi interni con selezione di quelli strategici, di supporto e di *core* (o critici) dai quali dipende la sopravvivenza operativa dell'organizzazione.

A questi corrisponde l'individuazione degli *asset* strategici a supporto oggetto di un *assessment* volto a identificare e ponderare i rischi endogeni ed esogeni correlati sia in termini tecnici che di *compliance* mediante la combinazione di indicatori e *score* in grado di ottenere un quadro completo del livello di rischio dell'azienda e implementare un *Proactive Cyber Risk Management* costituito da modelli predittivi e analitici ciclicamente sottoposti a monitoraggio e riesame secondo un approccio PCDA (*Plan-Do-Check-Act*).

In particolare, può evidenziarsi la necessità di: a) identificare i ruoli e le responsabilità del trattamento dei dati, nonché delle informazioni e i relativi principi di classificazione dei soggetti coinvolti con particolare attenzione ai rapporti con informatici *outsourcer*, con i quali sarà altresì opportuno definire clausole contrattuali relative alla qualifica e al controllo sulla gestione delle misure di sicurezza onde prevenire possibili addebiti per *culpa in eligendo* o *in vigilando*; b) assicurare un'adeguata protezione delle apparecchiature incustodite; c) garantire il corretto e sicuro funzionamento degli elaboratori di informazioni, la protezione da *software* pericolosi, il *backup* di dati e *software*, la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti nonché una verifica dei *log* che registrano le attività degli utilizzatori; d) adottare procedure, sistemi di *warning* o *check list* semplici e limitate, comunque non lunghe o ripetitive, in modo da non alimentare la tendenza a pericolose scorciatoie o deviazioni idonee a generare, sia pur in modo episodico o occasionale, elusioni, omissioni o vuoti di tutela; e) istituire un *Cyber Security Manager* chiamato assicurare il corretto funzionamento di soluzioni anti-spionaggio e misure di prevenzione specifiche contro attacchi informatici [23] nonché di intervento diretto e immediato in caso di falle; f) elaborare protocolli di *disaster recovery* o *computer forensics* idonei a recuperare i dati persi per via di incursioni illecite; g) programmare e svolgere, eventualmente a cura del *Responsabile Information Technology*, attività di *audit, internal investigations o simulazione* (ad esempio, tramite invio di false mail di *phishing*) volte a sondare l'effettiva vulnerabilità della rete e allo stesso tempo l'affidabilità del personale; h) documentare nel tempo le *performance* ottenute grazie ai sistemi utilizzati e il livello di sicurezza nel tempo raggiunto, oltre che l'esposizione di eventuali attac-

[23] A mezzo VPN (*Virtual Private Network)*, IDS (*Intrusion Detection System)*, *patch*, *firewall*, programmi antivirus, URL *filtering*, sistemi OTS (*One Time Password)*, di *logging* e *monitoring*, etc.

chi informatici subiti e la reazione del *network*; i) curare attività formativa personalizzata a seconda dell'incarico e diretta a far comprendere come i diversi comportamenti [24] possano essere causa di un attacco, a fornire strumenti utili ad individuare i tentativi dell'*hacker* nonché a incentivare la collaborazione e sedimentare una cultura della prevenzione [25].

Ma soprattutto si dovrà adottare, aggiornare, diffondere e far osservare – a pena di sanzione disciplinare, in conformità alle disposizioni dello Statuto dei Lavoratori (art. 7, legge n. 300/1970) – un manuale relativo all'utilizzo delle risorse informatiche aziendali che definisca pure i requisiti di autenticazione, registrazione, assegnazione/revoca di *password* o altre credenziali di accesso ai sistemi informativi nonché regolamentare l'uso di *pc, device* (*tablet* o *smartphone*), servizi IM (es. *Skype*) o *clouding*, *browser* e *social network* (come *Whatsapp, Facebook* o *Instagram*) a fini lavorativi.

Per la gestione di informazioni sensibili, potrebbe stabilirsi il ricorso a sistemi crittografici o steganografici per la trasmissione in rete di documenti e l'implementazione di c.d. *penetration test* per la c.d. *vulnerability assessment*.

Con riguardo alla gestione delle attività *online* svolte dai dipendenti, a protezione dello scambio di informazioni sensibili in relazione al *business* di impresa, potrebbe invece valutarsi l'obbligatorietà della registrazione di attività eseguite su sistemi, applicazioni e reti, potenzialmente lesive per la sicurezza aziendale.

5. Il raccordo con la prevenzione dei "reati informatici-fine" e dei "reati informatici-mezzo" nei modelli organizzativi *ex* d.lgs. n. 231/2001

Da ultimo, per quanto più d'interesse penalistico, il modello di *cybersecurity* si interseca con la prevenzione della criminalità informatica la cui disciplina risulta, ancora una volta, dal combinato disposto di normative nazionali (legge n. 547/1993,

---

[24] Ad esempio sotto forma di mancato utilizzo di sicuri collegamenti wi-fi, scelta di *password* deboli, commistione di *account* personali e di lavoro, *download* di *software*, utilizzo di *torrent*, navigazione su taluni siti *internet*, ecc.

[25] Anche nel settore pubblico, il Codice dell'amministrazione digitale (d.lgs. n. 82/2005) stabilisce, all'art. 13, che "*le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, attuano politiche di reclutamento e formazione del personale (...) Le politiche di formazione di cui al comma 1 sono altresì volte allo sviluppo delle competenze tecnologiche, di informatica giuridica (...)*".

A livello di istituzioni comunitarie, l'European Court of Auditors nello Special Report 05/2002 del 29 marzo 2022 ha parimenti invitato la Commissione, all'esito di un esame avente ad oggetto gli strumenti a disposizione per proteggersi dai cyberattacchi, a migliorare la preparazione del personale competente proponendo l'introduzione di regole vincolanti in tema di *cybersecurity* e l'aumento le risorse a disposizione dei *Computer Emergency Response Teams*.

legge n. 48/2008 e infine legge n. 238/2021)[26] e vincoli comunitari diretti – per lo più in seguito all'introduzione col Trattato di Lisbona della materia nelle competenze dell'Unione di cui all'art. 83 TFUE quantomeno per *serious crimes having a cross border dimension* – a ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione imponendo di punire la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo intenzionali di determinati strumenti (programmi per computer o password o codici d'accesso o simili), con l'intenzione di utilizzarli per realizzare accessi o interferenze illecite a sistemi di informazione[27]: anche la criminalizzazione di comportamenti prodromici o comunque incentrati sul pericolo presunto costituisce, infatti, strumento funzionale alla costruzione di uno spazio di sicurezza esteso alla rete.

In particolare, non può non tenersi conto di come l'ente si organizzi al fine di evitare la contestazione della responsabilità amministrativa di cui al d.lgs. n. 231/2001 che, se sin dall'origine prevede all'art. 24 la frode informatica (art. 640-*ter* c.p.) commessa a danno dello Stato o di ente pubblico[28], a seguito delle modifiche introdotte con l'art. 7 della legge n. 48/2008 emanata in ratifica ed esecuzione della nota Convenzione del Consiglio d'Europa sulla criminalità informatica svoltasi a Budapest il 23 novembre 2001, include all'art. 24-*bis* i delitti informatici rientranti nel paradigma del *computer facilitated crime*[29] e teoricamente strumentali al-

---

[26] Sulla definizione e sulle diverse articolazioni della c.d. "criminalità informatica" si rinvia a PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, diretto da CADOPPI-CANESTRARI-MANNA-PAPA, Torino, 2019, p. 59 ss.

[27] Così, ad esempio, rispettivamente, il considerando 1 e l'art. 7 della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione che, a seguito di procedura d'infrazione 2019/2033 aperta contro l'Italia dalla Commissione, ha condotto alle ultime modifiche apportate dall'art. 19 della legge n. 238/2021 ai delitti previsti negli artt. 615-*quater*, 615-*quinquies*, 617, 617-*bis*, 617-*quater* e 617-*quinquies* c.p.: in tema MONTANARO, in *lalegislazionepenale.it*, 4 luglio 2022.

[28] Divenuta, peraltro, procedibile a querela di parte anche a fronte di un danno patrimoniale di rilevante gravità ovvero di recidiva nei casi in cui integra un'aggravante ad effetto speciale, a seguito delle modifiche apportate dal d.lgs. n. 155/2022, in vigore dal 30 dicembre 2022 (stante l'art. 6 d.l. n. 162/2022 convertito con legge n. 199/2022), con conseguenti possibili ricadute sulla contestazione del corrispondente illecito amministrativo all'ente ai sensi dell'art. 37 d.lgs. n. 231/2001.

[29] Artt. 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*quater*, 617-*quinquies*, 635-*bis,* 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*quinquies* e 491-*bis* c.p. su cui v., solo tra i più recenti, MELONI, sub *Art. 615-ter – Accesso abusivo ad un sistema informatico o telematico*, in *Codice penale commentato online*, a cura di RONCO-ROMANO, Milano, 2022; PARODI, *I reati patrimoniali*, SCORDAMAGLIA, *La falsità in documento informatico*, SALVADORI, *I danneggiamenti informatici*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., rispettivamente 103 ss., 323 ss. e 595 ss.; SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime*, a cura di CADOPPI-CANESTRARI-MANNA-PAPA, Milano, 2020, p. 693 ss.; PICCINNI, *Analisi di due tra i reati informatici più invasivi: l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche e l'installazione di*

la realizzazione di ulteriori reati-presupposto: dai delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies*1 come introdotto con d.lgs. n. 184/2021)[30] alla manipolazione del mercato (art. 25-*sexies* d.lgs. n. 231/2001) commessa mediante l'impiego delle tecniche di negoziazione algoritmica denominati *High-Frequency Trading* (HFT) di cui alla Direttiva UE 2014/65 (c.d. MIFID II) e capaci di operare, senza intervento umano, sulle piattaforme ad alta intensità operativa[31] sino alle diverse fattispecie di cyber (auto)riciclaggio, come peraltro estese dal d.lgs. n. 195/2021 (art. 25-*octies* d.lgs. n. 231/2001), contrassegnate dal pagamento con criptovalute che – specie a seguito delle modifiche introdotte alla disciplina di riferimento (artt. 15 ss. d.lgs. n. 231/2007) ad opera dei dd.lgs. nn. 90/2017 e 125/2019 – determinano una responsabilizzazione degli operatori di mercato (*wallet provider*, *exanger*, *broker*) in termini di verifica e registrazione della clientela, comparazione dei dati raccolti, aggiornamento periodico delle informazioni e segnalazione di fondi di provenienza sospetta, a prescindere dal ricorso ai

---

apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, *ivi*, 1, 2019, p. 125 ss.; ID., *L'art. 24 bis del d.lgs. 231/2001 e i reati di cui agli articoli 615 quater e 615 quinquies c.p.*, *ivi*, 3, 2018, p. 95 ss.; ID., *Panoramica sul delitto di accesso abusivo a sistema informatico o telematico: il crimine informatico più diffuso tra quelli inseriti tra i reati presupposto ex art. 24 bis del d.lgs. 231/2001, da cui deriva per le società e gli enti la responsabilità amministrativa da reato*, in *La responsabilità amministrativa delle società e degli enti*, 2, 2018, p. 85 ss.; SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *MediaLaws – Rivista dir. media*, 2, 2018, p. 235 ss.; ancora PICCINNI, *Il reato di danneggiamento di sistemi informatici e telematici disciplinato quale reato presupposto dall'art. 24 bis, d.lgs. 231/2001 per l'applicazione delle sanzioni in materia di responsabilità amministrativa delle società e degli enti*, *ivi*, 4, 2017, p. 127 ss.; MANCINI, *I reati contro l'integrità dei dati e dei sistemi informatici di pubblica utilità*, in *La digitalizzazione della società moderna. Incidenze e refluenze della tecnologia digitale sulle istituzioni pubbliche e il diritto nell'esperienza italiana*, a cura di CROCCO-NERI, Napoli, 2016, p. 123 ss.; DEZZANI-SANTORIELLO, *Il reato di accesso e trattenimento "abusivi" nel sistema informatico e la responsabilità amministrativa delle persone giuridiche*, in *La responsabilità amministrativa delle società e degli enti*, 1, 2012, p. 57 ss.

[30] In particolare, sulle possibili responsabilità del *financial manager* anche in relazione a reati di questo tipo commessi mediante tecniche di *phishing* v. Cass., sez. II, 11 marzo 2021, n. 9787, in *dejure.giuffre.it*. In tema v., di recente e più ampiamente, RECCIA, *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in *Arch. pen*., 2/2022, p. 1 ss. (spec. p. 13 ss.).

[31] Di recente, l'attenzione del legislatore europeo si è peraltro ulteriormente appuntata sulle cripto attività come strumenti finanziari stabilendo, col il Regolamento 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 di modifica della citata direttiva UE 2014/65, una disciplina *delle negoziazioni con tecnologia a registro distribuito* (*DLT – Distributed ledger technology*) *onerando i* gestori delle relative infrastrutture della protezione dei fondi dai rischi di accesso non autorizzato, pirateria informatica, degrado, perdita, attacco informatico, furto, frode, negligenza e altri gravi malfunzionamenti operativi e imponendo loro un obbligo di notifica alle autorità competenti di *qualsiasi prova di accesso non autorizzato, malfunzionamento rilevante, perdita, attacchi informatici o altre minacce cibernetiche, frode, furto o altri gravi abusi subiti.*

meccanismi di intelligenza artificiale della c.d. *transaction monitoring* fondata sulla generazione di *alert* [32].

Si pone dunque la necessità di un raccordo tra la prevenzione di attacchi *a danno* dell'impresa e quella avente ad oggetto, ai sensi dell'art. 5 d.lgs. n. 231/2001, reati informatici commessi viceversa (anche o soltanto) nel suo *interesse o vantaggio* [33], siano essi "fine" o "mezzo" per la realizzazione di ulteriori reati-presupposto [34] (ove pur accompagnati dalla temporanea compromissione dei propri sistemi, il cui ripristino comporti nell'immediato un costo economico).

6. (in particolare) I protocolli di comportamento sulla *gestione* dell'attacco informatico

Di specifico impatto, altresì, i protocolli di comportamento in caso di attacco informatico estorsivo, in termini di divieto di adesione, blocchi interni alla raccolta e all'utilizzo di denaro e denuncia alle competenti autorità.

A prescindere, infatti, dalla contrarietà del pagamento ai principi del proprio codice etico, ove realizzato nell'interesse dell'ente (ad esempio per comprare un silenzio e recuperare credibilità evitando migrazione della clientela, riduzione delle *revenue* e consequenziale abbassamento del valore delle azioni della società), esso potrebbe, di per sé, integrare determinati reati-presupposto *ex* d.lgs. n. 231/2001: da quelli di natura societaria *ex* art. 25-*ter* (ove la somma risulti pagata attraverso un indebito utilizzo di provvista sociale o non contabilmente tracciata) o di (auto)riciclaggio (ove si impieghino fondi di illecita provenienza) *ex* art. 25-*octies* sino a quelli di criminalità organizzata *ex* art. 24-*ter* (in considerazione della condotta tenuta durante l'attacco informatico e per la risoluzione di esso, dell'entità e delle modalità di corresponsione del riscatto e del livello di collaborazione prestato con l'autorità giudiziaria nazionale e internazionale) [35].

---

[32] Sulle peculiarità del riciclaggio e dell'aggiotaggio telematico v., in particolare, PARODI-LOMBARDO-GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 445 ss.; SICIGNANO, *I modelli di comportamento dell'ente nel riciclaggio mediante criptovalute*, in *Le Società*, 2021, p. 1284 ss.

[33] In tema RAZZANTE, *Cybersecurity e 231: il raccordo tra eventi e norme*, in *La responsabilità amministrativa delle società e degli enti*, 1, 2022, p. 34 ss.

[34] Per un approfondimento sulla possibile diversa articolazione del requisito dell'*interesse o vantaggio* – il primo notoriamente inteso come valutazione teleologica del reato apprezzabile *ex ante* secondo un metro di giudizio marcatamente soggettivo e il secondo in ottica essenzialmente oggettiva, come tale valutabile *ex post* sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito – in rapporto a "reati informatici-fine" e "reati informatici-mezzo" v., da ultimo, MINICUCCI, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari*, cit., p. 20 ss.

[35] BARTOLOMUCCI, *Pandemia cybercrime: prevenzione del rischio di estorsione da sequestro in-*

Un'ulteriore conferma del fatto che la *cybersecurity* aziendale si articola ormai in un più livelli tra loro intrinsecamente connessi e interdipendenti, quello delle tecniche di *bottom up* e quello delle valutazioni *top-down*, che impongono l'attuazione di modelli "circolari" caratterizzati dalla coerente produzione di normative stratificate (delibere, codici, regolamenti, manuali, ordini di servizio, circolari o istruzioni operative) e nell'ambito dei quali se il *manager* assicura il corretto funzionamento dei sistemi di prevenzione e l'*audit* provvede al ripetuto svolgimento di *stress-test,* è la *governance* a determinare *ex ante* la politica di sicurezza per sottoporla *ex post* a periodico riesame e imputarsi, nel tempo, una responsabilità per deficit infrastrutturali, organizzativi o di alta vigilanza che mentre sul versante civile può comportare il risarcimento dei danni derivanti dall'attacco informatico all'azienda o terzi, rispettivamente ai sensi degli artt. 2392 e 2050 c.c., su quello penale potrebbe persino sfociare in una contestazione a titolo di concorso nel reato altrui ai sensi degli artt. 110 ss. c.p. e/o di omesso impedimento dell'evento entro i limiti dell'art. 40 cpv. c.p., con ricadute anche sull'illecito amministrativo dell'ente *ex* d.lgs. n. 231/2001 [36]. Semmai, dovendosi distinguere a seconda che il reato sia commesso da *interni* all'azienda (dipendenti o collaboratori), rispetto ai quali il mancato esercizio di poteri-doveri di controllo gerarchico-funzionale, ove anche non di effettivo impedimento, può integrare forme di concorso morale o materiale ovvero da *esterni* (utenti, clienti, fornitori, consulenti) il cui operato potrà essere ascritto, per lo più, in quanto consapevolmente sorretto da analogo intento criminoso, non essendo altrimenti configurabile una capacità impeditiva in relazione ad attività che si pongono comunque al di fuori dell'organizzazione.

Un'ulteriore sfida, dunque, per la *governance* d'impresa, forse quella che la attraversa più trasversalmente e che la cambierà più radicalmente giacché, come pure è già stato teorizzato [37], chi avrà l'approccio più efficace al cambiamento tecnologico nel prossimo futuro dominerà il mondo. E il prossimo futuro è ormai già iniziato.

---

formatico e gestione emergenziale compliant *col d.lgs. 231/2001 e il regolamento privacy u.e. n. 679/2016*, in *La responsabilità amministrativa delle società e degli enti*, 1, 2018, spec. pp. 95-97.

[36] Sul punto, di recente, MINICUCCI, *Reati informatici e responsabilità degli enti: vecchi e nuovi scenari*, cit., p. 12 ss.

[37] Cfr., ad esempio, GUASTELLA, *Il dominio geopolitico dello spazio cibernetico*, Palermo, 2020, *passim*, spec. p. 151.