PROGETTO DI RICERCA
di Federica Delaini

PROGETTO DI RICERCA
DOMANDA DI DOTTORATO DI RICERCA IN SCIENZE GIURIDICHE EUROPEE ED INTERNAZIONALI XXXIX CICLO
UNIVERSITÀ DEGLI STUDI DI VERONA
ANNO ACCADEMICO 2023/2024

A. ***Titolo***: ***Cybersecurity, resilienza operativa digitale per il settore finanziario e tutela dei diritti, in prospettiva eurounitaria, interna e comparata***

B. ***Introduzione***

L'analisi proposta dal presente progetto di ricerca intende muovere le prime mosse da alcune fondamentali riflessioni: la *cybersecurity* rappresenta uno strumento di rilevanza strategica per garantire la continuità dei processi digitali e le politiche di innovazione tecnologica non possono prescindere da un quadro normativo idoneo a salvaguarne l'effettiva operatività e sicurezza, oltre che a favorirne la resilienza. Siffatte circostanze rivestono un ruolo vieppiù cruciale nell'ambito di settori fisiologicamente deputati a raccogliere, processare e trattare dati sensibili[1].

Come ineludibile corollario, le organizzazioni del settore finanziario, bancario ed assicurativo, nel presente momento storico, sono chiamate non soltanto alla *compliance* rispetto agli interventi normativi apportati dal legislatore nazionale ed europeo, bensì, anche ad una continua propensione al miglioramento, mediante l'implementazione di meccanismi connotati da rigore tecnico, volti a diffondere una comune cultura della sicurezza informatica[2].

[1] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.
[2] Valentini A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in www.cybersecurity360.it, del 06 aprile 2023.

C. <u>Sommario</u>: schema propositivo del lavoro di ricerca

- **Innovazione tecnologica ed innovazione giuridica**

  - *Lo stretto legame tra la trasformazione digitale (c.d. digitalizzazione) e la tutela dei diritti degli utenti e dei prestatori di servizi*

- ***Cybercrime* e *cybersecurity* nel mondo *Fintech:* le minacce che ledono i processi ed i sistemi informatici**

  - *Una nuova centralità per la cybersecurity nello scenario finanziario*

- **La risposta dell'Unione europea alle minacce informatiche: la nuova *roadmap* di istituti bancari e finanziari per fronteggiare i *cyber-attacks***

  - *La strategia europea in materia di sicurezza informatica: cybersolidarietà e lo scudo informatico europeo*
  - *La Direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva NIS – Network and Information Security)*
  - *Regolamento (UE) 2019/881 del 07 luglio 2029 (c.d. Cybersecurity Act)*
  - *Un excursus nella legislazione europea più recente in materia Fintech:*
    - *Regolamento (UE) 2021/694 del 29 aprile 2021*
    - *Regolamento (UE) 2021/887 del 20 maggio 2021*
    - *Raccomandazione (UE) 2021/1086 del 23 giugno 2021*
    - *Raccomandazione (CERS/2021/17) 2022/C 134/01 del 02 dicembre 2021*
    - *Parere della Banca Centrale Europea dell'11 aprile 2022 del 11 aprile 2022*
    - *Regolamento (UE) 2022/858 del 30 maggio 2022*
  - *La Direttiva (UE), n. 2022/2555 del 14 dicembre 2022 (c.d. Direttiva NIS 2)*
  - *Il Regolamento UE n. 2022/2554 del 14 dicembre 2022, (Digital Operational Resilience Act - c.d. Regolamento Dora)*
  - *Il Regolamento (UE) 2023/1113 del 31 maggio 2023riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività ed il Regolamento (UE) 2023/1114 del 31 maggio 2023 relativo ai mercati delle cripto-attività*
  - *Il sistema europeo di vigilanza finanziaria: le European Supervisory Authorities*
  - *L'Agenzia dell'Unione europea per la cibersicurezza (ENISA)*
  - *Verso un scudo informatico europeo: il EU Cyber Solidarity Act e gli impatti operativi della difesa comune*
  - *I risvolti pratici dei nuovi obblighi di cybersecurity per il mondo Fintech*

- **La strategia italiana in materia di *cybersecurity***

  - *Il quadro normativo passato, attuale e di prossima applicazione*
  - *La carenza di investimenti in materia di cybersicurezza ed il ruolo delle piccole e medie imprese*
  - *Il decreto-legge 17 marzo 2023, n. 25, coordinato con la legge di conversione 10 maggio 2023, n. 52, recante: «Disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech».*
  - *Sviluppi pratici e analisi statistica dei dati raccolti*

- **Uno sguardo comparatistico alle esperienze giuridiche europee**

  - *Il cammino della legislazione europea in materia di cybersecurity nel settore Fintech alla luce dei dati statistici e delle esperienze applicative europee*

- **Considerazioni finali**

  - *Compliance normativa e prontezza operativa*
  - *Le buone pratiche e le scelte organizzative degli operatori del settore per realizzare la conformità alla normativa*
  - *Risultanze degli obblighi di rendicontazione continua gravanti sugli attori del mondo Fintech*
  - *L'estensione dei poteri di controllo delle Autorità di vigilanza in materia finanziaria*
  - *L'adozione di misure tecnico-organizzative adeguate a mitigare i rischi di cyber-attacks*
  - *Tra obblighi e opportunità: verso una comune cultura della sicurezza informatica*

D. <u>Descrizione del progetto</u>: oggetto e struttura della ricerca

Lo studio intenderà offrire un ritratto della scelta del legislatore europeo di introdurre, con pubblicazione in Gazzetta Ufficiale dell'Unione europea datata 27 dicembre 2022, una serie di provvedimenti, ad aggiornamento ed integrazione del quadro normativo già implementato, in materia di *cybersecurity*, il cui obiettivo principe risiede nella creazione di un quadro giuridico unitario, caratterizzato dalla previsione di misure idonee ad assicurare e, contestualmente, a salvaguardare la resilienza dei sistemi informatici, all'interno di ambiti ove quest'ultima rappresenta un mezzo precauzionale indefettibile ed in cui gli interessi dei soggetti coinvolti appaiono di estrema sensibilità[3].

In particolare, trattasi del Regolamento UE n. 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022, c.d. *Regolamento Dora* (*Digital Operational Resilience Act*), relativo alla resilienza operativa digitale per il settore finanziario, e della Direttiva UE n. 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, c.d. *Direttiva Nis 2 (Network and Information Security 2)* relativa a misure per un livello comune elevato di *cybersicurezza* nell'Unione.

Nello specifico, scopo precipuo del *Regolamento Dora* deve essere individuato nello strenuo rafforzamento delle previgenti misure, mediante un'opera di armonizzazione dei principali requisiti ed adempimenti cui sono tenuti gli operatori nel settore finanziario, bancario ed assicurativo, oltre che i fornitori di criptoattività e di servizi strumentali[4].

Trattasi di obblighi di gestione dei rischi delle tecnologie, dell'informazione e della comunicazione (TIC), oltre che di segnalazione alle autorità competenti delle minacce informatiche, degli incidenti operativi, ovvero relativi alla sicurezza dei pagamenti, alla condivisione di dati sulla vulnerabilità, agli accordi contrattuali tra fornitori terzi di servizi TIC ed entità finanziarie ed all'avvio di un *framework* di sorveglianza per i fornitori terzi di servizi TIC[5].

Per altro verso, la *Direttiva Nis 2* è intervenuta al fine di modificare le previgenti regolamentazioni europee che, a vario titolo, avevano stabilito i requisiti connessi alla gestione dei rischi informatici nel settore finanziario, mediante l'apporto di una serie di modifiche necessarie per rendere chiara e coerente l'applicazione, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza, di adempimenti in materia di resilienza operativa digitale necessari per lo svolgimento delle attività e per la prestazione di servizi, garantendo, in tal modo, il corretto funzionamento del mercato interno[6].

---

[3] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.
[4] Ibidem.
[5] *DORA: il testo del Regolamento (UE) 2022/2554 in GU UE*, in *www.dirittobancario.it,* del 02 gennaio 2023.
[6] Ibidem.

Peraltro, di estremo interesse appare come la *Direttiva NIS 2* consideri soggetti meritevoli di attenzione anche gli enti pubblici minori e le piccole e medie imprese, oltre a diversi soggetti operanti nei settori della trasformazione e della distribuzione alimentare, nel settore sanitario e farmaceutico e, finanche, coloro che forniscono servizi digitali – trattasi, a titolo esemplificativo delle piattaforme di *cloud computing*, *data centre*, *content delivery network provide* -.

Appare di tutta evidenza come la scelta di politica legislativa delle istituzioni europee, già operata in passato, di intervenire nella presente materia non soltanto mediante lo strumento della Direttiva, bensì, anche a mezzo del Regolamento, rinvenga la propria *ratio* nella costante e progressiva rilevanza che sta acquisendo la tematica della *trasformazione digitale*[7]: essa inerisce alla catena di approvvigionamento e rende estremamente attuale il tema della sicurezza dei soggetti che ricevono, oppure forniscono, servizi digitali[8].

Ma vi è più. Sarà doveroso considerare come, attesa la estrema delicatezza ed attualità della materia in questione, il legislatore europeo abbia reputato che i settori finanziario, bancario ed assicurativo, fossero idonei a giustificare un grado di tutela maggiore di cittadini e, più in generale, di tutti gli *stakeholers* e, dunque, di obbligatorietà della normativa europea.

In tal modo l'Unione mira a superare le disparità legislative esistenti tra i diversi Stati membri ed i diversi approcci normativi, per evitare il rischio di pregiudicare la tanto ricercata ed auspicata resilienza operativa digitale[9].

La dissertazione intenderà, quindi, analizzare l'influenza dispiegata dalla nuova regolamentazione europea sull'attività degli attori del mondo *Fintech*, per tale intendendosi il nuovo mondo digitale delle valute e dei servizi finanziari, che, per l'appunto, negli ultimi anni, ha subito un'evoluzione tale da rendere necessaria l'introduzione di una normativa comune, in grado di disciplinare i diversi livelli in cui il medesimo si dispiega[10].

---

[7] Boscariol De Roberto F., *IP, IT E DATA PROTECTION, Codice europeo delle comunicazioni elettroniche: cosa prevede il D.Lgs. 207/2021*, in *Il Quotidiano Giuridico,* Wolters Kluwer, del 11 gennaio 2022; Ciccia Romito C., *Cybersicurezza: pubblicata la strategia nazionale (2022-2026)*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 26 maggio 2022; Galli C., *IP, IT E DATA PROTECTION Blockchain, NFT e Metaverso tra innovazione tecnica e innovazione giuridica,* in *Il Quotidiano Giuridico*, Wolters Kluwer, del 11 luglio 2022; Di Filippo A., *PNRR e transizione digitale: al via il decennio digitale 2030*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 09 gennaio 2023; Clarizia P., *La digitalizzazione*, in *Giornale di diritto amministrativo*, n. 3, 1 maggio 2023, pagg. 302 ss.; Megale L., *Il Garante della privacy contro ChatGPT: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giornale di diritto amministrativo*, n. 3, 1 maggio 2023, pagg. 403 ss.

[8] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.

[9] Valentini A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in www.cybersecurity360.it, 06 aprile 2023.

[10] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.

Il ricorso a nuove tecnologie in ambito finanziario genera un ecosistema in costante mutamento, che vede la disintermediazione di entità finanziarie centrali, con conseguente aumento della sperimentazione di nuovi modelli di *business* basati sulla tecnologia di frontiera. Ciò richiede lo sviluppo costante di nuovi presidi di *cybersecurity*: tali fenomeni si inseriscono in un contesto internazionale molto fluido ad istanze di rimodulazione degli assetti valutari e finanziari globali[11].

La *cybersecurity* è stata definita "*un diritto dell'uomo nella società delle reti, in quanto sfera che chiama in causa i diritti inviolabili di espressione, movimento, partecipazione, relazione*"[12]. Difatti, qualsiasi valutazione sul tema non può prescindere dalla considerazione che, in un'economia ed in una società fondata sui dati, proteggere questi ultimi significa tutelare, contestualmente, i singoli e la collettività stessa. Nel contesto della società digitale, ogni oggetto può rappresentare il canale d'ingresso di potenziali attacchi informatici: di qui, l'incontrollata moltiplicazione delle fonti di rischio, con la conseguenza che investire sulla protezione dei dati, dei sistemi e delle infrastrutture dovrebbe costituire l'obiettivo prioritario delle politiche pubbliche, in quanto, da un siffatto investimento, dipende la tutela stessa della persona, oltre che la sicurezza nazionale[13].

Pertanto, mediante la presente dissertazione, si approntera uno sguardo al crescente sviluppo del *cybercrime*, che vede le istituzioni, europee e nazionali, strenuamente impegnate nella progettazione e nella attuazione di discipline volte a fronteggiare i rischi in esso insiti.

A tal proposito, sebbene nelle fonti europee e sovranazionali non sia possibile rinvenire una definizione unanimemente riconosciuta di *cybercrime*, ossia *computer related crime*[14], sul piano

[11] Giannetto B., *Innovazione tecnologica e cybersecurity nel sistema finanziario*, in www.bancaforte.it, del 06 maggio 2021.
[12] Cannata M., *Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro*, in www.garanteprivacy.it, del 16 aprile 2020.
[13] Ibidem.
[14] Briat M. - Sieber U. (eds.), *Computer Related Criminality: Analysis of Legal Policy* in the OECDArea, Parigi 1986. Cfr. le Raccomandazioni n. R (89) 9 - sui profili di diritto penale sostanziale concernenti la lotta alla criminalità informatica - e n. R 95) 13, relativa ai problemi di procedura penale legati alla tecnologia dell'informazione; Convenzione Cybercrime adottata a Budapest il 23 novembre 2001; la Dir. 95/46/CE sulla tutela dei dati personali, nonché le direttive successive adottate in questo settore; le direttive in materia di protezione dei diritti d'autore e, in particolare, la Dir. 2001/29/CE; la Dir. 2000/31/CE sul commercio elettronico, le deci- sioni quadro contro gli attacchi informatici (2005/222/GAI), contro lo sfruttamento sessuale di minori e la pedopornografia (2004/68/GAI), contro il terrorismo (2002/475/GAI, parzialmente riformata dalla decisione 2008/919/GAI); sul piano processuale vedi quelle sul mandato d'arresto europeo (2002/584/GAI) e sull'applicazione del principio del reciproco riconoscimento delle decisioni di confisca (2006/ 783/GAI), che includono la "*criminalità informatica*" nelle liste di reati per cui si prescinde, in conformità con il principio del mutuo riconoscimento, dal requisito della doppia incriminazione per l'esecuzione diretta dei provvedimenti emessi dall'autorità giudiziaria dello Stato richiedente. Vedi per tutti L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in Riv. trim. dir. pen. ec., 4, 2011, 827 ss.

empirico la criminalità informatica abbraccia una molteplicità di comportamenti lesivi di interessi penalmente rilevanti, riconducibili ai c.d. *reati informatici*, in senso stretto[15] ed in senso lato[16].

Si esaminerà come, a seguito dell'affermazione di Internet, si sia verificata una progressiva transinzione dalla dimensione privata, del computer, alla dimensione pubblica, di sistemi basati sull'interconnettività globale[17]. Il crimine cibernetico, le cui condotte ineriscono, perlopiù, a fatti di furto e manipolazione di dati sensibili, oltre che al sistema delle criptovalute ed al riciclaggio, si distingue dalla criminalità tradizionale per l'assenza di confini fisici e geografici: l'impossibilità di percepire *ictu oculi* l'attacco disorienta le vittime, rendendole più vulnerabili. Peraltro, il *cybercriminale* è agevolato dalla disponibilità diffusa di *malaware* sulla rete e dalla circostanza che la commissione di un reato di tal sorta non richiede il possesso di spiccate capacità tecniche[18].

La legislazione italiana in materia di *cybercrime* è assai giovane e l'esigenza di positivizzare alcuni fondamentali strumenti di tutela è stata avvertita negli anni 80', simultaneamente alla graduale migrazione sulle reti della maggior parte delle attività lavorative e sociali: lo sviluppo del commercio elettronico e delle comunicazioni attraverso il web, oltre all'evoluzione delle tecnologie informatiche, hanno offerto ampie possibilità per la crescita di piccole e medie imprese prestatrici di servizi, quali *l'e-commerce*, l'*e-government*, l'*home banking* ed il *trading online*, che hanno coadiuvato una rilevante opera di efficientamento della società[19].

Purtuttavia, specularmente all'intensificazione degli scambi economici ed alla creazione di nuove opportunità di profitto, ha preso piede un pericoloso affermarsi della *criminalità virtuale*, sia nelle forme della criminalità comune, sia in quella delle organizzazioni criminali, le quali hanno, al pari delle prime, sfruttato i vantaggi della globalizzazione, perseguendo nei mercati internazionali e nella rete la propria strategia di arricchimento illecito[20].

---

[15] Weismann M.F., *International Cybercrime: Recent Developments in the Law*, in R.D. Clifford (ed.), *Cybercrime*, III ed., Carolina Academic Press, 2011.

[16] Si pensi, nell'ordinamento italiano, all'accesso abusivo a sistemi informatici (art. 615-ter c.p.) ovvero alla frode informatica (art. 640-ter c.p.). Questa categoria di reati informatici si connota per un nuovo oggetto passivo su cui la condotta ricade (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure dal fatto che il computer ed i prodotti informatici in genere costituiscono lo strumento tipico di realizzazione del '*fatto*' criminoso. Così Picotti L., *La nozione di "criminalità informatica*", cit.

[17] A. Mattarella, *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022, pag. 810.

[18] Vedasi sul punto il *Report annuale dello IOCTA (Internet Organized Crime Threat Assesment)* predisposto ogni anno dall'European Cyber Center, inserito all'interno di Europol.

[19] Mattarella A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022, pag. 812.

[20] Ibidem.

Difatti, a tutt'oggi, "*la sicurezza della dimensione cibernetica è costantemente esposta a minacce sempre più "ibride", tali da configurare una sorta di cyber guerriglia permanente*"[21].

La prospettiva d'indagine proseguirà con l'analisi della *cybersecurity* nell'ordinamento giuridico italiano: sino al momento della entrata in vigore della normativa oggetto della presente disama, un ruolo di cruciale rilevanza nella materia è stato rivestito dal *Cyber Security Act,* approvato con il Regolamento UE n. 2019/881, il quale si proponeva di realizzare un quadro unitario per la certificazione della sicurezza informatica dei prodotti e dei servizi digitali, secondo un modello di *security by design*, mediante il rafforzamento dei poteri e delle competenze dell'Agenzia dell'Unione europea per la cibersicurezza, c.d. *ENISA*[22], la quale sostiene gli Stati membri, le istituzioni dell'UE e le altre parti interessate nella gestione degli attacchi informatici[23].

La detta normativa ha stabilito in capo agli operatori di determinati servizi essenziali[24], come le infrastrutture digitali, il trasporto, il settore bancario ed i responsabili del trattamento dei dati, misure tecniche ed organizzative di prevenzione[25] e, finanche, un'insieme di obblighi di comunicazione alle Autorità nazionali diattacchi informatici che incidono sulla continuità dei servizi, tra cui i *data breach*[26].

In linea con la normativa europea, l'ordinamento italiano ha adottato il *Decreto Cybersecurity*[27] ed il *Piano nazionale per la Protezione Cibernetica e la Sicurezza Informatica*[28], che hanno rinnovato il sistema di prevenzione dei reati informatici[29].

In aggiunta, il D. lgs. n. 105/2019 ha istituito il *Perimetro di sicurezza nazionale cibernetica* che impone incisivi obblighi informativi a carico di tutte le pubbliche amministrazioni, al pari di enti ed operatori pubblici e privati competenti in materia di sicurezza[30], al fine di elevare lo standard di protezione informatica ed ampliare i poteri speciali attribuiti al Governo in tale ambito[31].

---

[21] Cannata M., *Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro*, in www.garanteprivacy.it, del 16 aprile 2020.
[22] Flor R., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3/2019, pagg. 461 ss.
[23] *Cibersicurezza: la risposta dell'UE alle minacce informatiche*, in www.consilium.europa.eu.
[24] Il D.Lgs. n. 65/2018, attuativo della Direttiva NIS, specifica in un elenco gli operatori a cui si applica la normativa.
[25] V. art. 32 GDPR e art. 12, D.Lgs. n. 65/2018.
[26] Sul punto, il Regolamento pone a carico del titolare del trattamento un obbligo.
[27] D.P.C.M. 17 febbraio 2017.
[28] D.P.C.M. 31 marzo 2017.
[29] Mattarella A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022, pag. 820.
[30] L'ambito oggettivo di applicazione del D.L. n. 105/2019 è determinato dal primo D.P.C.M. 30 luglio 2020, n. 131, entrato in vigore il 5 novembre 2020, per il quale i soggetti inclusi nel Perimetro nazionale sono individuati con atto amministrativo.
[31] Sul tema dell'evoluzione della normativa sovranazionale e italiana in materia di *cybersecurity* vedasi Picotti L., *Cybersecurity: quind novi?*, in *Diritto di Internet*, 2020, pagg. 13 ss.

Infine, non si potrà tralasciare un'analisi critica della recentissima novità legislativa apportata dal decreto-legge 17 marzo 2023, n. 25, recante: *«Disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech».*

Premessi alcuni cenni circa il quadro normativo sopra descritto, occorrerrà indagare la problematica che, in tale ambito, appare più grave ed urgente, ossia la cronica insufficienza degli investimenti in tema di *cybersecurity*, ditalchè l'Italia si colloca all'ultimo posto tra i paesi avanzati. In ragione di ciò, in molti auspicavano l'implementazione di un corposo intervento legislativo sulle tematiche della sicurezza cibernetica, al fine di innalzare gli standard di tutela in modo confacente al grado di sviluppo tecnologico del nostro Paese, atteso il concretizzarsi del pericolo di perdita di competitività sul piano internazionale[32].

Non a caso, sovente il diritto è stato definito "*l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza*" [33], così auspicando che un'alleanza tra tecnologia e diritto, potesse rappresentare la chiave di volta di una risposta democratica e lungimirante alle nuove minacce del digitale. Sifatto risultato, tuttavia, necessiterebbe, alla base, l'affermarsi di un difficile equilibrio tra discipline deputate a governare il rapporto tra le libertà ed il lato oscuro della tecnica, ovvero quella di protezione dei dati e quella a tutela della sicurezza cibernetica[34].

Nel delineare il quadro annuale sullo stato della sicurezza in Italia, il Rapporto Clusit del 2017 ha evidenziato come la piccola-media impresa italiana costituisca, a causa della lentezza dei modelli comportamentali di riferimento, l'anello debole della catena di sicurezza. Inoltre, si è ravvisata una inaspettata carenza di *big players,* ovvero di enti (pubblici o privati) di grandi dimensioni che agiscano in modo sinergico. Una siffatta frammentazione di competenze, unitamente all'assenza di un sistema-paese forte, rischia di far disperdere le conoscenze sino ad ora acquisite; da qui deriverebbe un consistente svantaggio competitivo per il nostro Paese, oltre al rischio di prestare il fianco a meccanismi di *dipendenza tecnologica*[35].

In ogni caso, è doveroso precisare che le direttive ed i regolamenti europei in materia, finanche i più recenti pubblicati in data 31 maggio 2023 - *Regolamento (UE) 2023/1113 riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività e Regolamento*

[32] Mattarella A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022, pag. 821.
[33] Cannata M., *Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro*, in www.garanteprivacy.it, del 16 aprile 2020.
[34] Ibidem.
[35] Mattarella A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022, pag. 821.

(UE) 2023/1114 relativo ai mercati delle cripto-attività - non hanno trovato impreparate le organizzazioni bancarie, e ciò, può dirsi, in ragione delle normative preesistenti emesse dall'*European Banking Authority* e dalla Banca d'Italia con il gruppo specializzato "*Gruppo di coordinamento sulla sicurezza cibernetica*", oltre che dalle indicazioni del *Certfin*, iniziativa cooperativa pubblico-privata finalizzata ad innalzare le capacità di gestione del rischio informatico degli operatori finanziari e la *cyber resilience* del sistema finanziario italiano, attraverso il supporto operativo e strategico alle attività di prevenzione preparazione e risposta agli attacchi informatici e agli incidenti di sicurezza.

A fronte del sopra delineato sistema economico e giuridico, sarà possibile apprezzare come il fine ultimo della neo-introdotta regolamentazione europea sia quello non soltanto di armonizzare le regole per tutti gli Stati Membri, bensì, financhè, di unificare le medesime, al precipuo scopo di rendere pienamente resiliente il settore *Fintech* in materia di *cybersecurity*.

Di conseguenza, si volgerà lo sguardo a come banche ed entità finanziarie, in considerazione del delicato *core business* di cui trattano, siano le protagoniste dell'intervento regolatore, in quanto sovente oggetto di numerosi attacchi da parte di criminali digitali. Difatti, il ruolo dalle stesse rivestito, le obbliga, ineludibilmente, ad adottare un atteggiamento rispondente ad elevati standard comportamentali in materia di sicurezza informatica[36].

Infine, di cruciale importanza come una siffatta normativa richieda, ineludibilmente, una forte e radicata cooperazione nello scambio di informazioni e di supporto tra le Autorità europee di Vigilanza e ed *ENISA*, le quali sono, altresì, deputate a fornire consulenza tecnica specifica in un'ottica di piena e costante collaborazione con gli operatori finanziari nelle attività di prevenzione e gestione del rischio[37].

In conclusione, il lavoro di ricerca mirerà ad effettuare una disamina degli sviluppi pratici ed operativi che prenderanno vita a seguito della implementazione ed attuazione delle nuove disposizioni: esse impatteranno in maniera notevole sui sistemi di gestione interni ed esterni del sistema *Fintech,* circostanza cui segue che valore imprescindibile avrà la predisposizione di un sistema di *governance* teso, per un verso, ad individuare i sistemi e le procedure da predisporre e, per altro verso, a garantire la continuità delle misure prese.

---

[36] Valentini A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in www.cybersecurity360.it, 06 aprile 2023.

[37] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.

Ciò nonostante, non si potrà tralasciare come il nuovo quadro europeo aprirà, altresì, le porte ad interrogativi e corollari di estrema sensibilità, che gli operatori del diritto, tanto a livello politico, quanto a livello legislativo e scientifico, sono chiamati ad affrontare e risolvere, al precipuo fine di garantire e preservare il potenziale valore aggiunto insito nella neo-introdotta normativa.

In tale quadro prospettico, dovrà senz'altro domandarsi ove l'azione legislativa in esame abbia correttamente individuato le minacce e le anomalie che potrebbero ledere la sicurezza dei sistemi e dei processi informatici nell'ambito *Fintech*, mediante la predisposizione di misure specifiche tese a fronteggiare i rischi e le vulnerabilità riscontrate nel quadro attuale.

Da ultimo, l'analisi vorrà concentrarsi sulla cura delle politiche di *business continuity* e *disaster recovery,* attraverso procedure volte al monitoraggio ed all'aggiornamento delle misure implementate, con lo scopo di assicurare il recupero tempestivo dei dati in caso di incidente fisico o informatico[38].

Infine, non si potrà trascurare come il neo-introdotto sistema richieda una rendicontazione continua sulle misure attuate da parte degli attori del sistema *Fintech*, in grado di comprovarne l'efficacia; inoltre, esclusivamente per determinate tipologie di destinatari, considerate più a rischio, esso impone l'obbligo di *freak led penetration testing*[39].

Lo studio si allargherà poi alla comparizione giuridica a confronto con le soluzioni applicate all'interno dei principali ordinamenti degli Stati membri dell'Unione: dopo aver fornito alcune preliminari nozioni circa il modello di *cybersecurity* ivi affermatosi, una disamina particolareggiata sarà dedicata alle diverse modalità di implementazione della normativa europea all'interno dei quadri culturali e giuridici di riferimento.

[38] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022 e Ciccia Romito C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.
[39] Ciccia Romito C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022.

E. Obiettivi e rilevanza dei risultati ottenibili nel contesto dello stato dell'arte

Orbene, il presente progetto intende mettere in luce gli auspicati benefici ed i risultati pratici cui si ritiene approderà la normativa introdotta dal legislatore europeo in materia *Fintech,* avendo specifico riguardo al *Regolamento Dora* ed alla *Direttiva NIS 2* nell'intreccio europeo e nazionale dei singoli Stati membri.

L'elevato grado di regolamentazione e progettazione che storicamente ha caratterizzato il sopra citato settore, in materia di *cybersecurity* europea, si spiega in ragione del fatto che il *core business* dell'ambito finanziario e bancario rappresenta il *quid* tanto desiderato dalla criminalità informatica.

È d'obbligo considerare che il *Regolamento Dora* e la *Direttiva NIS 2*, sebbene siano entrati in vigore il 16 gennaio 2023, saranno vincolanti il primo a partire dal 17 gennaio 2025[40] e la seconda dal 18 ottobre 2024,[41] così concedendo agli operatori del settore un periodo necessario ed utile per la messa a norma dei sistemi.

Di conseguenza, atteso che la sua applicazione determinerà l'adozione di molteplici ed inedite misure di sicurezza e *practices* in capo ai soggetti destinatari, i quali saranno tenuti ad una rendicontazione continua e costante del livello di sicurezza dei processi informatici adottati, si ritiene che rivesta estremo interesse, oltre che rilevanza strategica, l'opera di osservazione, monitoraggio e, eventualmente, di supporto che, mediante la presente dissertazione si intende proporre, allo scopo di coadiuvare la preparazione degli attori del mondo *Fintech* all'implementazione della neo-introdotta normativa ed alla sua reale ed effettiva attuazione.

A tal proposito, in molti si sono chiesti se la *compliance* normativa sia in grado di assicurare la prontezza operativa, oppure se essa richieda misure aggiuntive[42].

Primariamente, si è osservato come la predisposizione di meccanismi in piena conformità alla nuova regolamentazione costituisca, fuor di ogni dubbio, una leva volta ad incrementare la capacità delle aziende di proteggere i propri sistemi.

Tuttavia, la nuova regolamentazione potrebbe rappresentare, finanche, una seria opportunità per tutti gli operatori del settore, laddove gli stessi si rivelino in grado di sfruttare adeguatamente le potenzialità insite negli obblighi implementati, mediante la dotazione di strumenti organizzativi e tecnologici idonei a gestire le evoluzioni future degli scenari di rischio. Ciò consentirebbe non soltanto di raggiungere la conformità normativa, bensì, anche di dare vita ad un sistema capace di

---

[40] Meneghetti M. C., *In vigore il Regolamento DORA: nuovi obblighi di cybersecurity per banche, assicurazioni e finanziarie*, in www.dirittoaldigitale.com, del 27 dicembre 2022.
[41] Mauri T., *NIS2 e regolamento DORA: cosa devono fare le aziende per allinearsi alle nuove norme UE*, in www.cybersecurity360.it, 02 marzo 2023.
[42] Valentini A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in www.cybersecurity360.it, 06 aprile 2023.

individuare, presidiare e mitigare le nuove minacce[43], essenzialmente connaturate all'evoluzione della trasformazione tecnologica.

Peraltro, il *Regolamento Dora* e la *Direttiva NIS 2* offrono alle istituzioni finanziarie la possibilità di creare una cultura della sicurezza informatica in grado di coinvolgere tutti gli *stakeholders*, dai vertici aziendali sino ai clienti finali.

Sul punto, è apprezzabile come in molti abbiano individuato nella diffusione di una siffatta cultura e negli interventi da attuare a livello organizzativo i principali obbiettivi della nuova regolamentazione, cosicchè l'introduzione di mere misure tecniche sarebbe, invece, da considerarsi un insufficiente.

Pertanto, si prevede che il primo anno di implementazione della neo-introdotta disciplina sarà, perlopiù, finalizzato ad elaborare risposte concrete e confacenti alle istanze di chiarimenti avanzate dai soggetti *Fintech*, e, quindi, al perfezionamento del nuovo sistema.

Viceversa, il successivo anno 2024 sarà dedicato all'adeguamento delle strutture predisposte, così da assicurare la piena operatività delle medesime al momento della vincolatività delle disposizioni[44].

Ma vi è di più. A far data dal 17 gennaio 2025, le Autorità di vigilanza saranno munite di poteri maggiormente stringenti e penetranti in materia di sorveglianza, non soltanto sulle istituzioni finanziarie, ma anche sui fornitori di servizi ICT, in una logica più estesa di gestione del rischio delle terze parti[45].

Conseguentemente, apparirà di estremo interesse indagare gli esiti cui giungerà detta opera di monitoraggio, al fine di verificarne gli sviluppi pratici, a titolo esemplificativo in relazione ai criteri individuati dall'art. 31 del Regolamento Dora, quali l'impatto sistemico sulla stabilità, la continuità ovvero la qualità della fornitura di servizi finanziari, oppure l'importanza delle entità finanziarie che dipendono dal fornitore terzo di servizi ICT[46].

L'intervento riformatore si prefigge, tra i propri obbiettivi, altresì, l'identificazione e l'assegnazione di ruoli e responsabilità in capo agli operatori del settore, avendo specifico riguardo a

[43] Valentini A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in www.cybersecurity360.it, 06 aprile 2023.
[44] Ibidem.
[45] Chiocchio E., *Una nuova centralità per la cyber security nel settore finanziario*, in www.bancaforte.it del 28 luglio 2022.
[46] *Regolamento DORA: quali novità ci attendono?*, in www.roedl.it del 31.01.2023.

quattro ambiti: l'identificazione dei rischi, la predisposizione di misure di protezione e prevenzione, il rilevamento, la risposta ed il recupero in caso di incidenti e la formazione e la comunicazione[47].

Ditalchè, alle entità finanziarie sarà richiesto di definire e mantenere sistemi e processi ICT che riducono al minimo l'impatto delle minacce: i processi di identificazione e aggiornamento continuo introdotti saranno in grado di assolvere in modo puntuale e specifico alla funzione ad essi affidata?

L'attuazione ed il monitoraggio delle misure di sicurezza consentiranno il rilevamento delle anomalie in materia di *business continuity* e *disaster recovery*?

La nuova legislazione europea sarà capace di costituire, come tanto auspicato, un presidio stabile per la sicurezza e la resilienza operativa digitale nell'agenda del settore finanziario?

L'utilizzo delle tecnologie ICT è ormai pervasivo nell'erogazione dei servizi finanziari: la crescente digitalizzazione e le sempre più fitte interconnessioni, oltre a rappresentare un elemento abilitante per il *business*, amplificano i rischi, a tutt'oggi non sempre pienamente inclusi nel perimetro delle funzioni di controllo.

L'auspicio è, dunque, che gli attori di *Fintech*, superando il mero adeguamento alla norma, rivolgano la propria attenzione ai seguenti elementi: *commitment* nella gestione del rischio ICT con una maggiore responsabilità del *Board*; approccio multidisciplinare in considerazione della necessità di attingere a tipologie di competenze diverse (*cybersecurity, risk management, legal advisory, IT*); costruzione di un efficace programma di adeguamento che si integri sinergicamente, partendo da un'attività di *gap analysis*, nei *framework*, processi e progetti in essere[48].

L'opera legislativa perpetrata dalle Istituzioni europee sarà in grado di calarsi in modo efficae nell'organizzazione delle strutture finanziarie ed incrementarne realmente la resilienza operativa dei sistemi digitali?

Ogni riflessione sull'argomento non potrà trascurare che gli istituti bancari svolgono, da sempre, una funzione sociale che impatta non soltanto sulla macroeconomia, bensì, ancora prima, sulla microeconomia, la quale coinvolge quotidianamente ogni singolo risparmiatore. In ragione di ciò, tale profilo merita vieppiù di essere preso in considerazione nell'ambito dell'attuazione di riforme idonee a fronteggiare e, allo stesso tempo, a tutelare la grande trasformazione digitale che sta interessando l'ambito finanziario[49].

---

[47] *Regolamento DORA: quali novità ci attendono?*, in www.roedl.it del 31.01.2023.
[48] *Digital Operational Resilience Act: da obbligo a opportunità*, in *www.bancaforte.it* del 16 giugno 2023.
[49] Chiocchio E., *Una nuova centralità per la cyber security nel settore finanziario*, in *www.bancaforte.it* del 28 luglio 2022.

Alla luce del quadro sopra prospettato, appare ragionevole ritenere che i risultati cui il presente progetto di ricerca perverrà si incentreranno, primariamente, sullo studio e sull'analisi critica delle delle peculiarità, potenzialità e problematicità della neo-introdotta regolamentazione, avendo specifico riguardo all'interazione della medesima con i diritti degli utenti e, in generale, degli *stakeholders*.

La forza di penetrazione del diritto europeo in questo segmento dell'ordinamento è tutta da sperimentare e sarà interessante monitorare la forza modellante dallo stesso dispiegata sugli statuti dei settori abbracciati dall'intervento di riforma.

L'importanza dei quesiti sopra accennati – che costituiranno l'asse portante del'indagine - risiede nella circostanza che soltanto una corretta e ben combinata sinergia tra l'efficace coordinamento delle Autorità di vigilanza, europee e nazionali, unitamente alla predisposizione di meccanismi idonei a garantire il recepimento, effettivo e completo, degli standard comportamentali imposti in ambito europeo ed una profonda promozione di una cultura comune di sicurezza informatica, potrà aprire a nuove e promettenti frontiere per la neonata regolamentazione.

Mediante l'intervento legislativo oggetto del presente vaglio, l'Europa ha aggiunto un ulteriore e fondamentale tassello alla già intrapresa opera di protezione dei dati, rendendola un fattore identitario.

Peraltro, appare di estremo interesse come, in un momento storico in cui riaffiorano spinte divisive, il legislatore europeo abbia coltivato l'aspirazione federale, in un settore che concilia ambiti di cruciale rilevanza, quali tecnologia e diritti, economia e libertà.

Una siffatta vocazione unitaria, che, purtroppo, sovente latita in altri ambiti, ha permesso di superare i particolarismi che spesso privano il diritto del suo necessario "*sguardo lungo*", consentendo a questa disciplina di divenire il fronte più avanzato di una *governance del digitale*, a cui molte altre normative (anche extraeuropee) hanno attinto[50].

Tanto premesso, si ritiene che la nuova regolamentazione di matrice europea, sia in grado di attribuire la necessaria rilevanza ad idee e progetti capaci di governare la neo-affermatasi società digitale, al fine di garantire i diritti degli *stakeholders* e le libertà degli utenti, quali beni giuridici rispetto ai quali la protezione dati è da considerarsi come una bussola imprescindibile.

[50] Cannata M., *Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro*, in www.garanteprivacy.it, del 16 aprile 2020.

Si ritiene che nel corso degli anni 2024 e 2025 sarà senz'altro possibile apprezare gli sforzi pratici intrapresi dalle organizzazioni finanziarie, bancarie e assicurative, al fine di prepararsi all'attuazione delle nuove misure e, negli anni successivi, l'opera di monitoraggio, di analisi critica e di studio consentirà di pervenire, altresì, mediante il supporto e l'analisi di dati statistici frattanto raccolti, a valutazioni e considerazioni ponderate in riferimento alle questioni sopra prospettate.

Il nuovo assetto europeo in materia di *cybersecurity* e di resilienza operativa digitale nel sistema *Fintech* è atteso alla prova dei fatti e l'auspicio è che il presente lavoro possa fornire un concreto sostegno alla sua effettiva attuazione e funzionamento, mediante lo studio di soluzioni operative in grado di imprimere una nuova dinamica, foriera di nuovi sviluppi.

F. Arco temporale di sviluppo della ricerca

Delimitato l'oggetto dell'indagine, occorre dar conto delle coordinate metodologiche sulla base delle quali la ricerca potrà svilupparsi.

Nel corso dei primi quattro mesi si potrà procedere all'acquisizione delle opere dottrinali, nazionali e straniere, rilevanti in materia, oltre a quelle già conosciute.

La ricerca richiederà lo svolgimento di un periodo di studi presso centri di ricerca europei e la raccolta di dati presso organizzazioni finanziarie e bancarie.

Sulla base dei contributi e delle risultanze acquisite, nei successivi due mesi si provvederà alla sistematizzazione dei risultati degli approfondimenti compiuti.

Infine, gli ultimi sei mesi potranno essere dedicati alla stesura del prodotto della ricerca, che nella sua conformazione finale si tradurrà in uno o più contributi scientifici da pubblicare su riviste specialistiche nazionali e/o straniere.

G. Bibliografia

BOSCARIOL DE ROBERTO F., *IP, IT E DATA PROTECTION, Codice europeo delle comunicazioni elettroniche: cosa prevede il D.Lgs. 207/2021*, in *Il Quotidiano Giuridico,* Wolters Kluwer, del 11 gennaio 2022.

BRIAT M. - SIEBER U. (eds.), *Computer Related Criminality: Analysis of Legal Policy* in the OECDArea, Parigi 1986.

CANNATA M., *Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro*, in www.garanteprivacy.it, del 16 aprile 2020.

CHIOCCHIO E., *Una nuova centralità per la cyber security nel settore finanziario*, in *www.bancaforte.it* del 28 luglio 2022.

Cibersicurezza: la risposta dell'UE alle minacce informatiche, in www.consilium.europa.eu.

CICCIA ROMITO C., *Cybersecurity: pubblicati in GUUE la Direttiva NIS 2 e il Regolamento Dora*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 10 gennaio 2023.

CICCIA ROMITO C., *Cybersicurezza: pubblicata la strategia nazionale (2022-2026)*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 26 maggio 2022.

CICCIA ROMITO C., *Regolamento Dora: obbligo di Cybersecurity per il mondo fintech*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 29 novembre 2022.

CLARIZIA P., *La digitalizzazione*, in *Giornale di diritto amministrativo*, n. 3, 1 maggio 2023, pagg. 302 ss.

DI FILIPPO A., *PNRR e transizione digitale: al via il decennio digitale 2030*, in *Il Quotidiano Giuridico*, Wolters Kluwer, del 09 gennaio 2023.

Digital Operational Resilience Act: da obbligo a opportunità, in *www.bancaforte.it* del 16 giugno 2023.

DORA: il testo del Regolamento (UE) 2022/2554 in GU UE, in *www.dirittobancario.it,* del 02 gennaio 2023.

FLOR R., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3/2019, pagg. 461 ss.

GALLI C., *IP, IT E DATA PROTECTION Blockchain, NFT e Metaverso tra innovazione tecnica e innovazione giuridica,* in *Il Quotidiano Giuridico*, Wolters Kluwer, del 11 luglio 2022.

GIANNETTO B., *Innovazione tecnologica e cybersecurity nel sistema finanziario*, in *www.bancaforte.it*, del 06 maggio 2021.

MATTARELLA A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Diritto penale e processo*, n. 6/2022 pagg. 810 ss.

MAURI T., *NIS2 e regolamento DORA: cosa devono fare le aziende per allinearsi alle nuove norme UE*, in *www.cybersecurity360.it*, 02 marzo 2023.

MEGALE L., *Il Garante della privacy contro ChatGPT: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giornale di diritto amministrativo*, n. 3, 1 maggio 2023, pagg. 403 ss.

MENEGHETTI M. C., *In vigore il Regolamento DORA: nuovi obblighi di cybersecurity per banche, assicurazioni e finanziarie*, in *www.dirittoaldigitale.com,* del 27 dicembre 2022.

PICOTTI L., *Cybersecurity: quind novi?*, in *Diritto di Internet*, 2020, pagg. 13 ss.

PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale diritto penale* ec., 4, 2011, pagg. 827 ss.

Regolamento DORA: quali novità ci attendono?, in www.roedl.it del 31.01.2023.

Report annuale dello IOCTA (Internet Organized Crime Threat Assesment) predisposto ogni anno dall'European Cyber Center, inserito all'interno di Europol.

VALENTINI A., *Cyber security, la nuova roadmap di banche e istituti finanziari*, in *www.cybersecurity360.it*, del 06 aprile 2023.

WEISMANN M.F., *International Cybercrime: Recent Developments in the Law*, in R.D. Clifford (ed.), *Cybercrime*, III ed., Carolina Academic Press, 2011.