La gestione del cyberischio in ambito societario: un confronto tra Stati Uniti ed Europa

di **MARCO COLUZZI**

SOMMARIO: 1. CONTESTO DI RIFERIMENTO E APPROCCIO ALLA DISCIPLINA DEL C.D. CYBER RISCHIO. – 2. LA DISCIPLINA STATUNITENSE: LE SEC RULES. – 3. LA DISCIPLINA EUROPEA: IL DORA. – 4. UN CONFRONTO TRA I DUE APPROCCI REGOLATORI *DE JURE CONDITO*. – 5. ULTERIORI RIFLESSIONI COMPARATISTICHE *DE JURE CONDENDO*: LA SITUAZIONE IN EUROPA E NEGLI STATI UNITI.

Abstract

Nowadays, cybersecurity represents a significant part of the corporate governance system and has also become a fundamental component in terms of market stability. Therefore, from a policy standpoint, the regulators face the issue of how to approach the so-called "cybersecurity risk management", which can be seen and addressed either from an "entrepreneurial" perspective or from a "systemic risk" perspective. This different understanding of risk has produced two different regulatory approaches in the US and Europe.
In the United States, the Securities and Exchange Commission, focusing on market disclosure, in July 2023 approved the rules on "cybersecurity risk management, strategy, governance, and incident disclosure" for listed companies. Additionally, US case law is evolving to consider the failure to monitor IT systems as a violation of directors' fiduciary duties. In Europe, the awareness that cyber risk can represent a structural and systemic risk has led in December 2022 to the adopting of the regulation on "digital operational resilience for the financial sector" (DORA) for financial entities.
This paper aims to provide some preliminary reflections on the issue of cybersecurity risk management from the US and European regulatory standpoints, as well as to explore potential points of contact between these regulatory frameworks, evaluating whether and which elements each legal system could or should take from the other.

1. 1. Contesto di riferimento e approccio alla disciplina del c.d. cyber rischio.

Nel mondo moderno il tema della c.d. cybersicurezza[1] trascende ormai l'ambito puramente tecnico per incidere – tra l'altro – sulla continuità operativa ed aziendale[2]. Lo stesso tema – oltre a rivestire carattere critico nella prospettiva della *governance* societaria – si sta allargando a componente

[1] V., in generale, N. MICHIELI, *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in *Banca, impresa, società*, 2024, 2 ss.
[2] OECD, *OECD Policy Framework on Digital security: Cybersecurity for Prosperity*, dicembre 2022, disponibile *online* all'indirizzo: https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page1. V. anche G. SCHNEIDER, *La resilienza operativa digitale come materia di* corporate governance*: prime riflessioni a partire dal DORA*, in *Riv. Corp. Gov.*, 2022, 555.

fondamentale in termini di stabilità dei mercati, tanto è vero che, anche a segno della consapevolezza delle Autorità di vigilanza sul tema (soprattutto dal punto di vista della regolamentazione finanziaria), nella rappresentazione integrata dei rischi aziendali a fini prudenziali il "rischio informatico" è ormai considerato tra i rischi operativi, reputazionali e strategici[3]. È vero, infatti, che una quota via via crescente dell'attività economica dipende dai sistemi tecnici ed informatici, per cui l'eventuale interruzione degli stessi può avere effetti significativi su (ma non solo) gli emittenti quotati e, nel caso di attacchi su larga scala, addirittura effetti sistemici sul sistema economico nel suo complesso. Ed infatti, il rischio legato alla sicurezza dei sistemi informatici assume la valenza di "rischio sistemico"[4] posta la marcata interconnessione tra le istituzioni finanziarie unitamente alla tendenza delle stesse alla digitalizzazione, fattori che rendono globale la portata di un possibile *cyber attack*[5].

In tale scenario, l'evidenza empirica dimostra come negli ultimi anni si sia verificato un aumento sostanziale degli incidenti di sicurezza informatica, spinto da diversi fattori, tra cui, per citarne alcuni, l'aumento del lavoro a distanza (stimolato dalla pandemia) e la crescente dipendenza da fornitori di servizi terzi per i servizi di tecnologie dell'informazione e della comunicazione (di seguito, anche, "**TIC**" o "**ITC**")[6].

---

[3] Cfr. P. CIOCCA, *Workshop Università Cattolica del Sacro Cuore e Consob «Cyber Security, Market Disclosure & Industry». Intervento del Commissario Consob Paolo Ciocca*, 27 febbraio 2023 (disponibile *online* all'indirizzo: https://www.consob.it/documents/1912911/2129425/intervento_Ciocca_20230227.pdf/3bd26698-5c6a-4e72-0984-007c2e36e6b7).

[4] Per «rischio sistemico» si intende «*un rischio di perturbazione del sistema finanziario che può avere gravi conseguenze negative per l'economia reale dell'Unione o di uno o più dei suoi Stati membri e per il funzionamento del mercato interno. Tutti i tipi di intermediari, mercati e infrastrutture finanziari sono potenzialmente importanti in certa misura per il sistema*» (art. 2, comma 1, lett. c) del Regolamento (UE) n. 1092/2010 del Parlamento Europeo e del Consiglio del 24 novembre 2010 che ha istituito il Comitato europeo per il rischio sistemico (CERS).

[5] Cfr. A. PERRONE-I. GIRARDI, *Innovazione tecnologica e stabilità finanziaria*, in M. CIAN-C. SANDEI (a cura di), *Diritto del Fintech*, Milano, Cedam, 2024, 28. Enfatizzando tale prospettiva "globale", gli Autori riportano il seguente esempio: «*invece di rapinare un contro, una filiale o una impresa, un aggressore è nelle condizioni di rapinare o attaccare tutti i conti e tutte le filiali, di molteplici imprese, in molteplici ordinamenti e nello stesso momento*».

[6] Cfr. negli USA la proposta del 9 marzo 2022 della *Securities and Exchange Commission* di alcune *rules* sulla "*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11038*".

In aggiunta, i costi e le conseguenze negative (anche in termini di potenziali contenziosi) degli incidenti di sicurezza informatica per le società sono notevolmente aumentati e non rappresentano più un elemento trascurabile[7].

Da un punto di vista di *policy*, dunque, si pone il tema per il regolatore di come approcciare la disciplina del c.d. *cyber* rischio. Ma, a sua volta, questa decisione è funzione della differente declinazione che il plurivoco termine "*cyber* rischio" può assumere. Invero:

- se lo si guarda sotto il profilo "imprenditoriale", tale rischio riguarda qualunque tipo di impresa (e non, quindi, solo quelle "finanziarie")[8];
- viceversa, se lo si approccia sotto il profilo del rischio "sistemico", di rilievo prevalente per le istituzioni finanziarie, la prospettiva "*ex ante*", in funzione impeditiva di un'eventuale propagazione del rischio, diventa prevalente[9].

Tale differente concezione del rischio ha prodotto, tra i vari possibili[10], due differenti approcci regolatori negli USA e in Europa.

Per quanto riguarda gli Stati Uniti, il 26 luglio 2023, la *Securities and Exchange Commission* (di seguito, anche, "**SEC**") ha adottato la versione finale

[7] *Ibid*.

[8] Il rischio in questione, ad esempio, riguarda l'impresa a cui vengono sottratti i dati sensibili dei propri clienti, la quale subisce, quindi, un danno reputazionale, perde quote di mercato e si espone a contenziosi, ovvero, per altro verso, l'impresa che subisce un grave attacco informatico ed è costretta ad interrompere la produzione (con, tra le altre cose, effetti negative sulle vendite). In tale prospettiva, l'attacco informatico rileva come una sorta di "*material adverse event*" che può essere fronteggiato sia *ex ante*, sul piano organizzativo della singola impresa (ossia quello delle misure interne finalizzate a gestirlo), sia *ex post*, in prospettiva più di mercato (quantomeno per gli emittenti quotati), come informazione sensibile qualora l'incidente informatico effettivamente si realizzi.

[9] Richiamata la nozione di rischio sistemico di cui alla nota 4 *supra*, si osserva che il rischio in questione è quello, ad esempio, cui è esposta una banca che subisce un attacco informatico su larga scala, con fuga di dati, blocco dei sistemi, *etc*., con la conseguenza che tale attacco spaventa e/o spazientisce i correntisti, innescando pressanti richieste di rimborsi e provocando una c.d. *bank run* e con essa, persino, il collasso della banca stessa (che, appunto, se propagato ad altri istituti finanziari rischia di innescare l'effetto sistemico in questione). In questa prospettiva, come è stato notato in dottrina, il rischio cyber esula dalla tradizionale categoria del rischio operativo relativo alla singola istituzione finanziaria ed assume i tratti di una possibile minaccia alla fiducia nel funzionamento del sistema finanziario e quindi della sua stabilità. Cfr. A. PERRONE-I. GIRARDI, *op. cit*., 28.

[10] Vedasi, peraltro, in Italia, il disegno di legge n. 1717 approvato dalla Camera dei Deputati il 15 maggio 2024 recante "*disposizioni in materia di rafforzamento della cybersicurezza nazionale e reati informatici*", che enfatizza la prospettiva penalistica (apportando principalmente modifiche al codice penale e al codice di procedura penale).

delle *rules* su «*cybersecurity risk management, strategy, governance, and incident disclosure*» per le società quotate (di seguito, anche, "***Rules***" o "**SEC *Rules***")[11]. A tali *Rules*, come si dirà nel prosieguo, va necessariamente aggiunto il formante giurisprudenziale (pur in evoluzione), dato che, nei sistemi di *common law*, il *case law* può essere elevato, per certi versi, ad approccio regolatorio.

Dal punto di vista europeo, invece, la consapevolezza che il rischio *cyber* può rappresentare un rischio "strutturale" e sistemico si è tradotta, per quanto di interesse in questa sede[12], per tutti i soggetti "finanziari" rientranti nell'ambito di applicazione della disciplina, nell'emanazione, nel dicembre 2022, del Regolamento UE 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (di seguito, anche, "**DORA**")[13] che, a partire dalla sua entrata in vigore (prevista nel gennaio 2025), mira ad innalzare gli *standard* comuni di sicurezza informatica per tutto il settore finanziario, accentrando la vigilanza dei fornitori terzi di servizi critici TIC.

Ciò premesso, il presente contributo mira a fornire alcuni preliminari spunti di riflessione sulla questione del c.d. *cybersecurity risk management* dal punto di vista della regolamentazione americana ed europea nonché a cercare potenziali punti di contatto tra queste discipline, valutando anche se e quali elementi ciascun sistema legale potrebbe o dovrebbe prendere in considerazione dall'altro.

---

[11] Per un primo commento sulle *Rules* (seppur con riferimento alla proposta del 9 marzo 2022), v. G. SCHNEIDER, S*.E.C. Proposal: Cybersecurity Risk Management Rule*, in *Quaderni Assosim*, 2023, I, 41. V. anche P. CIOCCA, *op. cit*.

[12] Si osserva che tale consapevolezza si è anche dapprima tradotta con riguardo al settore bancario, nella pubblicazione, da parte dell'*European Banking Authority* (di seguito, anche, "**EBA**"), il 28 novembre 2019, degli "*Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (ICT) e di sicurezza*", a cui sono seguiti, nel novembre 2022, in Italia, significativi interventi sulla Circolare della Banca d'Italia n. 285/2013 (di seguito, anche, "**Circolare 285**"), volti a modificare il Capitolo 4 "*Il sistema informativo*" e il Capitolo 5 "*La continuità operativa*" del Titolo IV della Parte Prima.

[13] Come osservato (N. MICHIELI, *op. cit*., 10-11), le disposizioni del DORA si inseriscono in un tessuto normativo già articolato. Esse, infatti, sono state predisposte alla luce delle proposte già avanzate dall'*European Supervisory Authority* (ESA), dall'EBA, dall'*European Securities and Markets Authority* (ESMA) e dall'*European Insurance and Occupational Pensions Authority* (EIOPA). A livello europeo, le disposizioni del DORA si dovranno, inoltre, confrontare anche con le numerose altre disposizioni applicabili nei vari segmenti dei servizi finanziari oltre che, a livello nazionale, come visto, quantomeno con riferimento al comparto bancario, con la Circolare 285.

2. La disciplina statunitense: le SEC *Rules*. Come anticipato, negli Stati Uniti, il tema della cybersicurezza è affrontato nelle *Rules*, il cui testo finale adottato nel luglio 2023 è frutto dell'approvazione di una proposta presentata nel marzo 2022 dalla SEC[14], con cui quest'ultima intendeva riformare le alluvionali regole esistenti in materia di cybersicurezza, consapevole che le minacce e gli incidenti digitali si connotano per un crescente grado di rischiosità «*to public companies, investors, and market participants*»[15].

Per quanto qui d'interesse, in sintesi, le *Rules* richiedono agli emittenti quotati di:

(i) in primo luogo, comunicare tempestivamente (entro quattro giorni) ogni incidente cibernetico che ritengano, a loro giudizio, "*material*", descrivendone, da un lato, la natura, la portata e le tempistiche e, dall'altro lato, l'impatto attuale o prospettico sulle condizioni finanziarie e sull'operatività dell'emittente;

(ii) in secondo luogo, redigere un *report* con cadenza annuale per descrivere: (a) le procedure che gli emittenti abbiano eventualmente adottato per valutare, identificare e gestire i rischi "*material*" derivanti da minacce cibernetiche; e (b) l'attività di "supervisione" svolta dagli amministratori della società, nonché il loro ruolo ed esperienza nella gestione dei rischi derivanti dalle minacce cibernetiche;

(iii) in terzo luogo, inviare alla SEC delle comunicazioni periodiche (annuali) riguardo alla *disclosure* al mercato sugli incidenti cibernetici

[14] V. *supra*, nt. 6.

[15] La proposta, a sua volta, era frutto di orientamenti interpretativi emanati dalla SEC nel 2011 e 2018, ancora una volta alla luce dell'assenza di adeguate regole di settore, e mirava a consentire agli investitori di valutare adeguatamente l'esposizione degli emittenti quotati ai rischi legati alla cybersicurezza e ai relativi incidenti, nonché la loro abilità nel gestire e mitigare i suddetti rischi. Come osservato dal Chairman della SEC Gary Gensler nel comunicato stampa del 27 luglio 2023 «[w]*hether a company loses a factory in a fire – or millions of files in a cybersecurity incident – it may be material to investors* […] [c]*urrently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them*».

che gli emittenti divulghino in una giurisdizione estera.

Al riguardo, mentre è stato osservato che le nuove norme migliorano certamente la trasparenza sui rischi di cybersicurezza che possono causare impatti negativi sui mercati dei titoli (e, dunque, per tale ragione, rappresentano un elemento di interesse per la conoscenza degli investitori), le *Rules* – nell'ampia fase di consultazione – non sono andate esenti da critiche[16].

In ogni caso (e fermo restando quanto sopra), va osservato che le *Rules* si inscrivono armonicamente nel più ampio approccio della *securities regulation* nordamericana, ove non è presente, quantomeno a livello legislativo o regolamentare[17], un generale dovere di pronta diffusione della "*material non-public information*" (ossia un obbligo di informazione continua), ma gli obblighi di informazione gravanti sugli emittenti quotati presentano esclusivamente carattere periodico o episodico[18].

---

[16] È stato, infatti, obiettato che lo stringente frangente entro cui comunicare le informazioni dettagliate sull'attacco informatico potrebbe essere controproducente, posto che imporrebbe al *management*, in caso appunto di attacco informatico, di predisporre la documentazione da trasmettere alla SEC, rischiando di sviare l'attenzione rispetto alla reazione e risoluzione dell'incidente di cybersicurezza. Sotto altro versante, è stato rilevato che l'introduzione di obblighi di *disclosure* aggiuntivi, relativi agli aspetti di cybersicurezza, andrebbe ad alimentare la già voluminosa mole informativa messa a disposizione del pubblico, così risultando in un inefficiente *information overload* anche sul fronte della cybersicurezza. Per una sintesi delle questioni poste, v. anche G. SCHNEIDER, S*.E.C. Proposal*, cit., 41.

[17] Sul punto, v. S. GILOTTA, *Le società quotate e l'informazione societaria*, in *Il Testo Unico Finanziario*, Bologna, Zanichelli, 2020, 1470. La differenza, certamente significativa, non va, però, oltremodo enfatizzata in quanto obblighi di *disclosure* su base continua sono contenuti nelle *listing rules* delle più importanti borse nordamericane: il regolamento di borsa del *New York Stock Exchange* impone ad esempio alle società quotate sui propri listini l'obbligo di diffondere rapidamente al pubblico qualsiasi notizia o informazione che possa incidere significativamente sul mercato dei titoli della società (cfr., ad esempio, *NYSE Listed Company Manual*, 202.05). La giurisprudenza ha poi elaborato una serie di doveri complementari rispetto alle prescrizioni legislative e regolamentari, come ad esempio il dovere dell'emittente di aggiornare le proprie precedenti comunicazioni quando in ragione di fatti nuovi l'informazione in esse contenuta non risulti più accurata (c.d. *duty to update*), che avvicinano di molto, nei fatti, il sistema americano a quello europeo, riducendo gli spazi entro cui a una società quotata è consentito "tacere" in presenza di fatti nuovi rilevanti. V., *ex multis*, J.D. COX-R.W. HILLMAN-D.C. LANGEVOORT-A.M. LIPTON, *Securities Regulation. Cases and Materials*, New York, Aspen Publishing, 2021, 551 ss.

[18] Di converso, nell'Unione Europea il Regolamento (UE) n. 596/2014 (di seguito, anche, "**MAR**") impone agli emittenti di rendere pubbliche «*quanto prima possibile*» le "informazioni privilegiate" o "*price-sensitive*". Tale obbligo di pronta divulgazione delle informazioni è generalmente considerato un obbligo informativo "continuo", in quanto gli emittenti sono tenuti a comunicare al pubblico le informazioni privilegiate non appena si presentano e si distingue, pertanto, dagli obblighi di comunicazione a carattere "periodico" (*e.g*., le relazioni finanziarie di cui, in Italia, all'art. 154-*ter* del Testo Unico della Finanza) e da quelli a carattere "episodico" (*e.g*., fusioni o significativi mutamenti patrimoniali).

3. La disciplina europea: il DORA. Dal punto di vista europeo, a differenza degli Stati Uniti, ad oggi non sussiste alcuno specifico obbligo di *disclosure* dei rischi legati alla cybersicurezza e dei relativi incidenti per le società che abbiano subito un attacco cyber. Ciò – come si ritiene e come si dirà (v. par. 5.2 *infra*) – naturalmente nel presupposto che l'evento *cyber* non integri di per sé i requisiti per qualificare l'informazione come privilegiata; nel qual caso l'obbligo – ad esempio di predisporre un comunicato concernente l'avvenuto incidente informatico – continua ad essere presente anche in relazione ad informazioni od eventi legati alla cybersicurezza.

Dall'altro lato, però, come detto, sempre a differenza degli Stati Uniti, in Europa la consapevolezza che il rischio *cyber* può rappresentare un rischio "strutturale" negli attuali modelli di *business* e, quantomeno in alcuni settori, un rischio di potenziale impatto sistemico (non più relegabile, quindi, alla sola sfera dei rischi operativi) si è tradotta, per tutti i soggetti "finanziari" nel DORA.

Al riguardo, si osserva anzitutto che il DORA si applica a un ampio novero di operatori finanziari[19] e , oltre a contemplare un ampliamento del raggio e dell'incisività dei poteri di sorveglianza in materia di sistemi informatici, prevede – per quanto di interesse in questa sede – un rafforzamento delle responsabilità delle società finanziarie e, in particolare, dei corrispondenti organi gestori relativamente alla identificazione e gestione dei rischi informatici[20].

[19] Quali enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi, società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di rating del credito, amministratori di indici di riferimento critici, fornitori di servizi di *crowdfunding*, repertori di dati sulle cartolarizzazioni. Inoltre, il DORA si applica ai fornitori di servizi ICT. V. art. 2 DORA.

[20] In sintesi, le previsioni del DORA hanno ad oggetto: (i) il consolidamento dei compiti e delle responsabilità degli organi di gestione delle società finanziarie coinvolte, con particolare riguardo agli standard di sicurezza informatici e all'adattamento delle relative politiche di controllo; (ii) l'affidamento ad un organo di controllo indipendente delle responsabilità della gestione e sorveglianza dei rischi ICT, oltre alla possibilità di esternalizzare la funzione compliance in materia di gestione dei rischi informatici; (iii) il rafforzamento delle misure volte a garantire la continuità operativa dell'ente finanziario, mediante la predisposizione di analisi volte a prevedere gli impatti che eventuali gravi criticità nelle funzioni commerciali, nei processi di supporto, nelle dipendenze

L'obiettivo è quello di garantire condizioni di parità in punto di *governance* dei rischi tecnologici[21], dando diretta attuazione alle indicazioni delle autorità europee di vigilanza che avevano sottolineato la necessità di un superamento del quadro frammentario in materia di rischi TIC nel settore finanziario[22].

Di tal guisa, è sancito il principio della «*piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria*»[23], che comporta il «*costante coinvolgimento dell'organo di gestione a controllare il monitoraggio della gestione dei rischi informatici*»[24]. Ed infatti, il DORA, piuttosto che "relegare" la cybersicurezza a mero obbligo di *compliance*, assegna all'organo con funzione di supervisione strategica specifici doveri di conformazione dell'organizzazione societaria alla gestione dei rischi informatici. Il DORA si innesta quindi sul fondamentale assunto normativo che la cybersicurezza, intesa in senso lato come la «*sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie*»[25], sia materia di competenza – nel passaggio iniziale della definizione del quadro di gestione e di controllo interno, nel momento fisiologico della supervisione tecnologica, e da ultimo nell'eventualità patologica della responsabilità – del consiglio di amministrazione[26]. Il rischio ICT viene quindi gestito dall'organo

da terzi e/o nei patrimoni informativi individuati e censiti, nonché nelle loro interdipendenze possono avere sulle attività aziendali.

[21] V. G. SCHNEIDER, *IA, rischi d'impresa e le (mancate) risposte del diritto... DORA per tutti?*, in N. ABRIANI-R. COSTI (a cura di), *Diritto societario, digitalizzazione e intelligenza artificiale*, Milano, Giuffrè, 2023, 141.

[22] V. *supra*, nt. 13. Il DORA muove quindi da una definizione di «*rischi informatici*» molto ampia per tali intendendosi «*qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale o fisico*» (Art. 3, n. 5, DORA).

[23] Considerando 46 DORA.

[24] Considerando 45 DORA.

[25] Art. 3(5) DORA.

[26] G. SCHNEIDER, *La resilienza*, cit., 566. Il consiglio di amministrazione si assume così «*la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria*» (cfr. art. 4 DORA) e deve adempiere a specifici doveri organizzativi e informativi in materia di resilienza operativa digitale. Questi doveri si riflettono a loro volta in un più generale dovere di intervento da parte dei componenti dell'organo amministrativo rispetto alle infrastrutture tecnologiche impiegate, che vengono ora incluse nel fulcro delle strategie di *governance* dell'impresa finanziaria. È il consiglio di amministrazione ad avere infatti il compito di definire politiche «*miranti a garantire il*

amministrativo al pari di tutti gli altri rischi di impresa che le entità finanziarie sono solite prevenire, monitorare o gestire (rischio di liquidità, di integrità del capitale etc.).

In tale prospettiva, per quanto di interesse, è prevista la necessità di dotarsi di un processo di gestione degli incidenti connessi alle tecnologie informatiche che deve assicurare «*la segnalazione agli alti dirigenti interessati almeno degli incidenti gravi connessi alle TIC*» nonché informare «*l'organo di gestione almeno in merito a detti incidenti, illustrandone l'impatto e la risposta e i controlli supplementari da introdurre*»[27].

Così, come parte dell'approccio regolatorio, il Regolamento richiede all'organo gestorio di istituire appositi canali di comunicazione con i ruoli competenti per l'IT ed è previsto – in termini di *reporting* verso l'organo amministrativo – un obbligo di segnalazione e di informativa: (i) in merito alle risultanze dei *test* sulla resilienza operativa digitale[28], e (ii) degli incidenti gravi connessi alle tecnologie, nonché dell'impatto di questi, della risposta e dei controlli supplementari da introdurre[29].

4. Un confronto tra i due approcci regolatori *de jure condito*. Richiamato, per i fini che qui interessano, il contenuto, da un lato, delle *Rules* e, dall'altro lato, del DORA, può essere utile confrontare i due approcci regolatori, ponendo fin da subito l'attenzione – in logica di giustapposizione – sulla circostanza che la disciplina europea, a differenza delle *Rules*, non affronta il

mantenimento di standard elevati di disponibilità, autenticità integrità e riservatezza dei dati» (cfr. art. 5, co. 2, lett. *b*), DORA).

[27] Art. 17, co. 3, lett. *e*), DORA.

[28] In questo caso l'obbligo è a carico del personale di grado più elevato addetto all'IT.

[29] Al riguardo, gli assetti informativi così configurati mirano a garantire che gli amministratori siano adeguatamente informati in materia di sicurezza informatica in conformità al precetto generale di cui all'art. 2381, co. 5, c.c. (ai sensi del quale «[g]*li organi delegati curano che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa e riferiscono al consiglio di amministrazione e al collegio sindacale, con la periodicità fissata dallo statuto e in ogni caso almeno ogni sei mesi, sul generale andamento della gestione e sulla sua prevedibile evoluzione nonché sulle operazioni di maggior rilievo, per le loro dimensioni o caratteristiche, effettuate dalla società e dalle sue controllate*»), che nel Regolamento DORA viene declinato come un vero e proprio dovere di vigilare sulla *governance* dei dati e, più in generale, degli strumenti tecnologici impiegati. Cfr. G. SCHNEIDER, *La resilienza*, cit., 571.

tema della *market disclosure*, mentre reca disposizioni in materia di *governance* dei rischi cibernetici, con particolare attenzione sul ruolo dell'organo di gestione delle società finanziarie.

Nello specifico, in USA, alla luce dell'obbligo di *disclosure* posto dalle *Rules* (il quale, però, beninteso non è concepito solo come *disclosure* "ad evento", ma anche come *reporting* a cadenza annuale), la prospettiva appare essere incentrata su un profilo di informativa al mercato. Di converso, in Europa la regolamentazione affronta il medesimo tema della cybersicurezza dal punto di vista dell'assetto di *governance* interno – seppur di soggetti giuridici per così dire "qualificati" (e, peraltro, attraverso un approccio "orizzontale", ossia indipendentemente dall'attività svolta nello specifico e dal tipo di tecnologia impiegata) come le società finanziarie[30] – incidendo su tasselli essenziali della dimensione endosocietaria degli stessi, quali il dovere di istituzione di assetti adeguati, il dovere di agire informato nonché le competenze dell'organo amministrativo[31].

In altri termini, le *Rules* sono volte a rendere gli investitori (e, più diffusamente, gli *stakeholders*) edotti (e, dunque, a metterli nelle condizioni di giudicare consapevolmente) della capacità delle aziende di gestire le crescenti minacce informatiche e di quanto tali minacce impattano sulla redditività dell'azienda (ossia, in definitiva, sul rendimento dei loro investimenti). La regolamentazione europea, invece, elegge la *governance* societaria quale sede più effettiva di presidio dei rischi tecnologici da cui viene a dipendere la resilienza operativa delle società finanziarie e, di riflesso, la stabilità e l'integrità del sistema finanziario nell'era digitale[32].

Dunque, il rischio cibernetico nella prospettiva degli Stati Uniti è affrontato – verso l'esterno – in termini di *disclosure* al pubblico delle informazioni, mentre in Europa viene "endosocietarizzato" (quantomeno per le istituzioni finanziarie) – nella dimensione, appunto, interna – nel contesto più ampio degli obblighi

[30] Come definite nell'art. 2, co. 1, DORA.
[31] G. SCHNEIDER, *La resilienza*, cit., 559.
[32] *Ibid*., 563.

dell'organo di gestione di predisposizione di assetti adeguati[33].

Tale differenza di approccio rispecchia anche la differente *ratio* e nomogenesi delle due discipline.

Invero, soffermando l'analisi nello specifico sul DORA – che non si rivolge agli emittenti quotati – il regolatore europeo ha inteso fare della materia della cybersicurezza autonomo oggetto di regolazione settoriale – insieme, per quanto si tratta di iniziative tra loro eterogenee, alla disciplina sulle cripto-attività contenuta nel Regolamento MICA[34] e alla definizione di un quadro normativo sulle infrastrutture di mercato basate sulla tecnologia di registro distribuito cristallizzato nel c.d. Regime Pilota[35] – nell'ambito della Strategia per la finanza digitale[36]. Ciò in quanto, come era già stato messo in luce nel 2020 dal Comitato europeo per il rischio sistemico (CERS), l'elevato livello di interconnessione tra entità finanziarie, mercati finanziari e infrastrutture del mercato finanziario, e in particolare l'interdipendenza dei rispettivi sistemi TIC, può costituire una potenziale vulnerabilità sistemica, dal momento che incidenti informatici localizzati possono rapidamente diffondersi da una qualunque delle numerose entità finanziarie dell'Unione all'intero sistema finanziario, senza trovare alcun ostacolo nelle frontiere geografiche[37].

Di converso, negli Stati Uniti, le *Rules* si applicano agli emittenti quotati in

[33] Si esprime nel senso di una "necessità" di una lettura "societaria" dei rischi informatici all'interno del DORA, EAD., *op. ult. cit.*, 559.

[34] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

[35] Regolamento UE 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i Regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE, 2 giugno 2022, OJ L 151/1.

[36] Per una panoramica generale sul contesto della Strategia per la finanza digitale, v. V. FALCE-M. RABITTI-A. SCIARRONE ALIBRANDI-M. SIRI-F. ANNUNZIATA, in F. DONATI-A. PAJNO-A. PERRUCCI (a cura di), *Le decisioni automatizzate in materia finanziaria: una ricognizione*, in *La rivoluzione dell'intelligenza artificiale: profili giuridici*, Bologna, Il Mulino, 2022, vol. 3, 397 ss.

[37] In tale prospettiva, il rischio sistemico sussisterebbe in quanto «[g]*ravi violazioni delle TIC che si verifichino nel settore finanziario non si limitano a colpire entità finanziarie isolate, bensì spianano anche la strada alla propagazione di vulnerabilità localizzate attraverso tutti i canali di trasmissione finanziaria e possono provocare conseguenze avverse per la stabilità del sistema finanziario dell'Unione, dando luogo ad esempio a pressanti richieste di rimborsi e a una generale perdita di fiducia nei mercati finanziari*» (Considerando 3 DORA).

generale, a prescindere dal settore di appartenenza (e, quindi, non necessariamente agli operatori finanziari) e la prospettiva, come detto, è sulla *disclosure*: il rischio, anche in questi termini, potrebbe pure essere percepito come sistemico, ma la *disclosure*, piuttosto che l'adozione di adeguati assetti di *governance*, rappresenterebbe il miglior rimedio avverso tale rischio e, più in generale, il miglior strumento di tutela degli investitori e di efficienza del mercato finanziario.

Ed infatti, ancora sotto altro profilo, come accennato in premessa, si può ritenere che negli Stati Uniti il rischio cibernetico sia da inquadrare come una componente del rischio di impresa, che si riflette dunque sulla formazione dei prezzi di mercato: di qui gli specifici obblighi di *disclosure*, senza peraltro indicazione di una specifica modalità di governo del rischio cibernetico (in quanto rientrante nel *business judgment* degli amministratori). In Europa, di converso, il rischio cibernetico è visto come fattore fondamentale di efficienza (o inefficienza) della infrastruttura del mercato finanziario (ed infatti il DORA si applica solo agli operatori del mercato finanziario ed incide direttamente sugli assetti di governo di tali soggetti regolamentati): l'impressione è quindi che si voglia governare il rischio cibernetico per evitare che il funzionamento del mercato finanziario possa risentirne.

5. Ulteriori riflessioni comparatistiche *de jure condendo*: la situazione in Europa e negli Stati Uniti. Preso atto del differente approccio regolatorio, può valer la pena riflettere, ad esempio, se, a livello europeo, possa essere opportuno: (i) estendere la disciplina del DORA anche agli emittenti quotati; e/o (ii) introdurre degli obblighi di *disclosure* (soprattutto in caso di attacco informatico) equivalenti a quelli posti dalle *Rules*.

Circa il primo punto, considerata la pervasiva rilevanza del tema della cybersicurezza, un'estensione degli obblighi endosocietari di cui al DORA anche agli emittenti quotati può apparire, anche sulla scia della nascente dottrina sul

punto[38], opportuna nella logica (cui si è fatto cenno) di "responsabilizzazione" dell'organo con funzione di supervisione strategica.

Ed infatti, nel momento in cui l'impresa si integra con l'infrastruttura tecnologica, quest'ultima diviene rischio autonomo d'impresa che deve essere adeguatamente valutato e governato dall'organo amministrativo e misurato in base alle norme generali in materia societaria[39].

In tale prospettiva, come si dirà approcciando il secondo punto, la già attuale esistenza di un obbligo di *disclosure* (anche nel sistema europeo) in caso di attacco informatico per così dire "*price-sensitive*" potrebbe non essere di per sé sufficiente a "gestire" il rischio cibernetico se l'impresa non integra anche un sistema di *governance* che – attraverso altresì i flussi informativi tra le funzioni e l'organo di gestione – sia in grado di valutare adeguatamente il rischio e governarlo, anzitutto a livello endosocietario.

Dall'altro lato, occorre osservare che, mentre, come detto, gli sforzi sino ad oggi profusi in tema di sicurezza informatica e di informativa guardano per lo più al settore bancario e finanziario, non si può negare che la cybersicurezza acquisti un'ulteriore valenza se letta e coordinata con gli ultimi interventi relativi agli obblighi di adeguatezza degli assetti organizzativi amministrativi e contabili che il nuovo art. 2086, co. 2, c.c.[40] impone agli amministratori di tutte le società, senza alcun distinguo tra quotate e non quotate, di capitali piuttosto che di persone, e persino imprese individuali[41]. Ciò con evidenti implicazioni a livello di *policy* per l'Unione Europea, che dovrebbe essere allora volta a strutturare un (nuovo)

[38] Ci si riferisce alla dottrina che si è interrogata sull'impatto delle nuove tecnologie sul funzionamento societario sotto il profilo dei doveri degli amministratori (e non solo quindi per quanto attiene alle opportunità di *governance*). V., *ex multis*, N. ABRIANI-G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, Il Mulino, 2021, 191 ss.; C. PICCIAU, *The (Un)Predictable Impact of Technology on Corporate Governance, in Hast. Bus. L. J.*, 2021, 17, 67 ss.; A. SACCO GINEVRI, *Ancora su intelligenza artificiale e* corporate governance*, in Riv. trim. dir. econ.*, 2021, 3, 343 ss.

[39] V. G. SCHNEIDER, *La resilienza*, cit., 565, nonché N. ABRIANI-G. SCHNEIDER, *op. cit*., 235.

[40] Ai sensi del quale «[l]*'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale, nonché di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuità aziendale*».

[41] V. N. MICHIELI, *op. cit.*, 9.

paradigma generale (ed europeo) in tema di adeguati assetti organizzativi.

E, in tale prospettiva, ci si è interrogati (rispondendo in senso positivo), con riferimento alle previsioni sulla cybersicurezza di cui alla Circolare 285 (ma con conclusioni estendibili, ad avviso di chi scrive, al DORA), sull'opportunità di rendere tali principi «*un paradigma trasferibile, se del caso, anche alle società finanziarie semplici, ovvero a società quotate o persino non quotate, secondo le rispettive esigenze*»[42]. Ciò proprio «*in considerazione della fisiologicità del rischio* cyber *che, a sua volta, può divenire rischio operativo in qualsiasi tipo sociale e rispetto a società che possono svolgere qualsivoglia attività di impresa*»[43].

Del resto, parrebbe già delinearsi un *trend* in tale direzione nei nuovi Principi G20/OCSE di *corporate governance* approvati dal G20 nel settembre 2023[44].

Tali Principi, infatti, per i fini che qui interessano, intervengono in una duplice dimensione, attraverso l'integrazione dei rischi informatici nel più ampio quadro dei processi di gestione del rischio societario[45]: in primo luogo, si riconducono i rischi di sicurezza digitale tra quelli che devono essere oggetto di *reporting* finanziario, insieme a quelli di sostenibilità[46]; in secondo luogo si attribuisce la

[42] *Ibid*. Ciò quantomeno per le società quotate, con riferimento alle quali l'Autrice osserva che l'apertura al mercato incide anche sulla necessità di approntare maggiori tutele. Tuttavia, anche le società di piccole dimensioni e non quotate non potranno prescindere dal predisporre un'organizzazione interna capace di prevenire, ove possibile, e gestire tempestivamente questo tipo di rischi nell'ottica di tutelare, tra gli altri, l'operatività stessa della società (che un attacco cyber potrebbe mettere a rischio).

[43] *Ibid*. Osserva poi l'Autrice come, con riferimento alle società quotate, le funzioni in tema di gestione dei rischi ICT potrebbero trovare (e ciò sarebbe addirittura auspicabile) una loro naturale collocazione e devoluzione all'interno di un comitato endoconsiliare, anche appositamente costituito, ovvero all'interno del comitato quale quello di controllo e rischi ovvero potrebbero essere assegnate ad una funzione di *risk management*.

[44] OECD (2023), *G20/OECD Principles of Corporate Governance 2023*, OECD Publishing, Parigi, disponibile *online* all'indirizzo: https://doi.org/10.1787/ed750b30-en. V. anche la guida pubblicata dall'Assonime recante un'analisi dell'attuazione dei nuovi Principi G20/OSCE, disponibile *online* all'indirizzo:
https://www.assonime.it/_layouts/15/Assonime.CustomAction/GetPdfToUrl.aspx?PathPdf=https://www.assonime.it/attivita-editoriale/studi/Documents/Note%20e%20Studi%202-2024%20rev.pdf.

[45] Sul punto, v. anche G. SCHNEIDER, *La resilienza*, cit., 579.

[46] Rileva, sotto tale profilo, il principio IV.A.8. ai sensi del quale «*Users of financial information and market participants need information on reasonably foreseeable material risks that may include: risks that are specific to the industry or the geographical areas in which the company operates; dependence on commodities and supply chains; financial market risks including interest rate or currency risk; risks related to derivatives and off-balance sheet transactions; business conduct risks; digital security risks; compliance risks; and sustainability risks, notably climate-related risks*». Sul *reporting* finanziario e non finanziario, v., *ex multis*, E. DELLAROSA, ***Cosa c'è***

gestione della responsabilità di tali rischi al consiglio di amministrazione[47] (se del caso anche tramite l'istituzione di un comitato tecnologico con funzioni di *advisory* all'esecutivo sulla gestione della sicurezza cibernetica e, più in generale, sui processi di trasformazione tecnologica d'impresa)[48].

Circa il secondo punto, per valutare se sia opportuno introdurre in Europa degli obblighi equivalenti a quelli discendenti dalle *Rules*, occorre ragionare se la *disclosure* immediata, prevista dalle *Rules*, (i) sia necessaria solo in quanto si tratti di un incidente di natura cibernetica; ovvero (ii) sia rilevante in quanto informazione *price-sensitive* (e, quindi, soggetta alla tipica forma di *disclosure* per le informazioni privilegiate di carattere episodico)[49].

Gli aspetti possono essere esaminati congiuntamente.

Ed infatti, sotto il primo profilo, come detto, ad oggi, non esiste un obbligo per la società che abbia subito un attacco *cyber* di darne immediata comunicazione (o entro un certo periodo) dal momento in cui ne abbia avuto conoscenza[50]. Tuttavia, non pare che l'evento cibernetico possa richiedere, in quanto tale, un'autonoma *disclosure*, in assenza di alcun requisito ulteriore (perlomeno in termini di "materialità"[51]) atto a circoscrivere una diffusione

---

dietro la «G» di Esg: una nuova governance *bancaria per la sostenibilità*, in *Bancaria*, 2023, 5 ss.; M. L. PASSADOR, *Sull'utilità della* ESG disclosure *e sul ruolo dei comitati rischi e sostenibilità*, in *Banca, impresa, società*, 2023, 1 ss.; M. RESCIGNO, *L'evoluzione e il ruolo dell'informazione non finanziaria fra doveri informativi e obblighi gestori*, in *Rivista ODC*, 2023, 3 ss.

[47] Rileva, sotto tale profilo, il principio V.D.2. ai sensi del quale «[o]*f notable importance is the management of digital security risks, which are dynamic and can change rapidly. Risks may relate, among other matters, to data security and privacy, the handling of cloud solutions, authentication methods, and security safeguards for remote personnel working on external networks. As with other risks, these risks should be integrated more broadly within the overall cyclical company risk management framework*».

[48] Rileva, sotto tale profilo, il principio IV.E.2. ai sensi del quale «[s]*ome boards have also established a committee to advise on the management of digital security risks as well as on the company's digital transformation. Ad hoc or special committees can also be temporarily set up to respond to specific needs or corporate transactions*».

[49] La definizione di informazione privilegiata è contenuta nell'art. 7, par. 1, MAR, che definisce l'informazione privilegiata come «*un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati*».

[50] Sul punto v. anche N. MICHIELI, *op. cit.*, 5.

[51] Quanto al requisito della "*materialità*", per «*informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi degli strumenti finanziari* […]" (art. 7, par. 1, lett. *b*) MAR) si intende "*un'informazione che un investitore ragionevole probabilmente*

"incontrollata" (col rischio di rivelarsi perfino contraddittoria) di siffatte notizie[52].

Ed allora, muovendo al secondo profilo, è da ritenere che la *disclosure* immediata prevista dalle *Rules* sia da inquadrare, in Europa, nella fattispecie, già esistente, delle informazioni *price-sensitive* episodiche: a quel punto nulla dovrebbe cambiare rispetto al dovere – già presente nell'ordinamento comunitario – di pronta *disclosure* applicabile a qualunque informazione privilegiata[53]. In altri termini, posto che in Europa esiste un dovere di pronta diffusione delle informazioni privilegiate, il verificarsi di un incidente cibernetico potrebbe già rientrare in tale fattispecie, a patto naturalmente che lo stesso superi la soglia di materialità tale da qualificarlo come informazione *price-sensitive*.

Del resto, negli Stati Uniti, le *Rules* stesse prevedono che la valutazione sulla rilevanza dell'incidente debba avvenire senza ritardo affinché questo sia poi comunicato alla SEC entro i successivi quattro giorni lavorativi e che la comunicazione possa essere dilazionata solo laddove il Procuratore Generale degli Stati Uniti stabilisca che una *disclosure* immediata causerebbe un rischio sostanziale alla sicurezza nazionale.

Si tratta, a ben vedere, di una prospettiva funzionalmente non così dissimile da quella alla base dell'istituto del "ritardo" (nella diffusione delle informazioni) per la gestione delle informazioni *price-sensitive* prevista dal MAR[54]. Per quanto, si

---

utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento» (art. 7, par. 12, MAR).

[52] Altro problema, che dovrebbe essere risolto, è invece quello della tempistica della comunicazione dell'evento (che impatterà inevitabilmente sul valore del titolo e sul mercato) ovvero dell'individuazione del momento in cui rendere pubblico l'attacco informatico, spesso posticipato al fine di ritardare anche il danno reputazionale con una perdita di valore del titolo. V. N. MICHIELI, *op. cit*., 4.

[53] Dovere secondo cui l'emittente deve comunicare al pubblico, «*quanto prima possibile*», le informazioni privilegiate che riguardano direttamente detto emittente (art. 17, par. 1, MAR).

[54] Se infatti l'emittente, come detto, deve comunicare al pubblico quanto prima possibile, le informazioni privilegiate che lo riguardano, la disciplina MAR consente – a determinate condizioni – di ritardare la pubblicazione dell'informazione privilegiata. In particolare, ai sensi dell'art. 17, par. 4, MAR e in conformità alle Linee Guida "*Delay in the disclosure of inside information*" pubblicate dall'ESMA, è possibile ritardare la pubblicazione di un'informazione privilegiata in presenza delle seguenti condizioni: (i) l'immediata comunicazione pregiudicherebbe probabilmente i legittimi interessi dell'emittente; (ii) il ritardo nella comunicazione probabilmente non avrebbe l'effetto di fuorviare il pubblico; (iii) l'emittente è in grado di garantire la riservatezza dell'informazione privilegiata. Qualora il presupposto che ha giustificato il ritardo della pubblicazione dell'informazione venga meno, l'emittente deve tempestivamente pubblicare

potrebbe osservare, nell'Unione Europa il ritardo, con l'eccezione delle regole speciali previste per le istituzioni finanziarie, è strumentale alla tutela di interessi privati (ossia quello della società emittente a non subire il danno derivante dalla prematura diffusione dell'informazione); negli USA, al contrario, il "ritardo" in questione (se così si può definire) ha invece alla base la tutela di un interesse pubblico e quindi, pare, avere un ambito di applicazione ben più limitato di quello europeo.

Da una prospettiva opposta, interrogandosi sull'estensione agli Stati Uniti degli obblighi "in stile DORA" (oltre che naturalmente alle società finanziarie) nei confronti degli emittenti quotati, si può osservare che, mentre ad oggi in quell'ordinamento non esiste, in materia di *cybersecurity*, tanto sul piano normativo quanto in termini di *case law* specifico, un vero e proprio dovere degli amministratori di adozione di sistemi di monitoraggio e *reporting* dei rischi cibernetici al fine dell'assolvimento del dovere di agire informati, la giurisprudenza recente sembra nondimeno propendere verso la necessità di ricollegare al mancato monitoraggio sui sistemi informatici una violazione dei doveri fiduciari degli amministratori nell'ambito dei c.d. "*Caremark claims*"[55].

Al riguardo, nel caso *Caremark*[56], nel 1996, la *Court of Chancery* del

---

l'informazione privilegiata, comunicando subito dopo all'Autorità di vigilanza la motivazione che ha giustificato il ritardo della pubblicazione.

[55] Sul punto, v., da ultimo, H. J. PACE-L. J. TRAUTMAN, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, in *Wisc. L. Rev.*, 2022, 888 ss. La dottrina d'oltreoceano ha del resto ormai esteso le aree che sono comprese nell'acronimo ESG includendovi, nella parte relativa alla *governance*, anche la *cybersecurity* (in linea, peraltro, con l'approccio seguito nel presente contributo).

[56] *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996). Per una completa ricostruzione del caso *Caremark*, v. A. MORINI, *«*Good Faith*», buona fede: verso "nuovi doveri" degli amministratori di s.p.a.?*, in *Riv. dir. soc.*, 2011, *passim*. In estrema sintesi, nelle parole di H. J. PACE-L. J. TRAUTMAN, *op. cit.*, 889, «[u]*nder what has come to be known as a Caremark claim, corporate directors who fail to provide adequate oversight may be held liable for breaching fiduciary duties they owed the corporation. Caremark claims typically arise where corporate employees caused the corporation to engage in some unlawful conduct, and plaintiffs allege the unlawful conduct would not have taken place had directors acted properly. There are two types of Caremark claims: failure to implement ("Type I") claims and failure to monitor ("Type II") claims. Under a Type I claim, the plaintiff alleges that «the directors utterly failed to implement any reporting or information system or controls.» Under a Type II claim, the plaintiff alleges that although the board implemented controls, it «consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.» Conscious disregard is necessary; Caremark is a high bar*.».

Delaware ha riconosciuto la funzione di monitoraggio del consiglio di amministrazione quale attività strumentale e necessaria all'adempimento dei doveri fiduciari che su quest'ultimo gravano[57]. In sostanza, tale decisione ha dato avvio al processo di costruzione del sistema della *compliance*, da intendersi – nel contesto qui in esame – come verifica della legalità sostanziale dell'agire amministrativo[58].

Ventitré anni dopo, nel caso *Marchand v. Barnhill*[59], pur se non con riferimento al monitoraggio dei rischi cibernetici, la Corte Suprema del Delaware ha ravvisato – sotto la forma di un *Caremark claim* – una violazione dei doveri fiduciari degli amministratori per non avere predisposto un'adeguata struttura di *reporting*, tale da consentire al consiglio di essere informato su alcuni problemi di sicurezza con riferimento all'industria alimentare. Ai fini dell'individuazione della responsabilità del *board*, la Corte ha sottolineato la mancata predisposizione da parte di quest'ultimo di un sistema di informazione e monitoraggio ragionevolmente esigibile dallo stesso secondo il canone di buona fede.

In questi termini, la sentenza sembra aprire il varco a un sindacato giudiziale dell'adeguatezza dei sistemi di *monitoring*, suscettibile di valorizzare anche gli *standard* tecnologici invalsi sul mercato[60].

In altri termini, a seguito di *Marchand v. Barnhill* e del filone giurisprudenziale che pare essersi sviluppato a partire da tale decisione[61], «[t]*he*

---

[57] Cfr. A. MORINI-B. CASTELLINI, *ESG: impatto sulla governance societaria ed i doveri degli amministratori*, in *Atti del XIV Convegno nazionale ODC "Imprese, mercati e sostenibilità: nuove sfide per il Diritto commerciale"*, 9.

[58] Sul punto (e sull'inquadramento sistematico di *Caremark* e del successivo *case law*), v. A. MORINI, *op. cit*., *passim* nonché sia consentito rinviare a M. COLUZZI, *Responsabilità degli amministratori e diritto di ispezione del socio. Nota a margine del caso* Yahoo, in *Riv. dir. soc.*, 2018, 42 ss.

[59] *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019). Per un primo commento, v. N. ABRIANI-G. SCHNEIDER, *op. cit*. 155, nonché G. SCHNEIDER, *La resilienza*, cit., 573.

[60] N. ABRIANI-G. SCHNEIDER, Corporate governance *'compositiva', metodi computazionali e assetti adeguati: i riflessi sui controlli*, in *Atti del XV Convegno nazionale ODC "Impresa e mercati: numeri e* computer science*"*, 26.

[61] A *Marchand v. Barnhill* sono seguiti, tra i vari, almeno i seguenti quattro casi relativi ai *Caremark claims* che hanno trovato accoglimento: (i) nel caso *Clovis* (*In re Clovis Oncology, Inc. Deriv. Litig.,* No. 2017-0222-JRS, 2019 WL 4850188 (Del. Ch. Oct. 1, 2019), la *Court of Chancery* del Delaware ha riconosciuto un *Caremark claim* avverso gli amministratori di una società farmaceutica che avevano ignorato dei segnali d'allarme che indicavano come il *management* stesse riportando risultati inaccurati sui test clinici per uno dei farmaci dell'azienda in fase di

newly increased risk of Caremark liability drastically changes the landscape for potential liability because failure to properly monitor cybersecurity can violate the [*fiduciary duties*]»[62].

Sulla base di tali considerazioni, si può cominciare a vedere in filigrana che il modello europeo e quello americano potrebbero non risultare, nei fatti, così dissimili, in quanto il *case law* americano affronta la questione del *cybersecurity risk management* in sostanza nella prospettiva della *corporate governance* "in stile DORA" (e, quindi, in fin dei conti, con *focus* sugli assetti adeguati). Certamente, però, non si può negare nemmeno che sussistono comunque rilevanti margini di differenziazione tra i due sistemi, poiché il filone giurisprudenziale in questione (in ogni caso in divenire) si riferisce alla *corporation* in generale (e, dunque, non specificamente alle società "finanziarie") e non è – per la differente concezione, cui si è fatto cenno, che il cyberischio assume nei due ordinamenti – da inquadrare quale "rimedio" al rischio sistemico.

Se, pertanto, appare esservi un *trend* che – in prima approssimazione e con le precisazioni di cui sopra – potrebbe addirittura far ritenere che l'ordinamento

sperimentazione; (ii) nel caso *Hughes* (*Hughes v. Hu*, No. 2019-0112-JTL, 2019 WL 1987029 (Del. Ch. Apr. 27, 2020), la *Court of Chancery* del Delaware ha riconosciuto un *Caremark claim* avverso gli amministratori di una società cinese rilevando come le carenze nei controlli interni sul *reporting* finanziario avessero portato il *Board* a risultare inadempiente ai propri compiti di supervisione sul sistema di controlli contabili della società; (iii) nel caso *Chou* (*Teamsters Local 443 Health Servs. & Insur. Pian v. Chou*, No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. Aug. 24, 2020), la *Court of Chancery* del Delaware ha riconosciuto un *Caremark claim* avverso gli amministratori di una grande azienda farmaceutica che avevano ignorato dei segnali d'allarme e favorito così la presenza di un sistema di *reporting* assolutamente inadeguato rispetto al modello di *business* di una società controllata; (iv) nel caso *Boeing* (*In re The Boeing Co*. *Deriv. Litig*., No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021), la *Court of Chancery* del Delaware ha riconosciuto un *Caremark claim* avverso gli amministratori di una società produttrice di aerei per non aver posto in essere un sistema di *reporting* adeguato con riguardo a questioni inerenti alla sicurezza degli aerei, a cui erano seguiti a due incidenti.

[62] H. J. PACE-L. J. TRAUTMAN, *op. cit*., 894. Gli Autori proseguono, poi (938 ss.), con un'analisi volta ad individuare, mutuando i principi di *Marchand v. Barnhill* e applicandoli alla cybersicurezza, una serie di azioni per il *board* per andare esente da resposabilità in materia di cybersicurezza, rilevando che: (i) «*A board committee should either be devoted entirely to cybersecurity or have cybersecurity as a significant part of its portfolio*»; (ii) «*Protocols should be set to require management to regularly update the board on cybersecurity compliance practices, risks, or reports*»; (iii) *The board must discuss cybersecurity on a regular basis*»; (iv) "*Red flags should be reported up to the board*»; (v) «*Board reports on cybersecurity must include both favorable information and unfavorable information*»; (vi) «*The board should make use of third-party monitors, auditors, or consultants*»; (vii) «*Board minutes should reflect the above*»*; (viii)* «*Compliance with prophylactic government regulations alone is not enough*».

americano (beninteso, solo sul piano del *case law*) stia già andando nella direzione europea, ciò resta soggetto ad un importante *caveat* in merito alla declinazione che ne comporta l'applicazione alle società quotate. Infatti, l'eventuale esportazione del modello europeo in relazione agli emittenti quotati (e, quindi, per via normativa e/o regolamentare, probabilmente federale), incidendo su aspetti di *governance* interna delle società, andrebbe a toccare un ambito tradizionalmente appannaggio, negli Stati Uniti, della legislazione statale, sempre guardinga ad intervenire in merito a sfere tipicamente oggetto di disciplina pattizia tra i soci. Di tal guisa, si riproporrebbe la nota dialettica tra *Washington* (*i.e.* legislatore federale) e *Delaware* (quale "campione" della disciplina statale), deviando tuttavia dal *pattern* che si è ormai consolidato in quell'ordinamento secondo cui solo eccezionalmente – e tipicamente a seguito di momenti di crisi – il legislatore federale "invade" il campo di quello statale in materia, direttamente o indirettamente, rientrante negli *interna corporis* societari[63].

BIBLIOGRAFIA

N. ABRIANI-G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, Il Mulino, 2021

N. ABRIANI-G. SCHNEIDER, Corporate governance *'compositiva', metodi computazionali e assetti adeguati: i riflessi sui controlli*, in *Atti del XV Convegno nazionale ODC "Impresa e mercati: numeri e* computer science*"*

P. CIOCCA, *Workshop Università Cattolica del Sacro Cuore e Consob «Cyber Security, Market Disclosure & Industry». Intervento del Commissario Consob Paolo Ciocca*, 27 febbraio 2023

M. COLUZZI, *Responsabilità degli amministratori e diritto di ispezione del socio. Nota a margine del caso* Yahoo, in *Riv. dir. soc.*, 2018

J.D. COX-R.W. HILLMAN-D.C. LANGEVOORT-A.M. LIPTON, *Securities Regulation. Cases and Materials*, New York, Aspen Publishing, 2021

E. DELLAROSA, *Cosa c'è dietro la «G» di Esg: una nuova* governance *bancaria per la sostenibilità*, in *Bancaria*, 2023

V. FALCE-M. RABITTI-A. SCIARRONE ALIBRANDI-M. SIRI-F. ANNUNZIATA, in F. DONATI-A. PAJNO-A. PERRUCCI (a cura di), *Le decisioni automatizzate in materia finanziaria: una ricognizione*, in *La rivoluzione dell'intelligenza artificiale: profili giuridici*, Bologna, Il Mulino, 2022, vol. 3

S. GILOTTA, *Le società quotate e l'informazione societaria*, in *Il Testo Unico Finanziario*, Bologna, Zanichelli, 2020

[63] Ad es., solo per citarne alcuni, il *Securities Act* e il *Securities Exchange Act*, successivi allo *shock* borsistico del 1929; il *Williams Act*, successivo agli abusi delle OPA sotto forma di c.d. *cash tender offer – sub specie* dei c.d. *Saturday night specials* – degli anni '60; il *Sarbanes Oxley Act*, successivo agli scandali *Enron*, *Arthur Andersen* e *WorldCom* a cavallo dei due millenni; il *Dodd-Frank Act*, successivo alla grande recessione conseguente allo scoppio della bolla immobiliare, nota come crisi dei mutui *subprime*.

N. MICHIELI, *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in *Banca, impresa, società*, 2024
A. MORINI, «Good Faith*», buona fede: verso "nuovi doveri" degli amministratori di s.p.a.?*, in *Riv. dir. soc.*, 2011
A. MORINI-B. CASTELLINI, *ESG: impatto sulla governance societaria ed i doveri degli amministratori*, in *Atti del XIV Convegno nazionale ODC "Imprese, mercati e sostenibilità: nuove sfide per il Diritto commerciale"*
OECD, *OECD Policy Framework on Digital security: Cybersecurity for Prosperity*, dicembre 2022
OECD (2023), *G20/OECD Principles of Corporate Governance 2023*, OECD Publishing, Parigi,
H. J. PACE-L. J. TRAUTMAN, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, in *Wisc. L. Rev*., 2022
M. L. PASSADOR, *Sull'utilità della* ESG disclosure *e sul ruolo dei comitati rischi e sostenibilità*, in *Banca, impresa, società*, 2023
A. PERRONE-I. GIRARDI, *Innovazione tecnologica e stabilità finanziaria*, in M. CIAN-C. SANDEI (a cura di), *Diritto del Fintech*, Milano, Cedam, 2024
C. PICCIAU, *The (Un)Predictable Impact of Technology on Corporate Governance, in Hast. Bus. L. J.*, 2021
M. RESCIGNO, *L'evoluzione e il ruolo dell'informazione non finanziaria fra doveri informativi e obblighi gestori*, in *Rivista ODC*, 2023
A. SACCO GINEVRI, *Ancora su intelligenza artificiale e* corporate governance*, in Riv. trim. dir. econ.*, 2021, 3
G. SCHNEIDER, *La resilienza operativa digitale come materia di* corporate governance*: prime riflessioni a partire dal DORA*, in *Riv. Corp. Gov.*, 2022
G. SCHNEIDER, S*.E.C. Proposal: Cybersecurity Risk Management Rule*, in *Quaderni Assosim*, 2023, I
G. SCHNEIDER, *IA, rischi d'impresa e le (mancate) risposte del diritto... DORA per tutti?*, in N. ABRIANI-R. COSTI (a cura di), *Diritto societario, digitalizzazione e intelligenza artificiale*, Milano, Giuffrè, 2023