RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
*Periodico internazionale di diritto, giustizia e tecnologie*

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0269 • articolo sottoposto a peer review • pubblicato in anteprima il 21 apr. 2026


**Federica Delaini**

# Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA

Il contributo si inserisce nel dibattito sulle sfide che il diritto penale è chiamato ad affrontare nell'era della digitalizzazione, muovendo dall'evoluzione della criminalità informatica e dalla pervasività delle nuove tecnologie, che hanno posto in crisi il paradigma repressivo tradizionale. In tale contesto, il legislatore europeo ha adottato un approccio pragmatico e settoriale per contrastare le emergenti forme di criminalità, anticipando la soglia di tutela dei beni giuridici coinvolti. Questa politica legislativa segna una trasformazione verso la giuridicizzazione del rischio informatico e il rafforzamento della resilienza operativa digitale, attraverso l'adozione di pratiche organizzative virtuose e l'impiego della sicurezza informatica come strumento di prevenzione normativa. L'analisi si concentra sul settore finanziario, bancario e assicurativo, divenuti, a livello europeo, laboratori di sperimentazione giuridica. In questo quadro, il *Digital Operational Resilience Act* emerge come un modello di *governance* orientato alla prevenzione e alla proattività. L'obiettivo è individuare i caratteri "mobilitatori" che possono sostenere la tecnica legislativa penalistica nel quinto dominio.

*Diritto penale nell'era digitale – Criminalità informatica – Giuridicizzazione del rischio informatico*
*Cybersecurity governance – Digital Operational Resilience Act (DORA)*

## Towards a Criminal Law of Digital Security? Cyber compliance under the DORA Regulation

This article contributes to the ongoing debate on the challenges faced by criminal law in the digital age, starting from the evolution of cybercrime and the pervasive nature of new technologies, which have called into question the conventional repressive paradigm. In this context, the European legislator has adopted a pragmatic and sectoral approach aimed at addressing emerging forms of cybercrime while anticipating the threshold of protection of the legal interests involved. This legislative policy marks a significant transformation towards the juridification of cyber risk and the strengthening of digital operational resilience, grounded in the adoption of virtuous organisational practices and in the use of cybersecurity as a regulatory prevention tool. The analysis focuses on the financial, banking and insurance sectors, which have become, at the European level, laboratories of legal experimentation. Within this framework, the Digital Operational Resilience Act emerges as a model of governance geared towards prevention and proactivity. The article aims to identify the "mobilising" features that may support criminal legislative technique within the fifth domain.

*Criminal law in the digital age – Cybercrime – Juridification of cyber risk – Cybersecurity governance*
*Digital Operational Resilience Act (DORA)*

L'Autrice è dottoranda in Diritto penale nel programma di Dottorato in Scienze giuridiche europee e internazionali dell'Università di Verona. Il suo dottorato innovativo industriale è finanziato dall'Unione Europea nell'ambito del programma Next Generation EU, Missione 4, Componente 1, CUP B31I23000810004, in collaborazione con Generalfinance S.p.A.

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2,* a cura di Gaetana Morgante e Gaia Fiorinelli

## 1. Introduzione. Le sfide del diritto penale nell'era digitale

Nell'epoca della digitalizzazione, il diritto, e, in particolare, il diritto penale, si muove su un terreno segnato da un'elevata ambiguità e da una repentina mutevolezza, che impone al penalista di interrogarsi sulla strategia più efficace per dominare la globalizzazione tecnocentrica che interessa la nostra realtà sociale, economica e giuridica. Il progresso tecnologico ha ormai permeato ogni ambito della nostra esistenza e impone anche al diritto di adeguarsi, dal momento che la normativa si sostanzia nell'insieme delle regole che stabiliscono *chi vince e a quale prezzo*.

Analogamente a quanto accade con l'interazione tra uomo e macchina, che potenzia le capacità dell'individuo, anche il crimine informatico può beneficiare di tale sinergia. Per tale ragione, il diritto penale, lungi dall'assumere una connotazione squisitamente antropocentrica, potrebbe più opportunamente ampliare il suo sguardo alle modalità tecnologicamente connotate che possono sia contribuire alla commissione dei reati, sia, attualmente, caratterizzarla in via esclusiva.

Questa evoluzione sollecita una riflessione sulla metodologia che il diritto penale potrebbe adottare per contrastare efficacemente il cybercrime. Nello specifico, il diritto penale dell'informatica sta attraversando una trasformazione di portata epocale, che riveste una valenza paradigmatica, implicando un ripensamento delle categorie fondamentali della scienza penalistica.

L'evidenza empirica dimostra che un sistema fondato esclusivamente su logiche repressive si rivela inefficace, in quanto interviene quando il danno ha già avuto luogo. Al contrario, la promozione di strategie preventive – siano esse normative, tecniche o culturali – può ridurre la necessità di ricorrere alla sanzione penale, rafforzandone l'efficacia complessiva.

In tale prospettiva, la deterrenza assume una dimensione strutturale, non più fondata esclusivamente sulla minaccia della pena, bensì sull'anticipazione del rischio e sulla costruzione di un ambiente digitale sicuro e resiliente, attraverso comportamenti organizzativi e tecnico-informatici virtuosi.

Il contributo si propone di esaminare le frontiere e i limiti della nuova era che si è inaugurata per la tecnica penalistica, caratterizzata da un'importante espansione della legislazione europea, che evidenzia come un linguaggio minimo non sia più praticabile. Le direttive e i regolamenti hanno subito una trasformazione significativa, denotando uno sviluppo in senso pregnante, secondo una duplicità di direttrici, sistematiche e settoriali allo stesso tempo.

Inoltre, la nuova legislazione si distingue per una trasformazione concettuale di cruciale rilevanza, sintetizzata dall'espressione "dal rischio al diritto". Il rischio tecnologico, che, attualmente, è stato elevato a potenziale rischio sistemico a causa

dell'interconnessione infrastrutturale e della pervasività dei servizi digitali, è stato riconosciuto come una categoria autonoma di diritto, soggetta a una regolamentazione specifica e orientata alla prevenzione. Questo cambiamento segna il passaggio da una concezione puramente gestionale del rischio informatico a una sua piena "giuridicizzazione", con conseguente attribuzione di obblighi, responsabilità e standard organizzativi funzionali alla tutela di interessi primari.

Si tenterà, pertanto, di esaminare le caratteristiche innovative del nuovo quadro regolatorio europeo, che vede la sfida tecnologica collocarsi al centro della riflessione giuridica contemporanea.

A ciò si aggiunga che le entità finanziarie, bancarie e assicurative assumono un ruolo strategico e sistemico all'interno del mercato unico europeo, in quanto presidiano la stabilità dei mercati, la continuità dei flussi di pagamento, l'allocazione del credito e, più in generale, il funzionamento dell'economia reale. Di conseguenza, la loro resilienza operativa non assume rilievo esclusivamente in termini di microprudenza, ma si configura come condizione imprescindibile per la tutela della stabilità complessiva del sistema e per la salvaguardia di diritti fondamentali quali l'iniziativa economica, il risparmio e la protezione dei dati personali.

In tale contesto, gli attacchi informatici non rappresentano più eventi sporadici, ma fenomeni con il potenziale di generare effetti dirompenti, amplificati dall'elevata interconnessione tra operatori, infrastrutture e fornitori terzi di servizi digitali. La compromissione di sistemi critici può determinare conseguenze di vasta portata, tra cui interruzioni di servizi essenziali, perdite patrimoniali significative, erosione della fiducia degli investitori e dei risparmiatori, nonché ripercussioni sistemiche che possono incidere sull'ordine pubblico economico.

La cybersecurity nel settore finanziario, bancario e assicurativo assume, dunque, una rilevanza di interesse pubblico primario, richiedendo un approccio regolatorio integrato.

Quale corollario, il *Digital Operational Resilience Act*, c.d. Regolamento DORA, si configura come un modello di best practice per la gestione delle minacce informatiche derivanti dall'erogazione di servizi digitali nei settori sopracitati. L'approccio metodologico adottato ha saputo valorizzare i concetti di prevenzione, proattività, multidisciplinarietà, co-regolazione e responsabilità multilivello, delineando un sistema organico di resilienza operativa digitale.

Più precisamente, l'analisi si concentrerà sull'esame dei presidi introdotti per garantire la sicurezza della *supply-chain*, concepiti come requisiti contrattuali minimi obbligatori ai fini della compliance normativa, da cui dipende la *cyber-resilience* delle entità finanziarie, bancarie e assicurative. È emerso che tali presidi anticipano il momento di tutela a partire dalla configurazione contrattuale del servizio esternalizzato nel quale la minaccia cyber potrebbe manifestarsi. L'obiettivo primario del legislatore europeo è stato quello di consolidare un presidio sistemico contro le minacce informatiche, trasformando la sicurezza digitale da mero requisito tecnico a componente strutturale della tutela dei diritti fondamentali nell'economia digitale.

L'implementazione di una strategia legislativa che eleva la cybersecurity a nuova pietra angolare dei mercati digitali evidenzia la trasformazione sostanziale che sta attraversando il diritto penale dell'informatica.

La presente indagine si prefigge di esaminare gli emergenti caratteri di cui la tecnica penalistica potrebbe avvalersi ai fini del contrasto delle forme di criminalità cibernetiche nell'era contemporanea.

Nell'arsenale del penalista, infatti, riveste particolare importanza l'introduzione di misure preventive e proattive, come la sicurezza informatica. Tuttavia, affinché quest'ultima possa dirsi pienamente efficace, è necessario avviare un dialogo intenso e costante con le discipline scientifiche e tecniche, anche extragiuridiche, che possono contribuire a gettare solide fondamenta per il diritto penale nell'epoca della sicurezza digitale.

## 2. Verso un nuovo paradigma preventivo-proattivo

Il diritto penale, inteso come strumento di repressione e concepito esclusivamente per l'uomo, risulta antiquato rispetto all'incessante avanzamento del progresso tecnologico. Tale branca dell'ordinamento si è storicamente sviluppata come un "diritto di reazione", intervenendo *ex post*, ovvero una volta che il fatto lesivo, anche in termini di messa in pericolo del bene giuridico protetto, si è verificato, con l'obiettivo di sanzionare e dissuadere dal ripetersi di comportamenti penalmente illeciti. Questo paradigma, che per secoli ha rappresentato

il fulcro della legalità sostanziale, mostra, tuttavia, i suoi limiti nel contesto digitale.

Negli ultimi anni il diritto penale è stato chiamato a confrontarsi con una mutazione strutturale della criminalità economica e tecnologica[1]. Il cyberspazio[2], per sua natura transnazionale e decentralizzato, ha eroso i fondamenti del paradigma repressivo tradizionale, sovvertendone principi consolidati.

La sequenza tipica rappresentata da fatto, accertamento e sanzione, si è dimostrata progressivamente inadeguata di fronte a fenomeni che si manifestano in millisecondi e si estendono a diverse giurisdizioni. Ciò in quanto i cyber-attacchi e la manipolazione dei dati o dei sistemi algoritmici non seguono più le logiche spazio-temporali intrinseche alla condotta umana[3]. Peraltro, queste nuove forme di criminalità non possono definirsi nemmeno "bloodless", atteso l'impatto che sono in grado di provocare sui destinatari quando la minaccia, originariamente limitata all'ambiente digitale, diviene fisica. Basti pensare all'attuale contesto geopolitico, caratterizzato da una *escalation* di "guerre ibride diffuse", nelle quali la maggior parte degli attacchi sono stati perpetrati non mediante l'impiego di armi convenzionali, ma attraverso l'uso di tecnologie innovative, potenzialmente letali per intere comunità[4].

Dal punto di vista della tecnica penalistica, il fenomeno si inserisce in un universo radicalmente diverso da quello della criminalità non cyber, privo dei riferimenti spaziali e temporali su cui il diritto penale tradizionalmente si fonda[5]. Gli attacchi informatici si sviluppano nell'ordine dei millisecondi, attraversano più giurisdizioni e sono in grado di produrre effetti sistemici prima ancora di essere rilevabili.

La natura strutturalmente globale del cyberspazio influisce significativamente sulla configurazione della fattispecie incriminatrice. In merito, si evidenziano le difficoltà applicative che le categorie penalistiche classiche (*locus commissi delicti*[6], azione, evento[7] e bene giuridico tutelato[8]) incontrano laddove trasposte nel cyberspazio. Ciò nonostante,

1. Per un approfondimento a riguardo, si rinvia a Corasanti 2025; per la letteratura straniera, cfr. Parker 1974; Menelly 1985. Circa le difficoltà definitorie del concetto di criminalità informatica, si rinvia, tra i tanti, a Pecorella 2006.
2. Termine coniato da William Gibson nel 1986 nell'ambito della letteratura Cyberpunk. Per un approfondimento cfr. Flor 2019-a; Pietropaoli 2019.
3. Per una disamina della materia si rinvia a Cuomo 2000; Padovan 2023; Morgante 2025.
4. Il primo caso di *cyberwarfare* risale all'attacco dell'Estonia del 2007, uno dei paesi al mondo maggiormente informatizzato, noto per la vicenda "*Il soldato di bronzo*", in occasione del quale per la prima volta nella storia uno Stato membro della NATO ha richiesto l'attivazione dell'art. 5 del Trattato istitutivo dell'Alleanza Atlantica, a seguito di un attacco di natura cibernetica alle proprie infrastrutture digitali. Tuttavia, alla richiesta non venne dato seguito in quanto l'Estonia, pur fortemente danneggiata dai *cyberattacks*, non aveva subito vittime o distruzioni fisiche alle infrastrutture critiche e si ritenne di non poter ravvisare gli estremi dell'applicabilità della disposizione difettando il requisito "contro l'integrità territoriale di uno Stato". A questo proposito, vedasi Aterno 2022, pp. 215-217.
5. La questione dell'applicazione del diritto penale per sanzionare condotte perpetrate in ambito digitale è stata oggetto di approfondimento da parte di Fiorinelli 2024, p. 110 ss.
6. Questo profilo problematico è stato investigato in maniera significativa da Corona 2021; Aterno 2023. In talune circostanze, è stata adottata la "fisicizzazione" degli elementi del reato, collocando la condotta nel luogo dell'autore materiale e l'evento nel luogo della vittima, conferendo così materialità ad un reato virtuale. Per un approfondimento a riguardo vedasi Carrea 2017; Flor 2019-b; Razzante 2023.
7. L'elemento oggettivo del reato è stato esaminato in questi termini da Picotti 2000, p. 16 ss., Cuomo–Izzi 2002, p. 1018; , Cuomo–Razzante 2009; Mattarella 2022, p. 809.
8. La riflessione a riguardo è stata sviluppata da Donini 2013, p. 6. In riferimento al concetto di imprescindibilità epistemologica del bene giuridico tutelato si rinvia a Flor 2022, p. 145 che alla nota 38 rimanda a Rocco 1913; Pisapia 1948; Pagliaro 1965; Stella 1973; Bettiol 1959; Neppi Modona 1965; Bricola 1973; Mantovani 1977; Pulitanò 1981; Vassalli 1982; Fiandaca 1982; Angioni 1983; Stile 1985; Donini 2003; Donini 1999.

tale regione continua a rivestire un'importanza strategica per gli Stati, in quanto ospita la maggior parte delle attività economiche, sociali e governative, nonché delle interazioni tra i Paesi[9], di talché, "Il clic di un computer ha oggi un peso molto superiore al grilletto di una pistola"[10].

È sufficiente considerare che, nell'anno 2025, in Italia, si è verificato un aumento significativo del numero di realtà aziendali che sono dovute ricorrere alla cassa integrazione per i propri dipendenti a causa di attacchi *ransomware* che hanno compromesso seriamente la produzione e la stabilità finanziaria aziendale, causandone talvolta il tracollo[11].

Quale conseguenza, nel contesto digitale, la prevenzione assume una rilevanza sistemica e sistematica, non limitandosi esclusivamente alla protezione dell'ormai unanimemente riconosciuto bene giuridico della "sicurezza informatica"[12], ma estendendosi alla costruzione di condizioni organizzative e tecnologiche che ne prevengono la compromissione o la messa in pericolo. All'interno dell'armamentario del penalista emerge la cybersecurity[13], intesa sia come il processo che come il risultato di garantire la sicurezza nel cyberspazio. Tale misura precauzionale rappresenta il *nuovo volto della prevenzione penale*, che opera non solo su un piano individuale, ma anche su quello collettivo e collettivistico delle strutture e delle infrastrutture tecnologiche e organizzative la cui compromissione potrebbe arrecare pregiudizio a intere collettività.

A conferma di tale trasformazione concettuale, le nuove discipline di matrice europea estendono l'ambito applicativo delle regole di sicurezza informatica agli assetti aziendali, alle infrastrutture tecniche, alle filiere di fornitura e, in generale, agli ecosistemi di dati. Per l'effetto, la cybersecurity contribuisce a delineare un livello di protezione anticipato rispetto al momento in cui si verifica l'effettiva lesione dell'integrità delle informazioni, dei programmi o dei sistemi informatici, al fine di tutelare l'affidabilità e la fiducia collettiva della sicurezza dei rapporti giuridici instaurati tramite l'uso di strumenti tecnologici e spazi virtuali[14].

Ai fini della presente analisi, con il termine "sicurezza informatica" ci si riferirà alla sicurezza delle informazioni, ossia di dati organizzati e significativi[15]. La cruciale importanza dei dati deriva dalla loro natura dinamica e trasformativa: una volta elaborati e contestualizzati, i dati sono potenzialmente in grado di essere convertiti in informazioni[16], che costituiscono risorse strategiche e gli asset più preziosi e ambiti dell'ecosistema contemporaneo, divenuti oggi il fulcro della competizione economica, oltre che il principale obiettivo e la nuova moneta di scambio della criminalità in ambiente informatico.

In tale prospettiva, la cybersecurity si configura come un nuovo paradigma di diritto preventivo-proattivo, che realizza un'ibridazione tra diritto penale, diritto amministrativo, regolazione economica e informatica, capace di affiancare alla punizione, la necessaria e non più procrastinabile costruzione di comportamenti organizzativi ottimali, la cui omissione determina l'applicabilità di sistemi di diritto punitivo settoriali, ossia, sanzioni amministrative, oltre che l'operatività delle ordinarie discipline penalistiche vigenti, ai sensi

9. Per ulteriori approfondimenti, si veda Buckland–Schreier–Winkler 2015, p. 7 ss.; Martino 2018, I, p. 69; Ramadhan 2021, p. 161 ss.; Sharma 2022, p. 50 ss.; e, in tema di *cyberdiplomacy*, Fracchiolla 2022, pp. 463-484.
10. La citazione è tratta da Mattarella 2022, p. 44.
11. Di Cuia 2025; Fadda 2025.
12. Per un compiuto approfondimento della affermatasi autonomia del bene giuridico della sicurezza informatica rispetto ai beni giuridici tradizionali vedasi Cuomo 2000, Picotti 2011 p. 229 ss., Mattarella 2022, p. 813, che rinvia sul rapporto tra bene strumentale e finale, a Fiorella 1987; Corona 2023; Flor 2023, p. 138; Padovan 2023, p. 13 ss.
13. Per un'analisi dei tentativi di concettualizzazione sistematica dell'espressione *cybersecurity* vedasi Urgessa 2020; Flor 2023, p. 143; Blažič–Blažič 2024.
14. La riflessione sul punto è tratta da Flor 2023, pp. 139-141 al cui approfondimento si rinvia anche in riferimento alla concezione dell'area di intersezione fra dimensioni individuale e collettiva.
15. Per tale scelta semantica si rinvia ad Aterno 2022, pp. 181-182.
16. Cuomo–Razzante 2009, pp. 5-6.

del d.lgs. 231/2001 ovvero del combinato disposto degli artt. 110 e 40 cpv. c.p.[17]

Il diritto penale fornisce la *ratio*, l'idea di tutela anticipata, mentre il diritto europeo, di cui il *Digital Operational Resilience Act*[18], che rappresenta un esempio virtuoso, ne costituisce la traduzione operativa. La sicurezza informatica non si limita più ad assumere le vesti di una misura di protezione tecnica, ma si configura come uno strumento di prevenzione normativa volto a mitigare *ex ante* i rischi sistemici associati alle nuove forme di criminalità informatica.

## 3. Dal rischio al diritto: la costruzione europea della resilienza operativa digitale

La risposta europea alla sfida della criminalità informatica si fonda su una *trasformazione concettuale*: dal rischio al diritto. L'opera legislativa delle istituzioni europee, che hanno assunto un ruolo pioneristico in materia[19], non si è, infatti, limitata a gestire il rischio tecnologico, ma lo ha tradotto in obblighi giuridici, vincoli di governance e responsabilità operative, mediante l'introduzione di discipline di stampo preventivo e proattivo implementate secondo un approccio pragmatico[20] e settoriale, e attraverso una metodologia multidisciplinare e multilivello, in linea con la strategia di *security-by-design*[21] a lungo propugnata dalle istituzioni europee.

Il percorso ha avuto inizio con l'adozione del Regolamento generale sulla protezione dei dati (GDPR)[22], che ha introdotto il principio di accountability, ponendo l'accento sulla responsabilità attiva e documentata dei soggetti obbligati. Successivamente, il *Cybersecurity Act*[23], le *Direttive NIS*[24], il *Data Act*[25] e il *Digital Markets Act*[26] hanno contribuito a edificare un sistema multidimensionale in cui la resilienza operativa digitale è divenuta elemento strutturale del mercato unico europeo, non a caso invocato, ai sensi dell'art. 114 TFUE, quale base giuridica per l'adozione delle discipline appena citate. Il denominatore comune di tali normative è stato individuato nella volontà,

17. Cfr. Piva 2022, p. 537.
18. Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, cui, d'ora in poi, ci si riferirà con "Regolamento DORA".
19. Il percorso del legislatore europeo ha avuto inizio nel 2013, con la *Strategia sulla Cybersicurezza*. Per una disamina più approfondita della questione si rinvia a González Fuster–Jasmontaite 2020, pp. 97–115.
20. Tale qualificazione si deve a Flor 2019-a, p. 457.
21. Per ampliare ulteriormente l'analisi del concetto di *security-by-design* si rinvia a Marcialis 2023, p. 391, che evidenzia la necessità di progettare i sistemi informatici secondo una visione olistica e non soltanto frammentaria o di tipo modulare.
22. Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
23. Regolamento (UE) 2019/881 relativo all'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza).
24. Direttiva (Ue) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione e Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
25. Regolamento (Ue) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).
26. Regolamento (UE) n. 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contenibili nel settore digitale e che modifica le direttive (UE) m. 2019/1937 e (UE) n. 2020/1828 (Regolamento sui mercati digitali). Per un approfondimento sulla configurazione dei mercati digitali mediante una regolazione cooperativa e multi-partecipativa si veda Licastro 2025.

più o meno manifesta, di istituzionalizzare approcci trasversali di prevenzione digitale a protezione del mercato comune.

L'Unione europea si è proposta come un vero e proprio laboratorio giuridico per la regolazione del cyberspazio, promuovendo un approccio integrato che unisce il diritto dell'informatica, il diritto dei mercati e il diritto penale, ibridandolo al diritto amministrativo. Il concetto di "resilienza operativa digitale" è stato elevato a principio di governance, con una funzione paragonabile a quella della stabilità finanziaria. Si delinea un nuovo diritto della sicurezza informatica, che coinvolge istituzioni, imprese e individui in un sistema di co-regolazione e corresponsabilità multistakeholder.

Il legislatore europeo non si è limitato a imporre sanzioni *ex post*, ma ha definito un quadro preventivo in cui la resilienza digitale è divenuta un obbligo di conformità e un presupposto della legittimità operativa. L'innovazione si sostanzia nella formalizzazione giuridica del rischio tecnologico[27], che viene così classificato come una categoria di diritto: il rischio viene normato, valutato, comunicato e attribuito ad un responsabile. Tale cambiamento di prospettiva comporta che il rischio non è più inteso come un evento da eludere, ma, piuttosto, come un fattore da amministrare secondo principi giuridici e logiche aziendali.

Il diritto europeo ha adottato il linguaggio della prevenzione tecnica e lo ha trasformato in linguaggio di legalità, spostando l'asse della tutela penale: la lesione non è più esclusivamente l'attacco informatico o il danno economico, anche reputazionale, bensì l'omissione nella gestione del rischio, la mancanza di vigilanza, l'assenza di cultura organizzativa interna e esterna della sicurezza informatica.

La transizione "dal rischio al diritto" rappresenta il fondamento teorico per comprendere come DORA non si limiti a rivestire il ruolo di uno strumento di regolazione finanziaria, bancaria e assicurativa, ma si configuri come un modello di governance esportabile[28] a tutti i mercati digitali, in quanto la sua logica è in grado di estendersi oltre il suo ambito applicativo. La nuova tendenza è quella di accettare l'idea dell'estrema dinamicità dei mercati, oltre che la normatività della tecnologia di cui essi sono impregnati[29].

## 4. Il Digital Operational Resilience Act: una governance multidisciplinare e multilivello tra prevenzione, co-regolazione e responsabilità multistakeholder

Il Regolamento DORA, il cui obiettivo risiede nella salvaguardia della resilienza operativa digitale dei sistemi informatici a fronte di *cyber-attack*, introduce un *corpus* normativo che integra principi di gestione del rischio ICT e continuità operativa, delineando una governance che coinvolge le organizzazioni operanti nel settore finanziario, bancario e assicurativo, ma anche le relative Autorità garanti, nazionali[30] ed europee (EBA, ESMA, EIOPA), e i fornitori terzi di servizi ICT.

Con la sua emanazione, gli operatori sono stati chiamati a una continua propensione verso un miglioramento omnicomprensivo nella gestione della cybersecurity, che viene concepita come un mezzo precauzionale indefettibile nella moderna società delle reti. Nello specifico, la necessità dell'intervento regolatore è sorta dalla constatazione di una crescente dipendenza dei settori convolti dai processi digitali[31].

27. Tale rischio ricomprende, a tutt'oggi, nella sua tassonomia, anche gli l'utilizzo di strumenti di intelligenza artificiale. Sull'interazione tra il Regolamento DORA e l'AI Act si rinvia a Faraone 2024.
28. Questa via è stata anche indicata da Michieli 2024, cui si rinvia per una trattazione del Regolamento DORA.
29. Su tali aspetti si vedano le riflessioni di Lessig 1999.
30. A livello italiano, le Autorità garanti sono state istituite dal d.lgs. n. 23/2025, che, all'art. 3, prevede la partecipazione al forum di sorveglianza di Banca d'Italia, Consob, Ivass e Covip, cui viene attribuita la qualifica di Autorità competenti per il rispetto degli obblighi posti dal Regolamento DORA a carico dei soggetti vigilati, secondo le rispettive attribuzioni di vigilanza, nonché per le segnalazioni di gravi incidenti informatici e per le segnalazioni volontarie di minacce informatiche significative.
31. I dati su cui si basa la riflessione sono stati tratti da Associazione Italiana per la Sicurezza Informatica 2025. Sul punto, si rinvia anche alle opere di Michieli 2024; Raffaele 2024.

Primariamente, è d'obbligo sottolineare che il legislatore europeo ha optato per l'adozione del "più forte" degli atti di normazione secondaria a livello unionale, quello del regolamento, dotato per sua stessa natura del connotato della vincolatività e dell'efficacia *erga omnes*, in ragione dell'importanza del settore di intervento[32]. La suddetta scelta normativa riveste una notevole rilevanza all'interno del quadro regolatorio in esame, suggerendo una nuova direzione per la normazione europea, che sembra, sempre più spesso, muoversi verso l'abolizione del ricorso alle direttive e, al contrario, verso la concentrazione della tecnica legislativa sui regolamenti[33]. Tale cambiamento di indirizzo potrebbe contribuire in modo significativo alla neutralizzazione della frammentazione dell'ordinamento eurounitario, accrescendone l'efficacia e la capacità deterrente.

Le entità finanziarie[34], in considerazione del delicato *core business* di cui trattano e che costituisce, sempre più di sovente, il *quid* tanto desiderato dalla criminalità informatica, svolgono una funzione sociale che impatta tanto sulla macroeconomia, che interessa il sistema-Paese, quanto sulla microeconomia, la quale coinvolge, quotidianamente, ogni singolo risparmiatore[35]. Pertanto, l'investimento in materia di protezione dei dati, dei sistemi e delle infrastrutture nel settore Fintech è un fattore determinante per la tutela della persona, oltre che del sistema economico nazionale e europeo[36]. L'acquisita consapevolezza che il *cyber-risk* può rappresentare un rischio strutturale negli attuali modelli di business e un rischio di potenziale impatto sistemico[37], non più relegabile alla sola sfera dei rischi operativi, si è tradotta nelle nuove norme comuni sulla resilienza operativa digitale, per tale intendendosi la capacità di costruire, assicurare e riesaminare l'integrità e l'affidabilità operativa dei sistemi, garantendo, direttamente, oppure indirettamente, anche tramite il ricorso a fornitori terzi, l'intera gamma delle capacità connesse alle ICT necessarie per garantire la sicurezza delle infrastrutture di rete.

La struttura del Regolamento DORA si fonda su cinque pilastri fondamentali[38]: (i) *ICT risk management*, che richiede un'accurata identificazione, valutazione e mitigazione dei rischi ICT e impone agli istituti finanziari di istituire solidi quadri di governance e di controllo interni; (ii) *ICT Incident Managemen*t, in forza del quale devono adottare un processo standardizzato per identificare, gestire e segnalare adeguatamente gli incidenti ICT significativi; (iii) *Digital Operational Resilience Testing*, che si sostanzia nell'esecuzione di test regolari della resilienza organizzativa per garantire la preparazione a un'ampia gamma di rischi ICT, inclusi programmi completi per identificare, affrontare e mitigare le vulnerabilità; (iv) *ICT Third Party Risk Management*, che sottolinea l'importanza di gestire con attenzione i rischi derivanti da partnership esterne e richiede di valutare, approfondire e mantenere solide relazioni contrattuali con le terze parti; (v) *Information Sharing* che incoraggia la condivisione di informazioni sulle minacce

32. In questi termini si è espresso Barbara 2022, p. 508 cui si rinvia per un approfondimento della normativa europea analizzata.
33. Sulla medesima scia, si ritiene che si sia posta anche l'emanazione del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
34. L'espressione "entità finanziarie" verrà utilizzata per indicare sinteticamente le organizzazioni dei tre diversi settori destinatari dell'applicazione del Regolamento DORA: bancario, finanziario e assicurativo. Per un approfondimento circa l'ambito applicativo del Regolamento vedasi Pérez–Carrillo 2023; Busch 2024; Michieli 2024.
35. Cfr. Chiocchio 2022.
36. Per un approfondimento si rinvia a Garante per la protezione dei dati personali 2020.
37. A questo riguardo, si vedano i dati riportati da Angelini 2024, pp. 1-6; Associazione Italiana per la Sicurezza Informatica 2025, p. 112.
38. Il tema della governance dei rischi contrattuali alla luce dell'emanazione del Regolamento DORA è stato trattato da Schneider 2022; Ghignatti 2024.

informatiche per promuovere la resilienza collettiva e, promuovendo una cultura di condivisione collaborativa, mira a migliorare la preparazione e le capacità di risposta complessive del settore.

Il Regolamento DORA non è stato concepito come una normativa autonoma e indipendente, ma piuttosto come il risultato di una strategia legislativa complessa[39], progettata secondo un approccio settoriale, partecipativo e multilivello. Tale strategia muove le mosse dalla tendenza – sempre più incalzante – ad affidare la gestione dei servizi digitali a fornitori esterni[40], per motivi che includono l'ottimizzazione dei costi e delle risorse, la focalizzazione sul *core business*, la considerazione dell'esperienza maturata dall'*outsourcer* e della garanzia delle prestazioni, il *reengineering* dei processi e la mitigazione dei rischi.

Tuttavia, i fornitori di servizi digitali rappresentano una delle principali vie attraverso le quali si diffondono le minacce informatiche. Quale corollario, avendo riguardo al management delle esternalizzazioni, sono stati introdotti numerosi obblighi contrattuali che richiedono il possesso di specifiche *technicalities*[41], quali l'analisi e la gestione dei rischi, la realizzazione di stress test, l'attività di vigilanza, l'attenzione ai contenuti contrattuali e ai regimi di responsabilità, per equilibrare i rapporti di forza e di dipendenza tra i settori *Finance* e ICT, al fine di tutelare gli interessi degli investitori e del sistema europeo[42].

La neonata normativa configura la cybersecurity come una responsabilità multi-stakeholder, che necessita di essere implementata in vari livelli di governo, economia e società, coinvolgendo personale, consigli di amministrazione e Autorità garanti. È stata prevista una stretta collaborazione tra tutti gli attori, pubblici e privati, che compongono la filiera della protezione dei nuovi interessi digitali, al fine di strutturare strategie trasversali di prevenzione dagli attacchi informatici.

È stata delineata una *regolazione partecipativa*, in cui al regolatore pubblico spetta definire la normativa che influenzerà la struttura del governo societario dell'ente privato, mediante la previsione di obblighi *ex ante*, e al regolato (le istituzioni finanziarie) il compito di integrarne il contenuto *by design* nell'architettura dei propri modelli di *outsourcing*, secondo una logica collaborativa costruita su un'intensa partnership pubblico-privata. In tale contesto, è stato osservato il ruolo attivo affidato alle Autorità garanti, sia a livello nazionale che europeo, che svolgono la funzione di sorveglianza del nuovo quadro normativo, al fine di supportare i regolatori nella formulazione di strategie di conformità efficaci che considerino gli obblighi *ex ante*. Tali obblighi rappresentano le nuove coordinate per il mercato digitale europeo. Il legislatore ha, pertanto, implementato un sistema di conformità cooperativa, basato sul dialogo tra regolati, regolatore e guardiani. Le istituzioni sono concepite come partner attivi nei meccanismi di regolazione economica e di contrasto alle forme di criminalità informatica che presentano un impatto sistemico[43].

Il passaggio graduale dalla gestione interna dei servizi digitali all'affidamento a soggetti terzi ha reso essenziale esercitare un controllo efficace sull'accountability[44] del fornitore. L'obiettivo è verificare l'adozione di comportamenti proattivi e di misure volte a garantire la corretta implementazione del quadro di resilienza operativa digitale. Più precisamente, nel settore della sicurezza informatica, l'accountability si manifesta nella capacità di dimostrare il rispetto degli obblighi previsti dalla normativa, anticipando potenziali eventi dannosi e prevedendo misure organizzative e tecniche adeguate a prevenire una serie ampia di rischi calcolati. Tale approccio metodologico include la gestione di situazioni critiche e l'identificazione di eventi

39. Cfr. la pagina del sito della Commissione europea sul *Digital Finance Package* del 2020.
40. Il tema della co-dipendenza tra settore finanziario e ICT e dei fenomeni rilevanti generati per il diritto dell'economia che hanno conferito al FinTech un'autonoma rilevanza di mercato è stato approfondito da Pignatti 2024, p. 649.
41. Si pensi, a titolo esemplificativo, ai requisiti stabiliti in riferimento ai livelli di servizio, ai t*hread-lep-penetration tests* e alle *exit strategies* di cui all'art. 30, co. 2, del Regolamento DORA.
42. L'osservazione è tratta da Pignatti 2024, p. 653.
43. Per un approfondimento circa le origini storiche dell'istituto della funzione di compliance si veda Miller 2014, p. 2.
44. Così, Lorè–Musacchio 2021.

rischiosi, con l'obiettivo di sviluppare risposte che garantiscano un margine di sicurezza concreto.

L'Europa ha adottato un approccio che considera l'accountability e la governance come elementi cruciali per la resilienza operativa digitale, promuovendo l'integrazione del principio della compliance nelle normative. La logica sottostante è analoga a quella che ha guidato la progettazione del già citato GDPR, ma anche dell'*AI Act* e del *Data Act*, normative che presentano una connessione diretta con la struttura dei processi di gestione dei dati, sia personali che non personali, e con i rapporti contrattuali instaurati con i fornitori. L'approccio delineato incorpora una strategia integrata, al fine di sviluppare un sistema di gestione delle terze parti nell'ambito della politica complessiva di neutralizzazione dei rischi sistemici ICT. Inoltre, il framework impone l'adozione di una nuova cultura aziendale, basata su un approccio non solo quantitativo, ma anche qualitativo, e rivolta non solo alle istituzioni finanziarie, ma anche ai fornitori.

Infatti, affinché si possa garantire un'effettiva e proficua conformità alla normativa, numerose prescrizioni impongono inediti e onerosi adempimenti in materia di cybersecurity che riguardano non solo l'organizzazione interna, ma anche quella esterna. In un contesto sempre più interconnesso[45], le attività finanziarie affidano all'esterno lo svolgimento di operazioni anche di cruciale rilevanza e la dipendenza che si crea tra l'entità e il fornitore può comportare vulnerabilità significative, soprattutto laddove il terzo non sia in grado di assicurare e di mantenere in modo stabile e continuativo standard di sicurezza informatica elevati e adeguati al contesto, spaziale, temporale e tecnologico, nel quale il servizio viene erogato.

Per comprendere meglio l'importanza e la crucialità della scelta normativa europea, è opportuno esaminare il comparto di disposizioni che impongono alle entità finanziarie, in sede di stipula dei contratti di fornitura di servizi ICT, di rispettare standard specifici per garantire che le clausole contrattuali siano conformi a un livello comune e che sia possibile monitorare adeguatamente le attività svolte dai fornitori. Il legislatore ha, quindi, ideato un regime *ad hoc* per la gestione dei rapporti con le terze parti, con l'obiettivo di rendere cyber resilienti i rischi derivanti dall'esternalizzazione, soprattutto se a supporto di funzioni essenziali o importanti[46]. Ciò in quanto non è sufficiente che l'entità finanziaria sia resiliente, ma è indispensabile che lo siano anche i suoi fornitori.

### 4.1. Il regime di responsabilità in caso di violazione del Regolamento DORA

All'interno degli accordi di esternalizzazione, concepiti come strumento principe per la corretta ed equilibrata gestione della condizione di dipendenza del settore finanziario dai fornitori di servizi ICT, è necessario includere requisiti contrattuali specificamente individuati dal legislatore europeo, che consentono di monitorare i potenziali rischi e di mitigare gli effetti negativi derivanti dallo squilibrio di potere sopra descritto.

Per elaborare contratti di esternalizzazione cyber-resilienti, l'entità finanziaria dovrà muovere le mosse dalla consapevolezza delle minacce ICT cui è maggiormente esposta, attraverso l'analisi dei rischi, nota come *risk based approach*, che trae ispirazione dalle esperienze maturate in altri settori, come quello della responsabilità amministrativa delle persone giuridiche[47]. Tale approccio

45. Anche su questo tema, si rinvia nuovamente all'opera di Michieli 2024; Raffaele 2024.

46. L'art. 3, paragrafo 1, punto 22) del Regolamento DORA definisce "funzione essenziale o importante" una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività. La medesima definizione si applica alla funzione la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari.

47. Così come disciplinata dal decreto legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", che ha introdotto nell'ordinamento italiano il principio della responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio da amministratori, dirigenti o dipendenti. La suddetta normativa estende la responsabilità oltre la persona fisica e prevede sanzioni di natura pecuniaria, interdittiva e di confisca. Al fine di esonerare l'ente da tale responsabilità, si rende necessario implementare un Modello

si prefigge di ridurre l'asimmetria informativa tra le parti coinvolte[48], al fine di implementare i meccanismi e le misure organizzative e gestionali idonee a mitigare l'impatto di un rischio informatico sull'attività finanziaria. Risulta peculiare come tali rischi e opportunità risiedano al di fuori dell'ambito finanziario, richiedendo professionalità e competenze specifiche per la loro efficace gestione[49].

Quanto alle responsabilità in caso di violazione della normativa, il sistema sanzionatorio disegnato dal legislatore europeo si applica esclusivamente alle entità finanziarie, nello specifico all'organo di gestione[50]. Ai sensi del Regolamento DORA, il fornitore terzo incorrerà soltanto nelle responsabilità di natura contrattuale derivanti dal contratto di esternalizzazione stipulato con l'entità finanziaria[51]. Ciò implica che il consiglio di amministrazione sarà responsabile non solo delle procedure e dei quadri interni e del modo in cui sono stati predisposti, ma anche della sicurezza e dell'adeguatezza dei presidi elaborati dalla società terza incaricata della gestione delle informazioni e dei dati sensibili oggetto del servizio esternalizzato.

La limitazione della responsabilità alle sole entità finanziarie e non anche ai fornitori, appariva, tuttavia, eccessivamente gravosa e, finanche, violativa del principio di proporzionalità a cui la nuova legislazione dichiarava espressamente di ispirarsi[52]. Ciò in ragione del fatto che spesso queste organizzazioni faticano a rivestire un ruolo da protagoniste nella negoziazione delle clausole dei contratti di *outsourcing* che, nella maggior parte dei casi, fanno capo a contratti standardizzati, predisposti unilateralmente da parte del fornitore e senza possibilità di modifica.

Per tale ragione, nel periodo di *vacatio* tra l'emanazione del Regolamento DORA e la sua entrata in vigore (avvenuta il 17 gennaio 2025, fatta eccezione per gli intermediari finanziari *ex* art. 106 TUB, per i quali ne è stata posticipata l'entrata in vigore di due anni[53]), i fornitori, non essendo soggetti a sanzioni in caso di mancata ottemperanza, non hanno mostrato disponibilità a uniformare le proprie scritture contrattuali alla nuova legislazione europea. Era, quindi, previsto un meccanismo simile a quello vigente in materia di privacy: il rispetto degli adempimenti rilevanti restava in capo all'ente finanziario e non gravava direttamente sul fornitore.

Un rilevante cambio di scenario si è avuto soltanto con il d.lgs. n. 23 del 10 marzo 2025[54], che, in adeguamento al Regolamento DORA, ha esteso l'ambito applicativo delle sanzioni anche ai fornitori

Organizzativo, di Gestione e Controllo (MOGC) idoneo a prevenire i reati presupposto, sottoposto ad un Organismo di Vigilanza (OdV).

48. Più in generale, sul tema delle asimmetrie di potere esistenti tra banche e fornitori di servizi tecnologici, si rinvia a Cardani–Girardi 2024.
49. Così, Pignatti 2024, p. 654 cui si rinvia per la disamina della diversa natura dei rischi connessi alla sicurezza informatica.
50. La responsabilità dell'organo di gestione costituisce il principio guida, in quanto gravato dalla valutazione dell'adeguatezza delle clausole contrattuali che disciplinano i rapporti con i fornitori di servizi ICT ai sensi dell'art. 5, par. II, del Regolamento DORA.
51. I risvolti di tale quadro normativo sono stati analizzati da Pignatti 2024.
52. Cfr. art. 8 Regolamento DORA.
53. Ciò è quanto è stato previsto dall'art. 17 del Decreto legislativo 10 marzo 2025, n. 23, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/ CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario", in forza del quale il decreto entra in vigore il giorno successivo a quello della sua pubblicazione, salvo per gli intermediari finanziari cui è dedicato l'art. 6, commi 1 e 2, del decreto, per i quali la normativa si applica a decorrere dal 1° gennaio 2027.
54. Il d.lgs. n. 23/2025 si caratterizza per un'ampia estensione dell'ambito di applicazione del Regolamento DORA: la nuova normativa riguarda i soggetti che operano come intermediari finanziari, ossia Bancoposta S.p.A., Cassa

di servizi ICT, che, a seconda della tipologia di soggetto al quale erogano i propri servizi, sono soggetti a regimi sanzionatori diversi. Più nello specifico, le sanzioni sono applicabili tanto nei confronti delle persone giuridiche (le condotte più gravi sono sanzionate da 30.000 € al 10% del fatturato; quelle meno gravi da 30.000 €, con un massimo edittale del 7%), quanto nei confronti delle persone fisiche che svolgono funzioni di amministrazione, direzione o controllo, e che possono venire colpite anche dalla sanzione amministrativa accessoria dell'interdizione[55]. Inoltre, l'attenzione e la responsabilizzazione degli organi di vertice evidenziano la strategicità del rischio cyber, che non può essere più considerato una tematica esclusivamente tecnica, ma deve permeare l'intera attività del Consiglio, grazie all'*induction* dei consiglieri di amministrazione e dei componenti degli organi amministrativi, che devono possedere competenze sempre più avanzate in governance della cybersecurity.

In tal modo, il legislatore italiano ha ulteriormente implementato il carattere multilivello e multi-responsabilità di questa normativa di settore, introducendo logiche di diritto punitivo mediante la creazione di un sistema sanzionatorio estremamente oneroso in caso di mancata conformità.

### 4.2. I presidi a tutela della sicurezza informatica della supply-chain

L'articolo 30, paragrafo 2, del Regolamento DORA stabilisce una serie di criteri guida applicabili a tutto il ciclo di vita dell'accordo commerciale, che includono le fasi di conclusione, di esecuzione, di cessazione e anche il periodo post-contrattuale[56]. La disposizione in esame stabilisce, altresì, un repertorio di standard minimi, al fine di armonizzare le condizioni di fornitura dei servizi ICT nel mercato europeo.

Tra i requisiti che incidono maggiormente sulla capacità dell'organizzazione di garantire la propria sicurezza informatica, si menziona, in primo luogo, quello di cui alla lettera e), che, nell'ottica di implementare i presidi a fronte di *cyber-risk*, prevede specifiche previsioni in riferimento ai livelli di servizio, ossia la metrica del servizio che il fornitore si impegna a rispettare. L'obiettivo è quello di misurare la qualità del servizio erogato, definendo il livello qualitativo standard garantito, a cui vengono associati parametri oggettivi per monitorarne il rispetto. Questi parametri, noti come *Key Performance Indicators* (KPI), comunemente vengono valutati attraverso strumenti e software dedicati, nonché algoritmi di calcolo. A titolo esemplificativo, per l'ipotesi di erogazione di un servizio di data center, gli indicatori chiave di qualità del servizio possono essere distinti in quattro categorie: la disponibilità, la reattività a un input, il rispetto dei tempi di reportistica e la performance.

Corre l'obbligo di evidenziare che, seppure i contratti in esame rientrino, nella maggior parte dei casi, nella categoria dei contratti di durata, essi sono soggetti a una rapida obsolescenza tecnologica[57], con la conseguenza che si rende necessario

depositi e prestiti e gli intermediari finanziari di cui al TUB, con la specificazione che Banca d'Italia può individuare una categoria di intermediari da considerarsi significativi anche per tipologia di attività svolte e a cui applicare il management framework completo in luogo di quello semplificato. La normativa ha introdotto forme mirate di accordo informativo tra le Autorità competenti DORA e la Guardia di Finanza. Tale intervento è strettamente legato al fatto che gli incidenti che hanno un impatto su reti, sistemi informativi e servizi informatici inerenti al settore finanziario possono derivare da attacchi esterni compiuti da soggetti non interessati soltanto a testare la vulnerabilità dei livelli di sicurezza, bensì anche ad acquisire la disponibilità di dati ed elementi informativi di carattere strategico in grado di minare gli interessi economico-finanziari del Paese e suscettibili di essere sfruttati per fini illeciti, *in primis* nel settore dei mercati finanziari, immobiliari, nonché in quello fiscale, doganale, della spesa pubblica e in materia di valuta, titoli, valori e mezzi di pagamento. Per tale ragione, è stato previsto il coinvolgimento della Guardia di Finanza, istituzione cui è normativamente riconosciuta la competenza per la ricerca, la prevenzione e il contrasto degli illeciti economico-finanziari perpetrati sfruttando i mezzi tecnologico-informatici.

55. Cfr. art. 10 d.lgs. n. 23/2025. Queste sanzioni non sono assicurabili con polizze e rendono tale disciplina sensibilmente diversa rispetto a quella prevista dalla Direttiva NIS II e recepita in Italia con il d. lgs. n. 138 del 2024.
56. La materia è stata ampiamente tratta anche da Pérez Carrillo 2023, p. 1151.
57. In questi termini si sono espressi Portolano–Mazza 2023.

che i fornitori positivizzino all'interno delle scritture contrattuali il grado di evoluzione informatica che sono in grado di raggiungere con le proprie infrastrutture e con i propri servizi informatici e il cui rispetto si impegnano a garantire mediante la stipula.

Il service provider è tenuto a descrivere puntualmente i livelli di servizio, che si traducono nell'assunzione di obbligazioni, attraverso l'accordo su standard tecnici e qualitativi, metriche di performance attese, penali e modalità di monitoraggio e *reporting*. Questo aspetto è particolarmente rilevante nel contesto della *supply chain*, dove il livello di servizio è un indicatore chiave della probabilità di evitarne una carenza e della capacità dell'entità finanziaria di soddisfare le richieste e le aspettative dei clienti.

In aggiunta, è necessario che il fornitore, considerata la velocità dell'innovazione tecnologica, si impegni a prevedere e effettuare processi periodici di revisione e aggiornamento degli SLAs, allo scopo di neutralizzare, quanto possibile, il pericolo che i servizi prestati si rivelino obsolescenti, così ponendo in serio pericolo la *business continuity* dell'entità finanziaria.

Estremamente rilevante appare anche la previsione di cui alla lettera f), che impone di prevedere, in sede contrattuale, la prestazione di assistenza senza costi aggiuntivi ovvero ad un costo stabilito *ex ante* qualora si verifichi un incidente connesso al servizio ICT prestato. Il verificarsi di un incidente informatico costituisce uno degli scenari peggiori ai quali l'entità finanziaria può andare incontro e al ricorrere del quale risulta di cruciale rilevanza il ruolo e la collaborazione prestata dal fornitore che eroga e gestisce, altresì in termini di manutenzione, il servizio oggetto di minaccia. Al fine di garantire la massima tempestività nell'intervento, il fornitore dovrebbe predeterminare il costo dell'assistenza che si impegna a garantire, secondo condizioni economiche definite già in sede contrattuale. Il profilo della predeterminazione dei costi consente di intervenire con prontezza e, in tali casistiche, la rapidità della risposta può permettere una ristrutturazione del servizio tanto più proficua e sicura. Considerata la difficoltà di prevedere *ex ante* tutti i possibili casi di incidente ICT e i rimedi necessari per ciascuno di essi, sarebbe opportuno che il fornitore prevedesse, in sede contrattuale, esemplificazioni, da ritenersi non esaustive. Il contratto di fornitura potrebbe stabilire specifiche procedure di intervento in ordine ad ogni potenziale *cyber attack*, in riferimento a ciascuna sezione di funzionamento del servizio e assetti incentrati sul calcolo dei "giorni uomo", ovvero delle "ore uomo", richiesti per la gestione e l'efficace e tempestiva risoluzione dell'incidente di sicurezza informatica. L'entità finanziaria dovrebbe, quindi, verificare la completa e esaustiva predisposizione di un impianto contrattuale avente a oggetto le procedure e le tempistiche che devono essere osservate, i soggetti che gestiscono le comunicazioni e quelli che forniranno concretamente supporto ai fini del ripristino dei sistemi interessati dall'incidente.

Ulteriori e vieppiù pregnanti obblighi sono poi previsti dall'articolo 30, paragrafo 3, in relazione ai fornitori di funzioni essenziali ovvero importanti. L'incidenza di tali attività sui risultati finanziari e sulla solidità e continuità dei servizi giustifica, secondo il legislatore europeo, l'introduzione di un regime "aggravato" che impone previsioni volte a rafforzare i vincoli contrattuali[58]. La legislazione eurounitaria ha implementato standard minimi inerenti la descrizione dettagliata dei livelli di servizio, e, nello specifico, ha imposto, in sede contrattuale, l'esaustiva indicazione degli obiettivi quantitativi e qualitativi perseguiti, affinché l'entità finanziaria possa svolgere un proficuo monitoraggio, altresì, in termini di applicazione di misure correttive per il caso di violazione da parte del fornitore degli SLAs concordati. Inoltre, il fornitore dovrebbe essere tenuto contrattualmente ad impegnarsi a comunicare all'entità finanziaria, entro un congruo termine, l'implementazione di sviluppi tecnici, informatici ovvero tecnologici all'erogazione del servizio che potrebbero alterarne, ovvero comprometterne, la stabilità, oppure la sicurezza dei prodotti o del servizio erogato, e, non da ultimo, il soddisfacimento dei livelli di servizio assicurati.

Al fine di salvaguardare la sicurezza informatica delle ICT, il fornitore FEI dovrebbe impegnarsi a partecipare allo svolgimento del *threat-led-penetration-test*, per tale intendendosi un quadro informatico in grado di imitare le tecniche e le procedure di attori reali che generano minacce e che vengono percepiti come una minaccia autentica.

58. Così Pignatti 2024, p. 663.

Tale test consente di eseguire una verifica in ordine ai sistemi di produzione attivi e critici, in maniera controllata, mirata e basata sull'analisi della vulnerabilità, con l'obiettivo di esaminare le capacità difensive e migliorarle. Attraverso tali test, un attacco cyber non viene semplicemente simulato, bensì realmente realizzato per mettere alla prova la tenuta del sistema di sicurezza apprestato. I risultati del test, che deve essere effettuato ogni tre anni, vengono utilizzati per determinare le misure correttive volte ad implementare la *cyber-resilience* dell'entità finanziaria.

Infine, il contratto di fornitura di servizi FEI dovrebbe prevedere una disciplina stringente in punto di risoluzione contrattuale, mediante la predisposizione esaustiva di strategie di uscita, che rispondono alla finalità di proceduralizzare dei periodi di transizione obbligatori, durante i quali il fornitore deve continuare a prestare i propri servizi, allo scopo di ridurre il rischio di perturbazioni in capo all'entità finanziaria. L'obiettivo è, dunque, quello di consentire all'organizzazione di superare l'attacco in modo contenuto e senza inconvenienti, mediante l'utilizzo di altri fornitori ovvero, in alternativa, l'adozione di soluzioni interne, in funzione della complessità del servizio. Analogamente a quanto detto in riferimento agli SLAs, anche le strategie di uscita dovrebbero tenere conto dei rischi che la risoluzione del contratto di esternalizzazione potrebbe determinare nella *business continuity* aziendale, anche a causa di possibili disfunzioni dei fornitori, ovvero del deterioramento della qualità dei servizi in considerazione dei rischi di indisponibilità, del degrado dei livelli di servizio, dei cambiamenti rilevanti sulla fornitura sino alla risoluzione del contratto. A titolo esemplificativo, dovrebbero essere contemplate ipotesi di perturbazione dell'attività commerciale conseguente a una fornitura inadeguata o carente, oppure di gravi rischi connessi all'adeguatezza e alla continuità del servizio. I piani preventivi di uscita sono volti a consentire all'intermediario di esercitare la risoluzione senza arrecare disagio, ovvero sconvolgimento alcuno, alle proprie attività commerciali e in assenza di impatti sul rispetto dei requisiti normativi e all'operatività della *supply chain*, ivi compresa la qualità dei servizi forniti ai clienti finali. Infine, le *exit strategies* dovrebbero essere documentate accuratamente e sottoposte a test periodici che ne garantiscano la revisione e l'aggiornamento, al fine di garantire una piena e quanto più attenta conformità allo sviluppo tecnologico raggiunto sia dall'entità finanziaria sia dal fornitore. I piani di uscita dovrebbero essere realistici, fattibili e basati su scenari plausibili, oltre che prevedere un calendario di attuazione compatibile con le condizioni stabilite negli accordi contrattuali.

L'obiettivo finale consiste nel consentire all'entità finanziaria di identificare prontamente eventuali disfunzioni potenziali dei fornitori, nonché eventuali deterioramenti della qualità dei servizi e perturbazioni. Questo al fine di attivare meccanismi che consentano la risoluzione delle problematiche senza arrecare pregiudizio alla compliance, alla continuità e alla qualità dell'attività commerciale.

### 4.3. L'impatto del Regolamento DORA sulla prassi contrattuale attuale

In un contesto caratterizzato da una certa difficoltà degli operatori finanziari nell'imporre ai fornitori l'adozione di clausole contrattuali specifiche, assumono rilevanza gli obblighi che il quadro giuridico vigente impone alle entità finanziarie e ai fornitori. Questi ultimi, infatti, in sede di implementazione italiana del Regolamento DORA, sono divenuti anch'essi destinatari dell'oneroso quadro sanzionatorio previsto in caso di mancata conformità alla normativa. Un'attenta analisi ha messo in luce come gli obblighi in questione contribuiscano, seppur indirettamente, a garantire agli operatori finanziari una posizione di forza nelle trattative con il settore ICT, mitigando il rischio di svantaggio. In considerazione del quadro delineato, gli elementi standardizzati possono costituire un utile strumento per contrastare comportamenti opportunistici da parte dei fornitori. Tuttavia, non si può trascurare il fatto che le aziende ICT, oltre alla fase di conclusione dei contratti, sono in grado di esercitare un'influenza significativa anche sull'effettiva e corretta esecuzione delle prestazioni, poiché detengono un *know-how*, nella maggior parte dei casi esclusivo, proprio in tale ambito[59].

59. Il tema dello squilibrio delle competenze *tech* dell'organo di gestione nell'ambito di applicazione della normativa DORA è stato affrontato anche da Alfano 2024.

Le Autorità nazionali ed europee, nell'esercizio delle loro funzioni di vigilanza sulla gestione dei rischi e sull'attività contrattuale con i fornitori, svolgono un ruolo fondamentale di strumenti istituzionali di garanzia, mitigando le asimmetrie informative e promuovendo la tutela del risparmio. In merito, mentre la vigilanza interna garantisce un livello minimo di autonomia tecnica dell'operatore rispetto ai fornitori di servizi ICT, la vigilanza esterna rende i fornitori, generalmente non esercenti direttamente attività finanziarie in senso stretto, soggetti, invece, alla vigilanza delle Autorità garanti dei settori finanziario, bancario e assicurativo, soggiacendo così alla disciplina specifica di settore. Il quadro così delineato riveste una particolare rilevanza, promuovendo la cooperazione e il coordinamento delle attività delle Autorità attraverso una rete comune, fattore determinante per la stabilità del mercato europeo[60].

Dal punto di vista dell'operatore, la disparità di potere contrattuale rispetto al fornitore ICT si traduce nella corrispondente esigenza di possedere competenze tecniche adeguate, anche attraverso il rafforzamento del ruolo della vigilanza interna, che si estende alla gestione dell'evoluzione tecnologica dei servizi esternalizzati[61]. È evidente, infatti, l'elevato grado di sofisticazione che ispira la disciplina europea, che è stata in grado di coniugare due discipline a tutt'oggi strettamente interdipendenti: il diritto e l'informatica. Come evidenziato dall'analisi dei requisiti contrattuali, il legislatore ha operato un'attenta integrazione di regole tecniche e regole giuridiche[62], conseguendo un equilibrio armonioso tra i due settori. Tuttavia, a fronte della commistione nella progettazione della disciplina di tali saperi, si rende necessario che l'implementazione sia affidata a persone, sia fisiche che giuridiche, che possiedono la competenza necessaria per gestire ambedue i volti della nuova legislazione, al fine di garantire il rispetto e la piena valorizzazione di entrambi i caratteri della normativa.

Con l'intento di intervenire sui fragili equilibri di autonomia privata, il Regolamento DORA propone un nuovo paradigma di gestione integrata dei rischi cibernetici, in sinergia con le altre voci di rischio rilevanti, introducendo un nuovo modello di *best practice* per le modalità e i contenuti con cui ha intercettato un ambito di rischio del mercato finanziario in evoluzione esponenziale.

La nuova regolamentazione ha, inoltre, coinvolto tutti gli stakeholders nel processo di implementazione, mediante l'elaborazione di un insieme di norme che partono da principi generali e giungono sino a quelli più tecnici di cui agli RTS e agli ITS[63], mantenendo la flessibilità di individuare il punto di equilibrio tra il principio di proporzionalità e la gestione della complessità.

L'obiettivo principale è stato attribuire alle entità finanziarie un ruolo proattivo e propositivo nella governance della *supply chain*, al fine di garantire che l'esternalizzazione venga progettata e formalizzata attraverso tavoli negoziali di proficuo dialogo tra le parti interessate, in grado di considerare le reciproche esigenze e consolidare una partnership produttiva e duratura con il fornitore, che riveste un ruolo di estrema rilevanza nell'assicurare la resilienza operativa digitale dell'organizzazione.

60. Per un approfondimento in relazione alla figura dei fornitori critici, vedasi Pignatti 2024, pp. 663-664.

61. La riflessione che si condivide è stata tratta da Pignatti 2024, pp. 666-667.

62. Sul concetto di comprensione della regola tecnologica ai fini di una corretta interpretazione delle fattispecie legali si rinvia a Flor 2022, p. 143.

63. I regolamenti RTS e ITS rappresentano norme tecniche di dettaglio sviluppate dalle Autorità europee di vigilanza (EBA, ESMA, EIOPA) per specificare come applicare concretamente i requisiti di resilienza operativa digitale. Gli RTS (*Regulatory Technical Standards)* prevedono i criteri per la classificazione degli incidenti gravi, i requisiti per la gestione dei rischi ICT e le politiche di sicurezza per i fornitori terzi critici. Gli ITS (*Implementing Technical Standards)* forniscono modelli uniformi, formati e procedure per la segnalazione degli incidenti e la tenuta del registro delle informazioni sui contratti ICT. Di seguito i riferimenti: Regolamento delegato UE 2024/1772, Regolamento delegato (UE) 2024/1773, Regolamento delegato (UE) 2024/1774, Regolamento di esecuzione (UE) 2024/2956, Regolamento Delegato (UE) 2025/301, Regolamento di esecuzione (UE) 2025/302, Regolamento Delegato (UE) 2025/532, Regolamento delegato (UE) 2025/420.

## 5. Il Regolamento DORA come modello di best practice e la cybersecurity come nuova architrave normativa dei mercati digitali

La prospettiva delineata suggerisce che il Regolamento DORA ha contribuito a istituzionalizzare la responsabilità preventiva delle organizzazioni economiche coinvolte, affiancando alla sanzione postuma una *cyber-compliance* dinamica, che prevede l'obbligo di anticipare, gestire e condividere il rischio informatico con tutti i soggetti che compongono la catena di erogazione del servizio, da quelli privati alle Autorità garanti.

In quest'ottica, la normativa europea può ritenersi convogliare nel novero di quei modelli di co-regolazione[64] che si caratterizzano per l'adozione di forme di *responsive regulation*, note per reagire ai fallimenti e alle inefficienze dei mercati mediante la promozione di strategie di governance aziendali da attuarsi mediante la delega normativa delle funzioni di regolamentazione alle persone giuridiche private, seppur sotto il controllo rigoroso delle Autorità pubbliche deleganti[65].

L'architettura DORA, fondata su un paradigma virtuoso, configura un sistema regolatorio binario: preventivo-proattivo nella struttura, attraverso la regolamentazione preventiva dei processi e la gestione cautelativa dei rischi, e punitivo nella reazione, mediante la previsione di sanzioni economiche e interdittive di notevole entità. Il legislatore europeo, mediante la previsione di obblighi di conformità normativa in materia di cybersecurity, mira a neutralizzare le forme di criminalità informatica in una prospettiva *ex ante*, ovvero, sin dal momento della configurazione contrattuale del servizio attraverso il quale la minaccia si potrebbe introdurre. In linea con la necessaria anticipazione del momento di tutela nell'ambiente digitale, il congegnato meccanismo preventivo richiede la partecipazione attiva e fattiva delle entità private, anche in termini di cooperazione con le Autorità garanti. In assenza, troverà applicazione un sistema sanzionatorio basato su logiche di diritto punitivo.

Il legislatore ha adottato un approccio omnicomprensivo e poliedrico al fenomeno della criminalità informatica, sviluppando strategie trasversali di carattere multilivello. In primo luogo, l'attenzione è stata focalizzata sulle potenzialità degli strumenti precauzionali in grado di prevenire il *cybercrime*, a partire dalla sicurezza informatica, che emerge come la nuova architrave normativa dei mercati digitali. In tale contesto, le entità private sono soggette a un duplice livello di attenzione: il sistema europeo le considera come attori chiave del sistema preventivo, che supporta il sistema di stampo repressivo, variamente implementato in forza della potestà legislativa diretta conferita dall'art. 83 TFUE[66].

La dimensione penalistica della regolamentazione assume una rilevanza sistematica: l'accountability organizzativa si collega concettualmente con la colpa per omessa vigilanza, figura cardine del diritto penale dell'economia. Il Regolamento DORA, nel delineare un sistema di responsabilità proattiva degli operatori finanziari, concepisce l'accountability come un parametro di diligenza qualificata, la cui violazione integra non soltanto un deficit di compliance regolamentare, ma può fungere da indice sintomatico di colpa ai fini della responsabilità penale personale del management e di quella para-penale dell'ente. Difatti, i reati informatici, ai sensi degli artt. 24 e 24-*bis* del D.lgs. 231/2001, sono reati presupposto della responsabilità amministrativa degli enti[67] e parimenti deve dirsi per il trattamento illecito di dati in violazione del Regolamento UE 679/2016 (GDPR), che definisce la "violazione dei dati personali" una "violazione di sicurezza" [68], cui segue la necessità di un raccordo

64. Questa definizione di co-regolazione è richiamata da Licastro 2025, p. 95 che rinvia a riguardo a Black 2001, p. 117.
65. Per una disamina in materia di *responsive regulation* cfr. Ayres–Braithwaite 1992, p. 4.
66. Per un approfondimento sugli obblighi di penalizzazione europei vedasi Vadalà 2025, pp. 103-175.
67. In particolare, dopo l'introduzione dell'articolo 24-*bis*, che ha esteso il catalogo dei reati presupposto per includere varie fattispecie di *cybercrime*, come l'accesso abusivo, il danneggiamento di sistemi informatici, e le frodi informatiche, in seguito alla ratifica della Convenzione di Budapest sulla criminalità informatica con la legge 48/2008. Per questi profili cfr. Piva 2022, p. 525 ss.
68. Basti pensare che rispetto agli adempimenti imposti dal GDPR, la *cybersecurity* costituisce un "presidio comune", così Romolotti 2019.

tra la prevenzione da attacchi a danno dell'impresa e quella avente ad oggetto, ai sensi dell'art. 5 del d.lgs. 231/2001, reati informatici commessi anche o soltanto nel suo interesse o vantaggio[69]. Siamo di fronte all'ennesimo banco di prova della governance aziendale, che può comportare persino una responsabilità penale e a titolo di concorso per omesso impedimento dell'evento *ex* artt. 110 e 40 cpv. c.p. Ciò in quanto, il principio di "digital due diligence", che permea la normativa europea sulla resilienza operativa, si traduce in un nuovo standard di colpa specifica, in grado di ridefinire i confini della colpevolezza omissiva nell'epoca della digitalizzazione. La creazione di un sistema di governance efficace non garantisce esclusivamente un vantaggio competitivo, ma implica anche l'assunzione di un impegno organizzativo rigoroso e la mancata ottemperanza, indipendentemente dagli obblighi settoriali sanzionati amministrativamente o penalmente, può comportare responsabilità di natura apicale, in quanto la protezione dei dati è diventata una condizione imprescindibile per la stessa sopravvivenza[70] dell'entità finanziaria.

In tale prospettiva, la cybersecurity si configura come l'architrave normativa della legalità economica e digitale europea: essa non può più essere considerata esclusivamente come un requisito tecnico, ma piuttosto come un bene giuridico collettivo di nuova generazione[71], la cui tutela è garantita sia dal diritto penale che dal diritto della concorrenza. Vieppiù, essa dovrebbe costituire il parametro razionale per l'orientamento delle scelte di politica criminale, valorizzando la sua qualifica di *comprehensive concept*, "sostanziale" e "prepositivo", edificato su un triplice livello: infrastrutture, informazioni e tutela dei dati personali[72]. Soltanto tale accezione può essere in grado di guidare in maniera coerente e sistematica l'attività del legislatore. Una concezione che ne riconosca la natura composita e trasversale consente, infatti, di ancorare le scelte legislative a una lettura sostanziale e non meramente formalistica dei beni giuridici, sottraendoli a mere contingenze emergenziali o a pressioni tecnocratiche. Non vi è dubbio che, al fine di contrastare efficacemente la criminalità informatica, è necessario dotarsi di strumenti tecnologici avanzati; tuttavia, questi non possono essere impiegati in modo tecnocratico.

Ne consegue che la sicurezza informatica emerge come un ambito di pertinenza per la costruzione di interventi normativi proporzionati, razionali e orientati alla tutela effettiva dei diritti fondamentali[73], contribuendo a edificare un diritto penale della sicurezza digitale che sia al contempo efficace e garantista. Tale traguardo rappresenta, a sua volta, un presupposto fondamentale per l'architettura del sistema di giustizia penale nell'era digitale.

In conclusione, il modello DORA assume una configurazione circolare e non può essere considerato esclusivamente una disciplina settoriale, ma fornisce una grammatica giuridica comune che utilizza il linguaggio della resilienza e della cooperazione per la governance dei mercati digitali. La grammatica delineata si fonda su cinque concetti chiave: accountability, testing, auditing, reporting e vigilanza coordinata.

La sua esportabilità si radica nella capacità di promuovere l'interoperabilità e la fiducia tecnologica tra gli operatori economici e di diffondere la cultura della prevenzione e della cyber-resilienza come criterio di legittimazione dell'attività economica digitale.

La sfida che si potrebbe prospettare è quella di estendere tale paradigma a tutti i mercati digitali, al fine di garantire che il principio di resilienza operativa digitale venga pienamente riconosciuto come la nuova misura della legalità tecnologica.

In tale contesto, il giurista non può limitarsi a una mera interpretazione della norma, ma è chiamato a contribuire alla costruzione di una cultura della sicurezza informatica condivisa, in cui il diritto diventa il linguaggio della fiducia tecnologica. Tale trasformazione sembra indicare l'emergere di una nuova metodologia, strettamente legata al concetto di "diritto penale della sicurezza digitale", volta alla costruzione di un sistema normativo

69. In tema, Razzante 2022, p. 34 ss.

70. In materia di obblighi di agire informato dei soggetti apicali cfr. Mongillo 2022, p. 2.

71. In questo senso vedasi Flor 2023, pp. 126-129.

72. La considerazione qui espressa trova approfondimento in Flor 2023, pp. 144-145.

73. Sul concetto di *cybersecurity* come di un nuovo diritto fondamentale si rinvia a Papakonstantinou 2022.

caratterizzato da affidabilità sistemica anche sul piano tecnologico. In tal modo, la prevenzione, che tradizionalmente ha rivestito un ruolo "debole", viene potenziata, assumendo valore cogente e misurabile attraverso procedure di audit e di vigilanza.

## 6. Riflessioni conclusive. I caratteri "mobilitatori" del diritto penale della sicurezza digitale

L'indagine ha perseguito l'obiettivo di articolare una proposta di lettura dell'attuale fisionomia del diritto penale nella specifica materia della sicurezza digitale, concentrandosi sui profili strutturali, assiologici e funzionali che ne definiscono l'essenza e ne orientano le traiettorie evolutive, con particolare attenzione alle implicazioni derivanti dalla progressiva permeabilità delle tecnologie nei processi giuridici ed economici. Dinanzi all'avanzata incessante della rivoluzione digitale – fenomeno caratterizzato da rapidità trasformativa e da tratti di contingente[74] instabilità, che ne accentuano la complessità, – la strategia che appare metodologicamente più efficace per contenere il disorientamento sistemico indotto da tale evoluzione sembra rinvenirsi nel ricorso al sistema delle definizioni. Tale sistema, concepito come strumento di delimitazione concettuale e presidio della funzione di garanzia propria del diritto, è inteso quale baluardo della certezza normativa e della tutela dei valori fondamentali dell'ordinamento.

L'individuazione dei caratteri "facilitatori" e "mobilitatori"[75] della scienza penalistica nell'era digitale ha costituito lo scopo finale della riflessione, scaturita dall'analisi delle scelte legislative a livello europeo, delle quali il Regolamento DORA, concepito per contrastare i fenomeni di criminalità informatica in un settore di assoluta strategicità per il sistema Paese e per il mercato unico eurounitario, rappresenta un esempio virtuoso. L'intento è stato quello di tentare di fornire un contributo all'edificazione di un paradigma penalistico valido nel quinto dominio, in cui si intersecano tecnologie, tangibili e intangibili, e innovazione.

In primo luogo, si osserva il carattere *binario* delle scelte legislative in parola, che perseguono non soltanto la funzione repressiva, ma anche una componente *preventiva*, che assume una duplice rilevanza, sistemica e sistematica. La scienza penalistica, intesa come strumento di repressione, è concepita esclusivamente per l'essere umano. Tuttavia, nel contesto dei reati informatici, una delle ulteriori finalità che possono sostenerla e aggiornarla è la prevenzione, intesa come il complesso di misure e presidi di matrice culturale, tecnico-informatica e giuridica, che, in un'ottica precauzionale, sono in grado di scongiurare gli effetti potenzialmente deleteri della criminalità informatica.

A tutt'oggi, come evidenziato dalle previsioni del Regolamento DORA, i meccanismi preventivi si concentrano sulla creazione di condizioni organizzative e tecnologiche adeguate a neutralizzare una serie ampia di rischi calcolati e coinvolgono gli assetti aziendali, le infrastrutture tecniche disponibili, le filiere di fornitura avviate e gli ecosistemi di dati oggetto di trattamento.

Nello scenario tecnologico, le attività preventive e repressive, tradizionalmente considerate separate, formano un sistema complesso e dinamico, paragonabile a una fitta rete di "vasi comunicanti"[76]. Questa interconnessione si manifesta con particolare evidenza nel cyberspazio, in cui le categorie tradizionali del diritto penale vengono significativamente sollecitate, a causa dell'asimmetria strutturale tra la velocità elevata con cui si sviluppa l'azione criminale e la lentezza delle risposte repressive.

Per tale ragione, la giustizia penale ha sviluppato una tendenza alla proiezione anticipatoria rispetto alla commissione del fatto di reato, finalizzata a neutralizzare le cyber minacce prima ancora che esse si concretizzino, attraverso l'implementazione di meccanismi di gestione preventiva, quali la cybersecurity, che si configura come un nuovo

74. Sul carattere contingente della tecnologia si rinvia a Calo 2026.

75. L'aggettivo "mobilitatore" è stato tratto dal Rapporto *Molto più di un mercato: velocità, sicurezza, solidarietà. Potenziare il mercato unico per garantire un futuro sostenibile e la prosperità di tutti i cittadini dell'UE* presentato il 18 aprile 2024 dall'ex Presidente del Consiglio italiano Enrico Letta al Consiglio europeo. Il rapporto mira a contribuire alla riflessione sul futuro dell'Unione europea e alla predisposizione dell'Agenda Strategica del Consiglio europeo per il periodo 2024-2029.

76. Aprati 2023, p. 469.

paradigma di diritto preventivo operante non solo su un piano individuale, ma anche su quello collettivo e collettivistico delle strutture e delle infrastrutture.

In tale prospettiva, il penalista è chiamato a concepire la sicurezza informatica come un bene giuridico collettivo, che incarna non soltanto la protezione dell'individuo, ma anche la stabilità e l'integrità dei sistemi tecnologici, da proteggere con strumenti normativi coordinati, quali standard minimi di sicurezza, obblighi di segnalazione di incidenti, piani di continuità operativa e sistemi di certificazione dei processi interni ed esterni.

La metodologia applicata dal legislatore europeo sembra focalizzata sulla *prevenzione situazionale*, con l'intento di ridurre le probabilità di attacco mediante la gestione di scenari critici e l'identificazione di situazioni a rischio, con l'obiettivo di sviluppare risposte che garantiscano un margine di sicurezza concreto.

Il volto preventivo del diritto penale nell'era digitale si caratterizza per la già menzionata ibridazione con il diritto amministrativo, nonché con il diritto della regolazione economica e il sapere tecnico-informatico. Alla sanzione viene affiancata la costruzione di comportamenti organizzativi virtuosi, la cui omissione determina l'applicabilità di sistemi di diritto punitivo, ossia sanzioni amministrative.

In questi termini, emerge il carattere *proattivo* del diritto penale contemporaneo, che non si limita più alla mera repressione del fatto, ma, nel cyberspazio, impone una riorganizzazione della risposta statale e privata secondo modalità, forme e tempi nuovi, allontanandosi dalla sua immagine tradizionale. La trasformazione concettuale attiene alla già citata traduzione della categoria del rischio informatico in una categoria autonoma di diritto, da cui discende l'obbligo di rispettare vincoli di governance interna ed esterna, e responsabilità operative. In quest'ottica, il Regolamento DORA impone alle entità finanziarie (e il d.gs. n. 23/2025 anche ai fornitori) rilevanti obblighi di conformità normativa, prescrivendo standard contrattuali minimi nell'esternalizzazione dei servizi ICT e concepisce l'accountability come un parametro di diligenza qualificata, che si collega concettualmente alla colpa per omessa vigilanza, la cui violazione integra non soltanto un deficit di compliance regolamentare, ma può fungere da indice sintomatico di colpa ai fini della responsabilità penale personale del management e di quella para-penale dell'ente. Per l'effetto, le suddette entità sono tenute a svolgere un ruolo attivo, propositivo e partecipativo sia nel corso delle trattative contrattuali con i fornitori, sia nella propria governance interna, oltre che, ovviamente, nei rapporti con le Autorità garanti, pena l'irrogazione delle sanzioni previste dalla normativa.

Inoltre, è stato osservato che la normativa analizzata presenta un carattere spiccatamente *multidisciplinare*, sintomatico della complessità ontologica del fenomeno criminale in esame. Le sfide emergenti poste dal cybercrime hanno condotto il legislatore europeo a una rilevante trasformazione concettuale: il rischio tecnologico non può e non deve più essere eluso, ma governato. Il passaggio "dal rischio al diritto" ha segnato una rivoluzione epocale nella gestione e nella neutralizzazione dei rischi informatici, introducendo normative fondate su strategie trasversali di prevenzione, sia di carattere tecnico che giuridico. L'approccio integrato, che unisce il diritto penale, il diritto amministrativo, il diritto dell'informatica e la regolazione dei mercati, ha elevato il concetto di resilienza operativa digitale a principio di governance, con una funzione paragonabile a quella della stabilità finanziaria. Nel laboratorio giuridico europeo, la resilienza operativa è stata elevata a indicatore di affidabilità dell'intero ecosistema, incarnando la trasposizione giuridica della fiducia tecnologica. A conferma di tale transizione, il Regolamento DORA stabilisce un modello normativo che traduce il linguaggio tecnico della gestione del rischio in linguaggio giuridico. Il nuovo paradigma di gestione integrata dei rischi cibernetici risponde a un elevato livello di sofisticazione tecnica, sia a livello tecnologico che a livello giuridico, e richiede il rispetto di numerosi obblighi contrattuali che necessitano del possesso di specifiche competenze e conoscenze in materia di obsolescenza tecnologica, procedure e tempistiche di gestione di un incidente ICT, analisi e gestione dei rischi, implementazione di stress test, metriche di performance attese, sviluppi tecnici, strategie di uscita, attività di monitoraggio e di reporting, attenzione ai contenuti contrattuali e ai regimi di responsabilità. Il grado di tecnicità richiesto dai nuovi requisiti contrattuali minimi è evidenziato dalla severa produzione normativa

che interessa i Regolamenti di secondo livello, i già menzionati RTS e ITS.

La vigilanza interna dell'entità finanziaria si estende, pertanto, alla gestione dell'evoluzione tecnologica dei servizi esternalizzati e la disciplina si distingue per una profonda consapevolezza della dinamicità e della mutevolezza del mercato di riferimento, delineando un modello di gestione che affida a tutti i soggetti della filiera l'identificazione delle metodologie ottimali e degli strumenti più adeguati, al fine di garantire un assetto nel quale operano una sostanziale conformità con gli obiettivi e i contenuti della normativa.

In tale scenario, il diritto penale non può più limitarsi alla mera considerazione del fattore umano, ma dovrebbe, invece, integrarlo con il dato tecnologico e prestare attenzione alle potenzialità insite negli strumenti precauzionali, come la cybersecurity, che diventa il criterio ordinante dell'intera normativa.

Non da ultimo, il diritto penale all'epoca della sicurezza digitale richiede l'implementazione di tattiche di difesa attiva, che si configurano come forme di *cyber compliance* dinamica di carattere *multilivello*, e prevedono l'obbligo di anticipare, gestire e condividere il rischio ICT con tutti i soggetti che compongono la catena di erogazione del servizio. Questo implica il coinvolgimento attivo di tutte le entità private, ossia le organizzazioni operanti nel settore finanziario, bancario e assicurativo, i fornitori di servizi ICT, e pubbliche, che compongono la rete comune di protezione dei nuovi interessi nell'era digitale, quale fattore determinante per la stabilità del mercato europeo, coinvolgendo diversi livelli di governo aziendale, economia e società, tra i quali personale dipendente, consigli di amministrazione e Autorità garanti, nazionali ed europee.

A ciò si aggiunga che è prevista una stretta collaborazione tra tutti gli attori coinvolti, secondo logiche di *co-regolazione* o di *regolazione partecipativa*, tra il regolatore, il regolato e le Autorità "*guardiane*". Tale meccanismo riecheggia le forme di cooperazione pubblico-privata già note al legislatore europeo nell'ambito del diritto penale processuale e si ritiene, pertanto, che la normativa stia evolvendo verso la riproposizione di tali modelli collaborativi virtuosi anche nel contesto del diritto penale sostanziale.

Il discorso sulla fisionomia del diritto penale dell'informatica e, più nello specifico, del "diritto penale della sicurezza digitale" costituisce un tema *in fieri*: la sua evoluzione risentirà, inevitabilmente, degli strumenti con cui il penalista affronterà e maneggerà la sfida tecnologica.

La scienza penalistica, storicamente antropocentrica, risulta, tuttora, impreparata rispetto alle peculiarità e alla velocità che caratterizzano la rivoluzione tecnologica. In assenza di sviluppi rilevanti, sussiste il rischio che il diritto penale non riesca a preservare la propria competitività e la propria capacità deterrente rispetto a fenomeni che possiedono il potenziale di innescare reazioni a livello globale.

Il contributo si prefigge di offrire una lettura della normativa esaminata, concepita come proposta di riflessione destinata a contribuire al dibattito sulle dinamiche evolutive del diritto penale. Attualmente, la sua frammentazione interna, la sua visione persistentemente antropocentrica, la sua spiccata reattività e l'isolamento rispetto alle altre discipline, configurano un insieme di fattori che possono collocarlo in una condizione di criticità operativa. Tuttavia, tali limiti non possono essere invocati per giustificare una resa concettuale o metodologica della scienza penalistica.

Al contrario, la traiettoria delineata dal legislatore europeo – che promuove il riconoscimento della rilevanza di strumenti di contrasto preventivo, fondati su logiche punitivo-proattive, multidisciplinari, multilivello e di co-regolazione – si configura come un approccio potenzialmente capace di farsi carico delle sfide emergenti poste dalla criminalità informatica, conciliando rigore normativo e funzionalità.

La possibile soluzione all'attuale *impasse* tecnologico, a sostegno della scienza penalistica, sembra rinvenirsi nella costruzione di una sinergia tra i diversi saperi disciplinari e nella valorizzazione dell'eterogeneità degli strumenti adottati, anche con riferimento ai differenti destinatari della normativa. Tale approccio consente, da un lato, di potenziare l'efficacia della risposta penale e, dall'altro, di fronteggiare in maniera consapevole le potenzialità lesive insite nei dati, i quali rappresentano la nuova incarnazione tecnologica del potere e, al contempo, un terreno complesso di tensione tra innovazione, controllo e responsabilità.

Il Regolamento DORA rappresenta una testimonianza della trasformazione strategica delle scelte legislative europee nel senso sopra indicato, avendo adottato un'impostazione orientata verso una cultura della sicurezza informatica basata sulla regolazione partecipativa e giungendo ad assumere la funzione di un manifesto di prevenzione giuridica. Il linguaggio tecnico della resilienza è stato integrato con quello giuridico della responsabilità condivisa e la cybersecurity è stata riconosciuta come principio trasversale della stabilità economica europea, costituendo una responsabilità collettiva che contribuisce alla sopravvivenza e alla tenuta del mercato digitale.

In tale contesto, il sistema penalistico è chiamato a svolgere un ruolo pionieristico in un momento di trasformazione epocale, assumendo la sfida di coniugare rigore normativo, efficacia preventiva e incisività operativa.

Il *file rouge* che ha guidato l'individuazione dei caratteri "facilitatori" e "mobilitatori" menzionati in precedenza risiede in una ravvisata esigenza di pragmatismo e concretezza nella materia. Tali criteri appaiono imprescindibili per l'edificazione di un "diritto penale della sicurezza digitale" solido, in quanto fondato su principi chiari, coerenti e capaci di resistere alla repentinità dell'evoluzione tecnologica, ed efficace, nella misura in cui consente interventi puntuali, proporzionati e tempestivi per fronteggiare le minacce informatiche emergenti. Un quadro giuridico concepito in tal modo sembra idoneo a confrontarsi efficacemente con le complesse dimensioni geo-politiche, sociali ed economiche di un'epoca caratterizzata da crescente tecnocentricità.

## Riferimenti bibliografici

G. Alfano (2024), *Rischi informatici nel settore finanziario: strumenti di prevenzione e resilienza operativa digitale,* in "Rivista di Diritto Bancario", 2024, n. 4 suppl.

P. Angelini (2024), *La cybersicurezza del settore finanziario: ruolo delle autorità e valore della cooperazione*, in "La cooperazione pubblico-privato per la resilienza cyber del settore finanziario italiano - Le opportunità per gli operatori e il ruolo del CERTF", Banca d'Italia, 2024

F. Angioni (1983), *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, 1983

R. Aprati (2023), *L'attività di prevenzione e l'acquisizione della notizia di reato*, in G. Colaiacovo (a cura di), "Sicurezza, informazioni e giustizia penale", Pacini Giuridica, 2023

Associazione Italiana per la Sicurezza Informatica (2025), *Rapporto Clusit 2025: l'evoluzione della minaccia cibernetica*, Security Summit, Milano, 11-13 marzo 2025

S. Aterno (2023), *Profili penali della vita nel Metaverso*, in G. Cassano, G Scorza (a cura di), "Metaverso. Diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023

S. Aterno (2022), *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini Giuridica, 2022

I. Ayres, J. Braithwaite (1992), *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, 1992

G. Barbara (2022), *La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive*, in "Corporate Governance", 2022, n. 4

G. Bettiol (1959), *L'odierno problema del bene giuridico*, in "Rivista italiana di diritto e procedura penale", 1959, n. 1

J. Black (2001), *Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world*, in "Current Legal Problems", vol. 54, 2001, n. 1

A.J. Blažič, B.J. Blažič (2024), *Toward effective learning of cybersecurity: new curriculum agenda and learning methods*, in "Journal of Cybersecurity", vol. 10, 2024, n. 1

F. Bricola (1973), *Teoria generale del reato*, in "Novissimo digesto italiano", vol. XIV, 1973

B. Buckland, F. Schreier, T. Winkler (2015), *Democratic governance challenges of cyber security*, in "DCAF Horizon 2015 Working Paper Series", 2015, n. 1

D. Busch (2024), *The future of Equivalence in the EU Financial Sector*, in "European Business Organization Law Review", vol. 25, 2024, n. 1

R. Calo (2026), *Law and Technology A Methodical Approach*, Oxford University Press, 2026

A.A. Cardani, I. Girardi (2024), *Impresa bancaria ed esternalizzazione di servizi tecnologici*, in "Orizzonti del Diritto Commerciale", 2024, n. 2

S. Carrea (2017), *L'individuazione del forum commissi delicti in caso di illeciti cibernetici: alcune riflessioni a margine della sentenza Concurrence Sàrl*, in "Diritto del commercio internazionale", 2017, n. 3

E. Chiocchio (2022), *Una nuova centralità per la cyber security nel settore finanziario*, in bancaforte.it, 28 luglio 2022

G. Corasanti (2025), *Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica*, in "Il diritto dell'informazione e dell'informatica", 2025, n. 1

F. Corona (2023), *I reati informatici*, in M. Iasselli, G.B. Caria (a cura di), "Cybersecurity & Cyberwarfare, Diritto tecnologia e sicurezza", EPC Editore, 2023

F. Corona (2021), *Il cybercrime: soggetto, oggetto e condotta*, in Id. (a cura di), "Reati informatici e investigazioni digitali", Pacini Giuridica, 2021

L. Cuomo (2000), *La tutela dei beni informatici*, in L. Cuomo, G. Di Giandomenico (a cura di), "Profili giuridici dell'informatica", Edizioni Scientifiche Italiane, 2000

L. Cuomo, B. Izzi (2002), *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in "Cassazione penale", 2002, n. 3

L. Cuomo, R. Razzante (2009), *La nuova disciplina dei reati informatici*, Giappichelli, 2009

M. Di Cuia (2025), *Cyber attacco, produzione bloccata: l'INPS può concedere la CIGO?*, in "Altalex", 19 marzo 2025

M. Donini (2013), *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in "Diritto penale contemporaneo", 2013, n. 4

M. Donini (2003), *Alla ricerca di un disegno. Scritti sulle riforme penali in Italia*, Cedam, 2003

M. Donini (1999), *Teoria del reato*, in "Digesto discipline penalistiche", vol. XIV, Utet, 1999

D. Fadda (2025), *In cassa integrazione per colpa del ransomware: sempre più casi in Italia*, in cybersecurity360.it, 20 febbraio 2025

N.M.F. Faraone (2024), *IA e vigilanza prudenziale: alla ricerca di un nuovo equilibrio tra presidio dei rischi e trasformazione digitale dell'impresa bancaria*, in "Rivista di Diritto Bancario", 2024, n. 4

G. Fiandaca (1982), *Il bene giuridico come problema teorico e come criterio di politica criminale*, in "Rivista italiana di diritto e procedura penale", 1982, n. 1

A. Fiorella (1987), *Reato in generale*, in "Enciclopedia del diritto", vol. XXXVIII, Giuffrè, 1987

G. Fiorinelli (2024), *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024

R. Flor (2023), *Lawful hacking, vulnerabilità tecnologica e diritto penale, fra esigenze di accertamento dei reati e tutela di beni giuridici di nuova generazione*, in L. Picotti (a cura di), "Automazione, diritto e responsabilità", Edizioni Scientifiche Italiane, 2023

R. Flor (2022), *Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale*, in R. Flor, S. Marcolini (a cura di), "Dalla data retention alle indagini ad alto contenuto tecnologico", Giappichelli, 2022

R. Flor (2019-a), *Cybersecurity e il contrasto ai cyberattacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in "Diritto di internet", 2019, n. 3

R. Flor (2019-b), *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime. Diritto e procedura penale dell'informatica", Utet Giuridica, 2019

D. Fracchiolla (2022), *La cyber-diplomacy, la nuova frontiera delle relazioni internazionali*, in "Digital Politics", vol. 2, 2022, n. 3

Garante per la protezione dei dati personali (2020), *Tecnologia e diritto devono allearsi per una corretta governance digitale. Intervista ad Antonello Soro*, in garanteprivacy.it, 2020

P. Ghignatti (2024), *DORA, inizia il conto alla rovescia per le aziende: i cinque pilastri per la compliance*, in cybersecurity360.it, 23 febbraio 2024

G. González Fuster, L. Jasmontaite (2020), *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. Christen, B. Gordijn, M. Loi (eds.), "The Ethics of Cybersecurity", Springer, 2020

L. Lessig (1999), *Code And Other Laws of Cyberspace*, Basic Books, 1999

A. Licastro (2025), *La configurazione dei mercati digitali a partire dal Digital Markets Act*, in "Rivista della Regolazione dei Mercati", 2025, n. 1

F. Lorè, P. Musacchio (2021), *Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva?*, in "Amministrativ@mente", 2021, n. 1

F. Mantovani (1977), *Il principio di offensività del reato nella Costituzione*, in "Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati", Giuffrè, 1977

G.L. Marcialis (2023), *La sicurezza informatica di frontiera: il modello "secure by design" nei sistemi biometrici*, in G. Colaiacovo (a cura di), "Sicurezza, informazioni e giustizia penale", Pacini Giuridica, 2023

L. Martino (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica&Società," 2018, n. 3

A. Mattarella (2022), *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in "Diritto penale e processo", 2022, n. 6

L. Menelly (1985), *Prosecuting Computer-Related Crime in the United States, Canada and England: New Laws for Old Offenses?*, in "Boston College International & Comparative Law Review", vol. 8, 1985

N. Michieli (2024), *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in "Banca Impresa Società", 2024, n. 2

G.P. Miller (2014), *Compliance function: an overview*, New York University School of Law, Law & Economics Research Paper Series, Working Paper n. 14-36, November 2014

V. Mongillo (2022), *Presente e futuro della compliance penale*, in sistemapenale.it, 2022

G. Morgante (2025), *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del law enforcement*, in "Rivista italiana di informatica e diritto", 2025, n. 2

G.N. Neppi Modona (1965), *Il reato impossibile*, Giuffrè, 1965

D. Padovan (2023), *La sicurezza informatica*, in M. Iasselli, G.B. Caria (a cura di), "Cybersecurity & Cyberwarfare. Diritto, tecnologia e sicurezza", EPC Editore, 2023

A. Pagliaro (1965), *Bene giuridico e interpretazione della legge penale*, in "Studi in onore di Francesco Antolisei", vol. II, Milano, 1965

V. Papakonstantinou (2022), *Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?*, in "Computer Law & Security Review", vol. 44, 2022

D.B. Parker (1974), *Computer-related crime*, in "Journal of Forensic Sciences", vol. 19, 1974, n. 2

C. Pecorella (2006), *Diritto penale dell'informatica*, Cedam, 2006

E.F. Pérez Carrillo (2023), *Cybersecurity in European Financial Institutions: new grounds for corporate governance reform*, in "European Business Law Review", vol. 34, 2023, n. 7

L. Picotti (2011), *Sicurezza informatica e diritto penale*, in M. Donini, M. Pavarini (a cura di), "Sicurezza e diritto penale", Bononia University Press, 2011

L. Picotti (2000), *Reati informatici*, in "Enciclopedia giuridica Treccani", vol. aggiorn. VIII, 2000

S. Pietropaoli (2019), *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in "Rivista di filosofia del diritto", 2019, n. 2

M. Pignatti (2024), *La resilienza operativa digitale per il settore finanziario tra vincoli contrattuali e responsabilità*, in "Diritto ed economia dell'impresa", 2024, n. 4

G.D. Pisapia (1948), *Introduzione alla parte speciale del diritto penale*, Giuffrè, 1948

D. Piva (2022), *Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up*, in "Corporate Governance", 2022, n. 4

A. Portolano, J. Mazza (2023), *Regolamento DORA: novità in arrivo per i contratti di fornitura dei servizi ICT,* in "Agenda Digitale", 28 giugno 2023

D. Pulitanò (1981), *La teoria del bene giuridico fra codice e Costituzione*, in "La Questione criminale", 1981, n. 1

F. Raffaele (2024), *Appunti sul c.d. Cybersecurity Risk Management tra disclosure statunitense e approccio regolatorio europeo*, in "Il Nuovo Diritto delle Società", 2024

I. Ramadhan (2021), *The Implication of Cyberspace Towards State Geopolitics*, in "Politicon: Jurnal Ilmu Politik", vol. 3, 2021, n. 2

R. Razzante (2023), *L'attribuzione degli attacchi informatici e il cyberterrorismo*, in Id. (a cura di), "Manuale di cybersicurezza", Pacini Giuridica, 2023

R. Razzante (2022), *Cybersecurity e 231: il raccordo tra norme ed eventi*, in "La responsabilità amministrativa delle società e degli enti", 2022, n. 1

A. Rocco (1913), *L'oggetto del reato e la tutela giuridica penale*, Fratelli Bocca, 1913

T.E. Romolotti (2019), *Cybersecurity: un ponte tra GDPR e d.lgs. 231/2001 alla luce del d.lgs. 101/2018*, in "Responsabilità amministrativa delle società e degli enti", 2019, n. 2

G. Schneider (2022), *La resilienza operativa digitale come materia di corporate governance: prime riflessioni a partire dal DORA*, in "Corporate Governance", 2022, n. 4

R. Sharma (2022), *Cyber Security to Safeguard Cyber Attacks*, in "International Journal of Information Security and Cybercrime (IJISC)", vol. 11, 2022, n. 2

F. Stella (1973), *La teoria del bene giuridico e i c.d. fatti inoffensivi conformi tipo*, Giuffrè, 1973

A. Stile (1985), *Bene giuridico e riforma della parte speciale*, Jovene, 1985

W.G. Urgessa (2020), *Multilateral cybersecurity governance: Divergent conceptualizations and its origin*, in "Computer Law & Security Review", vol. 36, 2020

R.M. Vadalà (2025), *La fattispecie penale tra economia digitale e diritto europeo*, Giappichelli, 2025

G. Vassalli (1982), *Considerazioni sul principio di offensività*, in "Studi in onore di Pietro Pioletti", Giuffrè, 1982