La *cyber security* nel settore bancario

di Simona Giannetti
Dottore di Ricerca in Diritto delle Persone, delle Imprese e dei Mercati
Dipartimento di Giurisprudenza
Università degli Studi di Napoli "Federico II"

ABSTRACT

The European Union considered the need for provisions on cyber risk and cyber security – meaning, network data and information security – to be enacted long ago.

Among the many, the last and most important EU piece of legislation in the area is the Network and Information Security Directive, no. 1148/2016 (known by the acronym NIS), which provides for a number of measures designed to establish a high and common level of security for networks and information systems. The provisions of the directive relate to operators of essential services and digital service providers, as listed in Annex II, and namely those operating in the transports, energy, banking, health, and drinking water sectors, as well as in the area of digital infrastructures and financial markets.

The paper investigates the application of the NIS Directive to the banking-financial sector, starting with an overview on the evolution of the system and, then analyzing the NIS Directive together with the implementing regulation no. 151 of 2018 and the national legislative decree implementing it, pointing out – also thanks to the advice contained in the CLUSIT 2019 Report – the critical issues to which the networks and the information systems are under.

SINTESI

L'Unione europea, già da tempo, ha sentito l'esigenza di legiferare in materia di cyber risk e cyber security, ovvero della sicurezza dei dati e delle informazioni della rete. Tra i numerosi atti che l'Unione europea ha adottato l'ultima, e forse più importante, Direttiva in materia è la Network and Information Security n. 1148/2016 (conosciuta con l'acronimo NIS), che contiene una serie di misure legislative atte a creare un comune ed elevato livello di sicurezza delle reti e dei sistemi informativi. Le disposizioni previste dalla Direttiva riguardano operatori e fornitori di servizi essenziali, che vengono elencati nell'Allegato II della Direttiva e sono quelli del settore dei trasporti, energetico, bancario, sanitario, dell'acqua potabile, nonché nell'ambito delle infrastrutture digitali e dei mercati finanziari.

Il presente lavoro, pertanto, intende soffermarsi sull'applicazione della Direttiva NIS al settore bancario-finanziario; partendo da una ricognizione sull'evoluzione del sistema si analizza la Direttiva NIS, unitamente al Regolamento attuativo n. 151 del 2018, e al Decreto legislativo nazionale di recepimento della Direttiva stessa, evidenziando le criticità cui le reti e i sistemi informativi sono sottoposti.

SOMMARIO: 1. Introduzione – 2. L'innovazione del settore bancario-finanziario: *FinTech* e *Bitcoin* – *2.1. (Segue) I rischi dell'innovazione nel settore bancario-finanziario* – 3. La Direttiva n.1148 del 2016: *Network and Information Security* (NIS) – *3.1. (Segue) Identificazione degli operatori dei servizi essenziali – 3.2. (Segue) Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, Autorità nazionali competenti, punto di contatto e rete CSIRT* – 4. Il Regolamento attuativo della Direttiva NIS, n.151/2018 – 5. Il Decreto legislativo n.65 del 2018 di attuazione della Direttiva NIS – 6. Il Rapporto CLUSIT 2019 – 7. Conclusioni

1. Introduzione

Da anni sono diventati familiari termini quali *cyber crime*, *cyber risk, hacker*, *risk management*, attacchi informatici, tutti termini strettamente collegati alla sicurezza informatica, tematica sovente sintetizzata nell'espressione *cyber security*.

Si tratta altresì di tema strettamente collegato al processo di **innovazione tecnologica**[1] che negli ultimi anni si è notevolmente sviluppata evolvendosi poi nella c.d. quarta rivoluzione industriale, conosciuta anche come *Industry 4.0*, termine utilizzato per la prima volta in Germania per descrivere l'**innovazione tecnologica** quale motore fondamentale della crescita e del progresso in tutti i settori, il cui grado di sviluppo varia in funzione del contesto organizzativo e istituzionale.

Nell'ultimo decennio abbiamo assistito ad un celere sviluppo dell'**innovazione tecnologica**,[2] con riferimento ai mutamenti[3] nell'attività delle imprese e delle istituzioni volta ad introdurre nuovi prodotti e servizi, nonché nuovi metodi per

[1] Per **innovazione tecnologica** si intende la combinazione tra "attività di invenzione" (cioè generazione di nuove idee) e "attività di sfruttamento commerciale" (cioè individuazione di opportunità per ottenere un guadagno dalla vendita dell'idea generata).

[2] Il termine **tecnologia/tecnologico** sta ad indicare l'insieme di conoscenza, tecnica ed organizzazione, mentre con quello di "innovazione" si individua il processo di avanzamento della conoscenza relativa all'integrazione stessa.

[3] Si v. *The Economist*, 1° Febbraio 1999: «… l'innovazione è diventata la religione industriale del XX secolo, le imprese la vedono come lo strumento chiave per aumentare i profitti e le quote di mercato, i governi si affidano ad essa quando cercano di migliorare l'economia. Nel mondo, la retorica dell'innovazione ha recentemente rimpiazzato quelle dell'economia del benessere, presente dal secondo dopoguerra. È la nuova tecnologia».

produrli e renderli disponibili agli utilizzatori (che di riflesso generano il successo dei produttori con la propria accettazione).

L'*Industry 4.0* coinvolge tutti i settori industriali ed è stata in grado di troncare qualsiasi legame con il passato obbligando le imprese a rivedere i propri modelli di *business*, di *mission* e di *vision* aziendale[4] in vista di una riorganizzazione ed un'inclusione al loro interno della c.d. componente digitale.

La trasformazione digitale interessa in particolar modo il settore bancario, poiché le imprese che vi operano si trovano di fronte alla necessità di modificare i propri assetti tradizionali e adottare forme organizzative idonee a reggere il peso competitivo del mercato e a mantenere alto il livello di soddisfazione di consumatori, sempre più esigenti perché, nell'attuale panorama industriale, quello bancario appare come il settore più arretrato rispetto al grado di innovazione tecnologica di altri ambiti.

Il processo in corso, non solo ha innovato il settore finanziario ed il modo di concepire le imprese bancarie, ma ha indotto i consumatori, o meglio ancora i risparmiatori/investitori, ad operare in un mondo sempre più digitale, modificando le abitudini e le modalità di soddisfacimento delle loro esigenze, grazie all'utilizzo di una rete *internet* e di un personal computer, di uno smartphone o di un tablet. In risposta all'evoluzione, sia in ordine al bacino di utenti sia alle possibilità di accesso, le imprese bancarie hanno dovuto ripensare il "modo di fare banca" e hanno ideato nuovi prodotti e servizi c.d. *real time*, che permettono ai clienti di poter investire i propri risparmi anche in maniera individuale, senza il supporto di un consulente. Ciò ha permesso di mantenere stabile il rapporto banche/clienti ed evitare che le stesse fossero sopraffatte dalla concorrenza, sviluppatasi notevolmente negli ultimi anni grazie alla creazione di nuove imprese bancarie e nuove società di intermediazione. Con l'innovazione dei prodotti è sorta altresì un'esigenza di semplificazione dei

[4] R. CAPPELLIN - M. BAVARELLI - M. BELLANDI - R. CAMAGNI - S. CAPASSO - E. CICIOTTI - E. MARELLI (a cura di), *Investimenti, innovazione e nuove strategie di impresa. Quale ruolo per la nuova politica industriale e regionale?*, Egea, Milano, 2017.

meccanismi negoziali, richiedendo dunque processi più semplici e posti in essere in modo automatico.

L'innovazione tecnologica, in qualsiasi settore venga applicata, ma soprattutto in quello bancario-finanziario, non ha solo lati positivi: il rovescio della medaglia riguarda, per quanto a noi interessa, il *cyber risk* cui è costantemente sottoposto il settore. Il moltiplicarsi degli attacchi informatici ha portato le istituzioni ad interessarsi al problema cercando di individuare soluzioni efficaci per evitare che eventuali violazioni delle infrastrutture erogatrici dei servizi c.d. essenziali potessero indurre conseguenze gravi. È questa per l'appunto la considerazione in base alla quale l'Unione europea ha inteso affrontare l'argomento adottando una serie di atti e direttive in merito al *cyber risk* e alla *cyber security.* La base giuridica, assunta a punto di partenza per l'adozione, a livello europeo, di direttive riguardo alle *Information and Communication Technologies* (ICT)[5] sono senza dubbio gli articoli 82 e 83 del TFUE dai quali emerge chiaramente come l'Unione sia autorizzata ad agire qualora si paventi un abuso collegato alle ICT e che sfoci in un crimine a carattere transnazionale.[6] Della normativa europea si parlerà nel prosieguo in sede di analisi dell'ultima Direttiva dell'Unione europea emanata in ambito di *cyber security*, ovvero la n.1148 del 2016, *Network and Information Security* (d'ora in poi Direttiva NIS), e il relativo Regolamento di esecuzione n.151 del 30 gennaio 2018 recante modalità di applicazione della Direttiva NIS. Verrà

[5] Le tecnologie dell'informazione e della comunicazione sono l'insieme delle tecnologie che consentono i sistemi di trasmissione, ricezione ed elaborazione delle informazioni.

[6] Si v. per un approfondimento A. ROTONDO, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo*, in S. MARCHISIO e U. MONTUORO (a cura di) *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, 2019, pp. 115-135. Negli artt. 82 e 83 TFUE si legge che "*laddove necessario per facilitare il riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e la cooperazione di polizia e giudiziaria nelle materie penali aventi dimensione transnazionale, il Parlamento europeo e il Consiglio possono stabilire norme minime deliberando mediante direttive secondo la procedura legislativa ordinaria*" e ancora che "*il Parlamento europeo e il Consiglio [...] possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale [... come la] criminalità informatica*". Direttiva 2011/92/UE del Parlamento europeo e del Consiglio relativa alla "Lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile", che sostituisce la Decisione quadro 2004/68/GAI del Consiglio del 13 dicembre 2011, G.U.U.E. L 335/1 del 17-12-2011.

altresì esaminata la normativa italiana emanata in recepimento della Direttiva NIS: il Decreto legislativo del 18 maggio 2018, n.65.

Prima però di spingerci nell'analisi della normativa europea e nazionale risulta necessario introdurre il tema partendo dall'illustrazione, seppur sommaria, dell'innovazione che il settore bancario e finanziario ha vissuto negli ultimi anni e che ha indotto gli istituti c.d. tradizionali ad addentrarsi in settori innovativi fornendo altri servizi ai clienti, quali ad esempio l'*internet banking* o le *cripto valute*, o addirittura reinventandosi in nuove forme di istituti quali le *FinTech*.

2. L'innovazione del settore bancario-finanziario: *FinTech* e *Bitcoin*

L'aumentato livello di concorrenza nel settore finanziario ha spinto le banche a digitalizzarsi, ideando prodotti e semplificando i servizi essenziali. Tradizionalmente quello finanziario è sempre stato un settore "protetto", a causa delle stringenti norme previste per l'autorizzazione. La nascita di nuovi istituti, anche non bancari, cui si è fatto cenno, che si sono inseriti in special modo nella tradizionale operatività bancaria, ha generato un incremento dei livelli di competitività nel settore finanziario. Questi nuovi soggetti hanno trovato terreno fertile soprattutto grazie alla stringente regolamentazione, seguita alla crisi, che ha limitato maggiormente la capacità competitiva delle banche "tradizionali".

La maggior parte degli operatori cui si fa riferimento sono rappresentati dalle imprese c.d. *FinTech*,[7] termine che «si riferisce alla *Financial Technology*, ossia l'offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica», che comporta forti spinte innovative nel mercato finanziario;[8] in altre parole, possiamo dire che le *FinTech* sono

[7] R. FERRARI, *L'era del Fintech. La rivoluzione digitale nei servizi finanziari*, Franco Angeli, Milano, 2016; M.T. PARACAMPO (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, G. Giappichelli Editore, Torino, 2017.

[8] Definizione fornita dalla Banca d'Italia nel "Canale FinTech", reperibile sul sito www.bancaditalia.it.. Si v. altresì, per un approfondimento al tema: BANCA D'ITALIA, *La trasformazione digitale nell'Ecosistema dei pagamenti al dettaglio. Conferenza BCE - Banca d'Italia, Roma 30 novembre - 1° dicembre 2017*, Altri Atti di Convegni, 30 novembre 2017; BANCA D'ITALIA, *Fintech: Ruolo dell'Autorità di Vigilanza in un mercato che cambia*, 8 febbraio 2019; BANCA D'ITALIA, *Fintech and the future of financial services*, 23 luglio 2018; BANCA D'ITALIA,

nient'altro che *start-up* innovative che offrono "servizi bancari" utilizzando tuttavia un maggiore livello tecnologico-innovativo che permette di contenere i costi dei servizi prestati. Ciò posto, sono proprio le caratteristiche, che possiamo definire dinamiche, a far sì che tali soggetti siano più competitivi rispetto ai tradizionali istituti bancari. Soprattutto nel settore dei prestiti, le *FinTech* sono molto più competitive delle banche tradizionali poiché si affidano a piattaforme di *lending crowdfunding* che, bypassando l'intermediazione degli istituti di credito, mettono in collegamento, attraverso *internet*, finanziatori ed investitori. La possibilità di proporre alternative all'intermediazione degli istituti di credito porta, da un lato, ad una sostanziale riduzione del tempo di attesa tra richiesta di finanziamento ed erogazione del prestito, dall'altro ad una riduzione dei costi dell'intermediazione creditizia, che appunto, viene superata con l'utilizzo di siffatte piattaforme.

Non solo le imprese *FinTech* stanno condizionando l'operatività delle banche, ma anche le c.d. "criptovalute". La più nota è sicuramente rappresentata dai *bitcoin*[9] che "si caratterizzano per essere una moneta digitale che consente di **acquistare beni sia virtuali sia reali**, con flussi di scambio bidirezionali con le monete convenzionali",[10] definizione dettata dalla Banca centrale europea che li

Fintech and banking: today and tomorrow, 12 maggio 2018; BANCA D'ITALIA, *Fintech e regole,* 10 maggio 2018; BANCA D'ITALIA, *FinTech in Italia. Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari*, 8 gennaio 2018; BANCA D'ITALIA, *I nostri istituti fuori gioco, se non si innovano. Amazon può diventare un big del credito*, 2 gennaio 2018; BANCA D'ITALIA, *Indagine conoscitiva sulle tematiche relative all'impatto della tecnologia finanziaria sul settore finanziario, creditizio e assicurativo.* Audizione di Fabio Panetta, Vice Direttore Generale della Banca d'Italia, 29 novembre 2017; BANCA D'ITALIA, *L'innovazione digitale nell'industria finanziaria italiana*. Intervento di Fabio Panetta, Vice Direttore Generale della Banca d'Italia, tenuto a Milano in occasione dell'inaugurazione del Fintech District, 26 settembre 2017.

[9] Per un approfondimento, si v. *ex multis*: G. LEMME e S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. Banc.*, *www.dirittobancario.it*, dicembre 2016, p. 43; G. LEMME, *Moneta scritturale e moneta elettronica*, Torino, 2003; G. BONAIUTI, *Le nuove forme di pagamento: una sintesi degli aspetti economici*, in *AGE - Anal. Giur. Economia*, 1/2015, pp. 17 e ss.; AA.VV., *The law of Bitcoin*, Bloomington, 2015; S. CAPACCIOLI, *Criptovalute e Bitcoin.Un'analisi giuridica*, Milano, 2015; M. MANCINI, *Valute virtuali e Bitcoin*, in *AGE - Anal. Giur. Economia*, 1/2015, pp. 117 e ss.; R. SCALCIONE, *Gli interventi delle autorità di vigilanza in materia di schemi di monete virtuali*, in *AGE - Anal. Giur. Economia*, 1/2015, pp. 139 e ss..

[10] F. LIONE, *Bitcoin: la rivoluzione della moneta virtuale e non governativa*, in *Diritto&diritti dal 1996*, reperibile nel sito *www.diritto.it*, 5 aprile 2018.

ha classificati come *virtual currency schemed with bidirectional flow*.[11] È in effetti una rete decentralizzata di pagamento *peer-to-peer* dove le transazioni, che avvengono senza un'autorità centrale o un intermediario, sono gestite esclusivamente dagli utenti della rete stessa. Senza dubbio le "criptovalute" sono un mezzo di pagamento "alternativo" rispetto alla tradizionale moneta (ritenuta dai più obsoleta), che permette di semplificare e rendere immediata una determinata operazione/transazione. Tuttavia anche i *bitcoin*, come il *FinTech*, hanno un rovescio della medaglia poiché, facendo capo a una "rete non regolamentata", mi sia passato l'utilizzo di questo termine, può essere utilizzata per attività illecite quali riciclaggio di denaro o finanziamento di attività terroristiche.

Ciò posto, a fronte dell'evoluzione derivante dall'innovazione tecnologica dell'*Industry 4.0*, il sistema bancario-finanziario deve in qualche modo adeguarsi e tutelarsi. Il fenomeno della *digital transformation*, sta notevolmente modificando le abitudini degli investitori/risparmiatori che pertanto si dirigono verso gli operatori che più riescono a soddisfare i loro bisogni, ossia verso quei soggetti che hanno compreso che, per sopravvivere all'interno del sistema bancario-finanziario, è indispensabile una riorganizzazione degli assetti e un'ingente adeguamento tecnologico.

2.1. (Segue) I rischi dell'innovazione nel settore bancario-finanziario

L'innovazione tecnologica nel settore bancario-finanziario ha apportato notevoli benefici (numerose banche hanno inteso perseguire sostanziali modifiche sotto il profilo del *business* e della *vision* aziendale), ma al contempo ha aumentato l'esposizione ai c.d. *cyber risks*.

Difatti, se da un lato la digitalizzazione ha modificato il "modo di fare banca", avvicinando clienti e istituti, investendo i risparmiatori/investitori di una maggiore autonomia grazie all'implementazione di sistemi informatici che hanno reso

[11] BANCA CENTRALE EUROPEA, *Virtual Currency Schemes*, Ottobre 2012.

molto più accessibile la normale operatività bancaria (aprire un conto corrente senza doversi recare presso la filiale dell'istituto bancario prescelto, predisporre un bonifico, sottoscrivere titoli o semplicemente controllare il proprio saldo di conto corrente attraverso un codice o con l'impronta digitale, o ancora attraverso un sistema di riconoscimento biometrico); dall'altro, questa "libertà" di manovra e di accesso, attraverso la rete, permette anche il verificarsi di fenomeni patologici e fraudolenti: per questo il *cyber risk* è divenuto oggi una delle sfide principali che gli istituti bancari si trovano ad affrontare, che è andata a sommarsi e ad amplificare quella di seguire la costante innovazione tecnologica.

L'Unione europea, come accennato, da tempo ha inteso affrontare il problema del *cyber risk*, tanto è vero che il primo atto in merito è risalente nel tempo. Il 10 marzo 2004 con il Regolamento CE n.460/2004 l'Unione europea ha istituito l'**Agenzia europea per la sicurezza delle reti dell'informazione** (ENISA)[12] con lo scopo di collaborare ed integrare il lavoro della Commissione e degli Stati membri, divenuta poi organo essenziale per lo sviluppo della *cyber security* europea. A partire da quel momento l'Unione europea ha emanato numerosi atti[13] sull'argomento fino ad arrivare a quello attualmente più rilevante, ossia la Direttiva NIS che inserisce, anche se indirettamente, nell'ambito della *cyber security* anche i temi della difesa e della sicurezza nazionale, predisponendo un elenco in cui sono evidenziati gli operatori e i fornitori di servizi ritenuti essenziali.[14]

[12] Per un approfondimento sui compiti dell'ENISA si v. il Regolamento (CE) n.460/2004 del Parlamento europeo e del Consiglio che istituisce **l'Agenzia europea per la sicurezza delle reti e dell'informazione**, del 10 marzo 2004, G.U.U.E. L 77 del 13-03-2004; e il contributo di A. ROTONDO, *op. cit.*, pp. 100 e ss., dove si legge «In modo particolare all'Agenzia sono stati affidati numerosi compiti in virtù del suo alto grado di competenza tecnica quali, ad esempio, la consulenza alle Istituzioni europee in materia informatica, l'analisi e la valutazione del rischio dei sistemi, delle reti e dei contenuti dell'informazione, l'attività di sensibilizzazione degli utenti e l'assistenza alla Commissione e agli Stati membri nel dialogo con le industrie di prodotti *hardware* e *software*».

[13] Per un approfondimento ed una ricostruzione storica degli atti emanati a livello europeo e a livello internazionale sulla *cyber security* si v. A. ROTONDO, *op. cit.*, pp. 100 e ss..

[14] Sul punto si rimanda a A. ROTONDO, *op. cit.*, pp. 106 e ss., dove nella nota 46 scrive: «… la Direttiva prevede una sorta di clausola di salvaguardia che *"lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di*

La Direttiva NIS è stata recepita a livello nazionale con il Decreto legislativo 18 maggio 2018, n.65.

Nonostante il rischio operativo nel sistema bancario e finanziario, considerato fondato e di rilevante importanza,[15] sia già ampiamente regolamentato, anche la Direttiva NIS se ne occupa. Come rilevato dalla BCE nel suo parere del 25 luglio 2014, tale Direttiva non incide sul regime giuridico dell'Unione ai fini della sorveglianza dell'Eurosistema sui servizi di pagamento e di regolamento,

tutela della sicurezza nazionale, comprese le misure volte a tutela e le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento dei reati", Direttiva (UE) 2016/1148 *cit.*, art. 1, § 6».

[15] Direttiva europea n.1148 del 2016, Considerando 13, "*… Copre tutte le operazioni comprese la sicurezza, l'integrità e la resilienza delle reti e dei sistemi informativi. Gli obblighi riguardo a tali sistemi, che spesso vanno al di là di quelli previsti nell'ambito della presente direttiva, sono stabiliti in vari atti giuridici dell'Unione, comprendenti le norme sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e le norme sui requisiti prudenziali per gli enti creditizi e le imprese di investimento, comprendenti obblighi in materia di rischio operativo, nonché le norme sui mercati degli strumenti finanziari, comprendenti obblighi sulla valutazione del rischio per le imprese di investimento e per i mercati regolamentati, le norme sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni, comprendenti obblighi in materia di rischio operativo per le controparti centrali e i repertori di dati sulle negoziazioni, e le norme sul miglioramento del regolamento titoli nell'Unione e sui depositari centrali di titoli, comprendenti obblighi in materia di rischio operativo. Inoltre, gli obblighi in materia di notifica di incidenti rientrano nella normale prassi di vigilanza nel settore finanziario e sono spesso inclusi nei manuali di vigilanza. Gli Stati membri dovrebbero prendere in considerazione dette norme e obblighi nell'applicazione della lex specialis*".

riconoscendo altresì l'ampia armonizzazione[16] del settore (Considerando n.12),[17] ma ha l'intento di andare ad implementare il sistema favorendo lo scambio di

[16] A riprova della consistente armonizzazione è stata istituita l'Unione bancaria dove la vigilanza e il controllo, rispetto agli obblighi in capo agli Stati membri, è affidato al Meccanismo di Vigilanza Unico. Per un approfondimento sull'Unione bancaria si rimanda a: S. MICOSSI*, Dalla crisi del debito sovrano all'Unione bancaria*, in M.P. CHITI e V. SANTORO (a cura di), *L'unione bancaria europea*, Pacini editore, Pisa, 2016, pp. 29 e ss.; L. TORCHIA, *La nuova* governance *economica dell'Unione europea e l'Unione bancaria*, in M.P. CHITI e V. SANTORO (a cura di), *L'unione bancaria europea*, Pacini editore, Pisa, 2016, pp. 53 e ss.; M. ORTINO, *L'Unione bancaria nel sistema del diritto bancario europeo*, in M.P. CHITI e V. SANTORO (a cura di), *L'unione bancaria europea*, Pacini editore, Pisa, 2016, pp. 65 e ss.; D. SCHOENMAKER, *Firmer foundations for a stronger European Banking Union*, Bruegel Working Paper n.13, novembre 2015; N.VÉRON, *Europe's radical banking union*, in *Essays and Lectures*, 880, Bruegel, 2015; M. XAFA, *European banking union, three years on*, CIGI papers n.73, giugno 2015. Considerando 11, Direttiva europea n.1148 del 2016, *"… All'interno dell'Unione bancaria, l'applicazione e la vigilanza con riguardo a tali obblighi sono assicurate dal Meccanismo di vigilanza unico. Per gli Stati membri che non fanno parte dell'Unione bancaria esse sono assicurate dalle pertinenti autorità nazionali di regolamentazione del settore bancario. In altri ambiti della regolamentazione del settore finanziario, il Sistema europeo di vigilanza finanziaria assicura anch'esso un elevato grado di analogia e convergenza nelle pratiche di vigilanza. Anche l'Autorità europea degli strumenti finanziari e dei mercati svolge un ruolo di vigilanza diretto per taluni soggetti (vale a dire agenzie di rating del credito e repertori di dati sulle negoziazioni)"*. In generale si v. M. RISPOLI FARINA, e G. ROTONDO, *La vigilanza sul sistema finanziario*, Giuffrè, Milano, 2005. Per una più approfondita panoramica si v.: A. ENRIA, *Nuove architetture e nuove regolamentazioni di vigilanza in Europa,* "Congresso Annuale delle Associazioni dei Mercati" (AIAF, ASSIOM, ATIC-FOREX), Napoli, 2010, p. 10; C. BRESCIA MORRA*, Le nuove autorità per la finanza europee: il miglior compromesso possibile?,* in *www.nelMerito.com*, 2010, p. 1; G. CAROSIO, *op. cit.*, p. 5; M. ONADO, *La supervisione finanziaria europea dopo il Rapporto de Larosière: siamo sulla strada giusta?,* Milano, in *www.bancaria.it*, 2009, p. 17; D. GROS e D. SCHOENMAKER, *European Deposit Insurance and Resolution in the Banking Union*, in *Journal of Common Market Studies*, Volume 52, Issue 3, maggio 2014, pp. 529 e ss.; S. ANTONIAZZI, *Il Meccanismo di vigilanza prudenziale. Quadro d'insieme*, in M.P. CHITI e V. SANTORO (a cura di), *L'unione bancaria europea*, Pacini editore, Pisa, 2016, pp. 175 e ss.; M. GNES, *Il meccanismo di vigilanza prudenziale. Le procedure di vigilanza*, in M.P. CHITI e V. SANTORO (a cura di), *L'unione bancaria europea*, Pacini editore, Pisa, 2016, pp. 243 e ss.. Si v. altresì per un approfondimento all'argomento: R. D'AMBROSIO, *Le Autorità di vigilanza finanziaria dell'Unione*, in V. SANTORO (a cura di), *La crisi dei mercati finanziari: analisi e prospettive,* Milano, 2012, p. 23. Sia consentito *ex multis* rinviare a: S. GIANNETTI, *L'Unione Bancaria Europea e l'accordo sul meccanismo unico di risoluzione delle crisi bancarie (Single Resolution Mechanism - SRM*), in *Associazione Synesis,* Collana Working Papers Numero speciale; S. GIANNETTI, *La crisi internazionale del 2008 in Spagna e la risposta europea*, in *Innovazione e diritto (www.innovazionediritto.it*), 2013, 5. Si v. altresì F. BELLI e V. SANTORO (a cura di), *La Banca centrale europea*, Giuffrè, 2003; S. ANTONIAZZI, *La banca centrale europea tra politica monetaria e vigilanza bancaria*, G. Giappichelli Editore, 2013; F. PAPADIA e C. SANTINI, *La banca centrale europea*, Il Mulino, 2012; F. MOROSINI, *Banche centrali e questione democratica. Il caso della Banca centrale europea* (*Bce*), ETS, 2014.

[17] Considerando 12 della Direttiva n.1148 del 2016: *"La regolamentazione e la vigilanza nel settore bancario e in quello delle infrastrutture dei mercati finanziari sono altamente armonizzate a livello dell'Unione, mediante l'applicazione del diritto primario e secondario dell'Unione e delle norme sviluppate con le autorità europee di vigilanza. All'interno dell'Unione bancaria, l'applicazione e la vigilanza con riguardo a tali obblighi sono assicurate dal*

informazioni ed esperienze relative alla sicurezza delle reti e dei sistemi informativi tra autorità competenti.[18]

3. La Direttiva n.1148 del 2016: *Network and Information Security* (NIS)

"Le reti e i sistemi informativi svolgono un ruolo vitale nella società" (Considerando n.1); è così che la Direttiva NIS inizia ad approcciare il tema della *cyber security*, proseguendo che *"è essenziale che siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno"*.[19] Il preambolo chiaramente introduce l'importanza che la Direttiva assume, quale dato regolamentare e soprattutto di prevenzione, nel settore dei rischi interconnessi nell'ambito delle reti e dei sistemi informativi, ambito che, sviluppatosi notevolmente negli ultimi anni, è ormai assunto ad elemento imprescindibile, al quale nessuno riesce a rinunciare, della vita quotidiana dei cittadini, oggetto di parecchi incidenti, relativi alla sicurezza, che rappresentano una grave minaccia per il funzionamento stesso delle reti e dei sistemi informativi. La Direttiva, al Considerando 2, conferma l'importanza di evitare l'insorgere di siffatti incidenti poiché, *"… possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione"*.[20]

La dimensione sovranazionale assunta dalle reti e dai sistemi informativi, primi tra tutti *internet*, e il loro ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone fa sì che l'eventuale danno arrecato a

Meccanismo di vigilanza unico. Per gli Stati membri che non fanno parte dell'Unione bancaria esse sono assicurate dalle pertinenti autorità nazionali di regolamentazione del settore bancario. In altri ambiti della regolamentazione del settore finanziario, il Sistema europeo di vigilanza finanziaria assicura anch'esso un elevato grado di analogia e convergenza nelle pratiche di vigilanza. Anche l'Autorità europea degli strumenti finanziari e dei mercati svolge un ruolo di vigilanza diretto per taluni soggetti (vale a dire agenzie di rating del credito e repertori di dati sulle negoziazioni)".

[18] Considerando 14 della Direttiva n.1148 del 2016: *"… Lo stesso vale per i membri del Sistema europeo di banche centrali non appartenenti alla zona Euro che esercitano tale sorveglianza sui sistemi di pagamento e di regolamento sulla base di leggi e regolamenti nazionali".*

[19] Direttiva europea n.1148 del 2016, Considerando 1.

[20] Direttiva europea n.1148 del 2016, Considerando 2.

uno di questi sistemi, a causa di un problema di sicurezza, indipendentemente dal luogo in cui si verifica, può ripercuotersi sui singoli Stati membri oltre che avere conseguenze su tutta l'Unione. È questo dunque il motivo per il quale si è arrivati alla conclusione che è necessaria, se non addirittura **essenziale** (termine utilizzato dal legislatore europeo nel Considerando 3 della Direttiva NIS), l'implementazione della sicurezza delle reti e dei sistemi informativi per far sì che l'armonioso funzionamento del mercato interno non venga ostacolato.

L'ambito nel quale è ricompresa la Direttiva NIS è quello del Forum europeo degli Stati membri atto a favorire i dibattiti e lo scambio di "consuetudini", che ha compiuto notevoli progressi in vari settori come, appunto, quello relativo all'elaborazione "principi della collaborazione europea in caso di crisi cibernetica". Il Forum europeo degli Stati membri è pertanto addivenuto alla decisione che, visto lo sviluppo delle reti e dei sistemi informativi, si rende necessaria *"l'istituzione di un gruppo di cooperazione composto da rappresentati degli Stati membri, della Commissione e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), al fine di sostenere ed agevolare la cooperazione strategica fra gli Stati membri"*[21] in tale settore. Il buon fine dell'istituzione di un gruppo di cooperazione, come ideato dal Forum europeo degli Stati membri, è strettamente collegato alla circostanza che essi si dotino di un livello minimo di capacità e di una strategia comune per assicurare la sicurezza, ad alto profilo, delle reti e dei sistemi informativi presenti sui loro territori, evidenziando pertanto come siano ancora carenti le risorse nazionali destinate a questi obiettivi.[22]

[21] Direttiva europea n.1148 del 2016, Considerando 4.

[22] Sotto il profilo dell'armonizzazione delle strategie atte ad assicurare la protezione delle reti e dei sistemi nazioni il legislatore europeo, nel Considerando 5 della Direttiva in esame, è netto sul punto, tanto è vero che, senza giri di parole, specifica che: *"I livelli di preparazione negli Stati membri sono molto diversi tra loro il che ha comportato una frammentazione degli approcci nell'Unione. Ne deriva un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dei sistemi informativi dell'Unione. La mancanza di obblighi comuni imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali rende inoltre impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione"*.

È proprio il conseguimento di un elevato e comune livello di sicurezza della rete e dei sistemi informativi dell'Unione, atto a migliorare il mercato interno, l'oggetto e l'ambito di applicazione dell'art. 1 della Direttiva NIS. Il legislatore europeo intende attuare un approccio globale, per poter dare una risposta efficace alle sfide riguardo alla sicurezza delle reti e dei sistemi informativi a livello dell'Unione, che abbia alla base altresì *"una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza"*[23] per i fornitori e per gli operatori dei servizi essenziali (di cui si tratterà nel prosieguo). Tanto è vero che la Direttiva, per raggiungere gli obiettivi preposti, obbliga: *a*) gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; *b*) istituisce un gruppo di cooperazione per sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri; *c*) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente – rete CSIRT; *d*) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; *e*) obbliga gli Stati membri a designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.[24] Al comma 6 dell'art. 1 è stabilito altresì che sono impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico.

Altresì, il legislatore, attuando unicamente un'armonizzazione minima non impedisce che gli operatori e i fornitori dei servizi essenziali nazionali si dotino di misure più stringenti, con riguardo alla sicurezza, rispetto a quelle dettate dalla Direttiva NIS (opportunità che il legislatore italiano non ha voluto cogliere e di cui si parlerà nei prossimi paragrafi), così come stabilito dall'art. 3. Al momento ci

[23] Direttiva europea n.1148 del 2016, Considerando 6.
[24] Art. 3 Direttiva NIS n.1148/2016.

preme sottolineare che, la Direttiva NIS esclude l'applicazione degli obblighi in capo agli operatori e ai fornitori di servizi essenziali che si occupano di fornire a reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della Direttiva 2002/21/CE del Parlamento europeo e del Consiglio,[25] perché tali imprese sono soggette a specifici obblighi di sicurezza e integrità previsti dalla direttiva; i suddetti obblighi non dovrebbero inoltre applicarsi ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n.910/2014 del Parlamento europeo e del Consiglio,[26] che sono soggetti agli obblighi di sicurezza previsti in tale regolamento,[27] e altresì lascia ampio margine di manovra agli Stati membri con riguardo alle misure atte ad *"assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati"*.[28]

Prima di addentrarci nell'analisi della Direttiva risulta opportuno soffermarsi sull'art. 4, rubricato *Definizioni*, per meglio comprendere il contesto di riferimento delle definizioni che ricorrono nel testo della Direttiva NIS. Quelle su cui si focalizzerà il nostro interesse attengono ai concetti di **rete e sistema informativo**, ovvero *"a) una rete di comunicazione elettronica ai sensi dell'art. 2, lettera a), della direttiva 2002/21/CE; b) un qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un*

[25] Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU L 108 del 24-04-2002, p. 33).
[26] Regolamento (UE) n.910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28-08-2014, p. 73).
[27] Direttiva europea n.1148 del 2016, Considerando 7.
[28] Direttiva europea n.1148 del 2016, Considerando 8. Il Considerando prosegue fornendo il dato legislativo, l'art. 346 del Trattato sul Funzionamento dell'Unione europea (TFUE), secondo il quale *"nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza. In tale contesto sono pertinenti la decisione 2013/488/UE del Consiglio (Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per le informazioni classificate UE) e gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo del semaforo (*Traffic Light Protocol*)"*.

programma, un trattamento automatico di dati digitali; o c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione"; per **sicurezza della rete e dei sistemi informativi** si intende *"la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi"*; la **strategia nazionale per la sicurezza della rete e dei sistemi informativi** consiste in *"un quadro che prevede obiettivi e priorità strategici in materia di sicurezza della rete e dei sistemi informativi a livello nazionale"*;[29] sulla definizione di **operatore di servizi essenziali**, a differenza delle precedenti, la norma, rimanda al successivo art. 5 che appunto è rubricato *Identificazione degli operatori di servizi essenziali* (su v. *infra*). In questa sede ci soffermeremo, in particolare, su cosa si intende per identificazione degli operatori dei servizi essenziali, per strategia in materia di sicurezza della rete e dei sistemi informativi, sulle Autorità nazionali competenti, su punto di contatto e su rete CSIRT.

3.1. (Segue) Identificazione degli operatori di servizi essenziali

L'art. 5 della Direttiva NIS, rubricato *Identificazione degli operatori di servizi essenziali*, stabilisce che, entro il 9 novembre 2018, gli Stati membri dovevano identificare, rispetto ai settori indicati nell'Allegato II – ovvero i settori: dell'energia; dei trasporti; bancario; delle infrastrutture dei mercati finanziari; sanitario; della fornitura e distribuzione di acqua potabile; infrastrutture digitali – gli operatori dei servizi essenziali che hanno sede nel loro territorio nazionale. È lo stesso art. 5, al comma 2, che individua i criteri di cui gli Stati membri devono tener conto nell'identificazione degli operatori dei servizi essenziali all'interno del proprio territorio, e pertanto statuisce che debbano essere dei **soggetti pubblici**

[29] Art. 4, comma 3, Direttiva NIS, n.1148/2016, *Strategia nazionale per la di sicurezza della rete e dei sistemi informativi*, strategia altresì oggetto dell'art. 7 della stessa Direttiva.

o privati che abbiano i seguenti criteri: *a*) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali; *b*) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e *c*) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.[30]

Al 3° comma è inoltre previsto l'obbligo per gli Stati membri di istituire un elenco (nazionale) degli operatori che forniscono servizi essenziali, che deve altresì essere regolarmente riesaminato ed aggiornato, dagli Stati membri, almeno ogni due anni a decorrere dal 9 maggio 2018.[31]

Nell'individuazione degli operatori dei servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali[32] per il proprio territorio, e quindi dei soggetti sottoposti alla disciplina della Direttiva NIS, gli Stati membri sono pressoché autonomi poiché corre solo l'obbligo di seguire un approccio uniforme applicando la definizione di **operatore di servizi essenziali** in modo coerente.[33]

Proprio con il fine di controllare la coerente applicazione della definizione, il legislatore stabilisce che periodicamente ogni Stato membro deve trasmettere alla Commissione dati e informazioni relative ai soggetti considerati **operatori di servizi essenziali**. A fronte di un settore in continua evoluzione, è altresì stabilito

[30] Art. 5, paragrafo 2, Direttiva europea n.1148 del 2016, *Identificazione degli operatori dei servizi essenziali*.

[31] Direttiva europea n.1148 del 2016, Considerando 19: "*…Al fine di garantire che eventuali evoluzioni del mercato siano tenute accuratamente in considerazione, l'elenco di operatori identificati dovrebbe essere rivisto periodicamente dagli Stati membri e aggiornato ove necessario…*".

[32] Direttiva europea n.1148 del 2016, Considerando 20: "*…Nel valutare se un soggetto fornisce un servizio essenziale per il mantenimento di attività sociali ed economiche fondamentali, è sufficiente esaminare se tale soggetto fornisce un servizio incluso nell'elenco di servizi essenziali. Si dovrebbe inoltre dimostrare che la fornitura del servizio essenziale dipende dalle reti e dai sistemi informativi. Infine, nel valutare se un incidente avrebbe un effetto negativo significativo sulla fornitura del servizio, gli Stati membri dovrebbero tenere conto di una serie di fattori intersettoriali, nonché, ove opportuno, di fattori settoriali*".

[33] Direttiva europea n.1148 del 2016, Considerando 1: "*… A tal fine la presente direttiva prevede la valutazione dei soggetti attivi in specifici settori e sottosettori, la definizione di un elenco di servizi essenziali, l'esame di un elenco comune di fattori intersettoriali per stabilire se un potenziale incidente avrebbe effetti negativi rilevanti, un processo di consultazione che coinvolga gli Stati membri interessati nel caso di soggetti che forniscono servizi in più Stati membri, e il sostegno del gruppo di cooperazione nel processo di identificazione… "*.

che l'elenco degli operatori dei servizi essenziali debba essere rivisto periodicamente ed aggiornato dagli Stati membri, ove risulti necessario.

A conferma dell'ampia autonomia lasciata dal legislatore europeo in capo agli Stati membri è a loro riconosciuta la possibilità di integrare l'elenco (di cui all'Allegato II) includendo nuovi servizi che, per ciascuno Stato, siano considerati essenziali, cosa che l'Italia non ha fatto (come accennato e di cui tratteremo in modo più approfondito in sede di analisi del recepimento della Direttiva NIS), limitandosi all'adozione dell'Allegato II così come stilato dal legislatore europeo senza integrare lo stesso di ulteriori servizi c.d. "essenziali".

L'implementazione dell'elenco dei **servizi essenziali** è visto come "*un ulteriore contributo nella valutazione della pratica regolamentare di ciascuno Stato membro al fine di assicurare il livello globale di coerenza nel processo di identificazione fra gli Stati membri*".[34]

3.2. (Segue) Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, Autorità nazionali competenti, punto di contatto e rete CSIRT

Per attuare gli obiettivi proposti dalla Direttiva NIS, anzitutto quello di mantenere un elevato livello di sicurezza della rete e dei sistemi informativi, è necessario che ogni Stato membro si doti di una strategia nazionale in materia e definisca gli obiettivi e gli interventi strategici da attuare:[35] tanto è stabilito dal legislatore sovranazionale, all'art. 7 (*Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi*). Anche in questo caso, il legislatore europeo raccomanda i punti che una valida strategia nazionale deve affrontare per avere dei risultati ottimali, e cioè gli Stati membri devono individuare: *a*) obiettivi e priorità della strategia nazionale; *b*) un quadro di *governance* per conseguire gli obiettivi e le priorità della strategia nazionale, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; *c*) misure di preparazione, risposta e recupero; *d*) programmi di formazione, sensibilizzazione e istruzione

[34] Considerando 23 della Direttiva n.1148 del 2016.
[35] Considerando 29 della Direttiva n.1148 del 2016.

relativi alla strategia; *e*) piani di ricerca e sviluppo relativi alla strategia; *f*) un piano di valutazione per identificare i rischi; *g*) un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale.[36] Anche in questo caso è prevista, da parte dello Stato, la comunicazione alla Commissione della Strategia nazionale entro 3 mesi dall'adozione.

Il legislatore europeo, conscio delle differenze strutturali di *governance* nazionale, al fine di tutelare gli accordi e/o le autorità di vigilanza e di regolamentazione già esistenti (in modo da evitare duplicazioni), stabilisce che ogni Stato membro debba designare più di un'**autorità nazionale competente**, *"responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi degli operatori di servizi essenziali e dei fornitori di servizi digitali"*[37], come stabilito dall'art. 8. Oltre all'Autorità nazionale competente, la Direttiva NIS, per agevolare la cooperazione e la comunicazione transfrontaliera, stabilisce altresì che ogni Stato membro designi un **punto di contatto nazionale unico** cui affidare il coordinamento della sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello dell'Unione,[38] confermato al 4° comma dell'art. 8, il quale precisa che "*il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione (…)*".

Autorità competenti e punti di contatto unici dovrebbero quindi essere dotati di risorse che, sul piano tecnico, finanziario ed umano, siano capaci di garantire, in modo efficiente ed efficace, i compiti a loro assegnati conseguendo gli obiettivi configurati dalla Direttiva (art. 8, comma 5). Anche rispetto alla designazione dell'Autorità nazionale e del punto di contatto unico la Commissione ricopre un ruolo importante poiché le devono essere comunicati i compiti affidati a questi organismi e altresì provvede a rendere nota la loro designazione attraverso la

[36] Art. 7 Direttiva n.1148 del 2016.
[37] Considerando 30 della Direttiva n.1148 del 2016.
[38] Considerando 31 della Direttiva n.1148 del 2016.

pubblicazione di un elenco sulla Gazzetta Ufficiale dell'Unione europea (art. 8, comma 7).

Vista la natura planetaria dei problemi connessi con la sicurezza delle reti e dei sistemi informativi è fondamentale una cooperazione internazionale per migliorare gli scambi di informazioni e promuovere un approccio globale e comune. Per questo motivo è necessario che gli Stati membri abbiano capacità tecniche ed organizzative che siano in grado di "*prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi*",[39] attraverso i **Gruppi di intervento per la sicurezza informatica in caso di incidente** (d'ora in poi CSIRT), le "vecchie" squadre di pronto intervento informatico - CERT, che facciano fronte a rischi ed incidenti e garantiscano una cooperazione a livello europeo[40] (art. 9). È prevista la possibilità di creare i CSIRT anche all'interno delle Autorità nazionali competenti (art. 9, comma 1). La *cyber* sicurezza è così delicata che risulta fondamentale una cooperazione massima, per questo i CSIRT devono partecipare alle reti di cooperazione nazionale, internazionale ed europea. Proprio in virtù del ruolo fondamentale affidato alla cooperazione, l'art. 10, affronta il tema della **cooperazione nazionale**, che prima delle altre è alla base di una tutela efficace della materia. CSIRT, punto di contatto e Autorità nazionale, qualora fossero separati, devono collaborare per adempiere agli obblighi previsti dalla Direttiva NIS (art. 10, comma 1), infatti gli Stati membri devono assicurare che gli istituti preposti (CSIRT, punto di contatto e Autorità nazionale) ricevano le notifiche riguardo gli incidenti ai sensi della Direttiva in esame (art. 10, comma 2).[41] Nell'ottica di controllo imposta dall'Unione europea

[39] Considerando 34 della Direttiva n.1148 del 2016.

[40] Considerando 34 della Direttiva n.1148 del 2016, "*… Per consentire a tutti i tipi di operatori di servizi essenziali e fornitori di servizi digitali di beneficiare di tali capacità e cooperazione, gli Stati membri dovrebbero assicurare che tutti i tipi siano contemplati da un CSIRT designato*".

[41] Su questo aspetto il legislatore europeo è puntuale, tanto è vero che statuisce anche i metodi di comportamento ove non venissero trasmesse le notifiche degli incidenti, e quindi prevede che: "*Ove uno Stato membro decida che i CSIRT non ricevano le notifiche, questi ultimi hanno accesso, nella misura necessaria per l'esecuzione dei loro compiti, ai dati sugli incidenti notificati dagli operatori di servizi essenziali ai sensi dell'articolo 14, paragrafi 3 e 5, o dai fornitori di servizi digitali ai sensi dell'articolo 16, paragrafi 3 e 6*".

anche in merito alla cooperazione è previsto che, a partire dal 9 agosto 2018 e in seguito ogni anno (almeno una volta l'anno), il punto di contatto unico debba trasmettere una relazione al gruppo di cooperazione con riguardo alle notifiche ricevute – specificando numero e natura degli incidenti – e alle azioni intraprese per la sicurezza, degli operatori e dei fornitori dei servizi essenziali (come stabilito rispettivamente dall'art. 14, 3° e 5° comma, e dall'art. 16, 3° e 6° comma).

Al fine di sostenere ed agevolare la cooperazione e lo scambio di informazioni fra Stati, l'art. 11 istituisce un **gruppo di cooperazione** composto dai rappresentanti degli Stati membri, della Commissione (a cui è affidata la segreteria) e dell'ENISA (art. 11, comma 2). Molteplici sono i compiti affidati al **gruppo di cooperazione**, tra i più importanti rilevano quelli di: *"fornire un orientamento strategico per le attività della rete CSIRT"*;[42] scambiare informazioni sulle notifiche degli incidenti; *"discutere le capacità e lo stato di preparazione degli Stati membri e valutare le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi e l'efficacia dei CSIRT e individuare le migliori pratiche"*;[43] scambiare informazioni e migliori pratiche in materia di sensibilizzazione, formazione ricerca e sviluppo riguardo alla sicurezza delle reti e dei sistemi informativi;[44] discutere modalità per la comunicazione di notifiche di incidenti di cui agli articoli 14 e 16. Scadenze relazionali sono fissate anche per il **gruppo di cooperazione**, infatti dal 9 febbraio 2018, e successivamente ogni due anni, deve stabilire un programma di lavoro sulle azioni da intraprendere per attuare gli obiettivi della Direttiva; entro il 9 agosto 2018, e successivamente ogni 18 mesi, deve elaborare una relazione in cui valuta l'esperienza acquisita riguardo alla cooperazione strategica posta in essere.

Come detto, la Direttiva NIS prevede anche la creazione di una **Rete CSIRT** – composta dai rappresentanti dei CSIRT nazionali e del CERT-UE[45] – con il

[42] Art. 11, comma 3, punto a), Direttiva n.1148 del 2016.
[43] Art. 11, comma 3, punto d), Direttiva n.1148 del 2016.
[44] Art. 11, comma 3, punto e) ed f), Direttiva n.1148 del 2016.
[45] Secondo l'art. 12, comma 2, la Commissione europea partecipa alla **Rete CSIRT** come osservatore, mentre all'ENISA è affidato il segretariato.

compito di favorire lo sviluppo della fiducia fra gli Stati membri e la promozione di una cooperazione rapida ed efficace (art.12, comma 1).

I compiti della **Rete CSIRT** sono molteplici e sono specificatamente individuati dalla Direttiva NIS al 3° comma dell'art. 12; tra i più importanti rilevano quelli che riguardano lo scambio delle informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT; sulla richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente e i rischi associati; tuttavia, qualsiasi CSIRT di uno Stato membro può rifiutare di contribuire a tale discussione se ciò rischia di compromettere l'indagine sull'incidente; fornire sostegno agli Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria; discutere, esaminare e individuare ulteriori forme di cooperazione operativa in relazione a categorie di rischi e di incidenti, preallarmi, assistenza reciproca e principi e modalità di coordinamento quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri; discutere gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA.

Anche la **Rete CSIRT** ha l'obbligo di relazionare, al gruppo di cooperazione, sull'esperienza acquisita in merito alla cooperazione operativa, alle conclusioni e alle raccomandazioni.

Nell'ottica dell'importanza del settore di cui si occupa la Direttiva NIS il legislatore europeo affida alla Commissione un ruolo di coordinamento e di controllo, tanto è vero che essa deve non solo coordinarsi con i comitati settoriali competenti e con gli organi costituiti a livello dell'Unione e degli Stati membri, ma deve altresì riesaminare, periodicamente e con scadenze regolari, l'ambito di applicazione della Direttiva in vista delle modifiche da apportare in funzione delle modifiche sociali, politiche, tecnologiche e/o delle condizioni del mercato. Tutto ciò per realizzare l'obiettivo principale della Direttiva NIS, cioè quello di *"conseguire un elevato livello comune di sicurezza delle reti e dei sistemi*

informativi nell'Unione", che non può essere conseguito in misura adeguata e sufficiente esclusivamente dagli Stati membri ma può essere conseguito meglio a livello di Unione.[46]

4. Il Regolamento attuativo della Direttiva NIS, n.151/2018

Per l'applicazione della Direttiva NIS, il Parlamento europeo e il Consiglio hanno emanato il Regolamento di esecuzione n.151 del 30 gennaio 2018, per specificare ulteriormente gli elementi che devono essere presi in considerazione, ai fini della gestione dei rischi della sicurezza delle reti e dei sistemi informativi e dei parametri, dai fornitori di servizi digitali per determinare l'eventuale impatto rilevante di un incidente.

Il Regolamento n.151/2018, seguendo le previsioni della Direttiva NIS, conferma la libertà dei fornitori dei servizi digitali di adottare misure tecniche ed organizzative adeguate e proporzionate alla gestione dei rischi a loro collegati, purché siffatte misure assicurino un adeguato livello di sicurezza, tenendo conto degli elementi prescritti dalla Direttiva. La libertà dei fornitori di servizi digitali è tuttavia condizionata all'obbligo di effettuare delle procedure di valutazione ed analisi atte a riguardare la gestione sistematica delle reti e dei sistemi informativi.[47] Nel processo di valutazione e analisi dei rischi i fornitori di servizi digitali dovrebbero altresì individuare i rischi specifici e stabilirne l'importanza, individuando, ad esempio, come specifica il Regolamento n.151/2018, le minacce alle risorse critiche e il modo in cui esse incidono sulle operazioni, determinando pertanto modalità di attenuazione di tale minacce in base alle capacità correnti e alle esigenze in termini di risorse.[48]

[46] Considerando 34 della Direttiva n.1148 del 2016: L'UE "*… può intervenire in base al principio di sussidiarietà sancito dall'art. 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo*".
[47] Regolamento n.151 del 30 gennaio 2018, Considerando 3.
[48] Regolamento n.151 del 30 gennaio 2018, Considerando 4.

Il regolamento altresì prevede, nel definire la rilevanza dell'impatto di un incidente, che i casi elencati sono solo da considerarsi un elenco non esaustivo di probabili incidenti rilevanti. Difatti, per consentire alle autorità competenti di avere informazioni su eventuali nuovi rischi, i fornitori di servizi digitali, volontariamente, dovrebbero fornire caratteristiche precedentemente sconosciute, come ad esempio, specifica il Considerando 11 del Regolamento, nuovi exploit, vettori di attacco e autori di minacce.

L'oggetto del regolamento, come accennato poc'anzi, è quello di specificare quali sono gli elementi che, i fornitori di servizi digitali, devono prendere in considerazione *"nell'identificazione e nell'adozione delle misure volte a garantire un livello di sicurezza delle reti e dei sistemi informativi che essi utilizzano nel contesto dell'offerta di servizi"*,[49] ma si precisano altresì i parametri da prendere in considerazione per determinare se un incidente abbia un impatto rilevante sulla fornitura di siffatti servizi oppure no.

In merito alla sicurezza delle reti e dei sistemi informativi, il regolamento specifica anche gli elementi di sicurezza, ovvero: "*a) la gestione sistematica delle reti e dei sistemi informativi, ossia la mappatura dei sistemi informativi e la definizione di una serie di politiche adeguate in materia di gestione della sicurezza informatica, comprese le analisi dei rischi, le risorse umane, la sicurezza delle operazioni, l'architettura di sicurezza, la gestione del ciclo di vita dei dati e dei sistemi protetti, e se del caso, la crittografia e la sua gestione; b) la sicurezza fisica e l'ambiente, ossia la disponibilità di una serie di misure volte a proteggere le reti e i sistemi informativi dei fornitori di servizi digitali dai danni attraverso il ricorso ad un approccio globale ai pericoli basato sui rischi, che affronti ad esempio gli errori di sistema, gli errori umani, gli atti dolosi o i fenomeni naturali; c) la sicurezza delle forniture, ossia la definizione e il mantenimento di politiche adeguate al fine di assicurare l'accessibilità e, se del caso, la tracciabilità delle forniture critiche utilizzate nella prestazione dei*

[49] Regolamento n.151 del 30 gennaio 2018, art. 1.

servizi; d) i controlli dell'accesso alle reti e ai sistemi informativi, ossia la disponibilità di una serie di misure volte ad assicurare che l'accesso fisico e logico delle reti e ai sistemi informativi, ivi inclusa la sicurezza amministrativa di tali reti e sistemi, sia autorizzato e limitato sulla base di esigenze aziendali e di sicurezza".[50] Esso indica anche quali sono le misure che il fornitore di servizi digitali deve adottare con riguardo al trattamento degli incidenti, ovvero: "*a) il mantenimento e la prove di processi e procedure di individuazione per assicurare l'individuazione tempestiva e idonea degli eventi anomali; b) i processi e le politiche per la segnalazione degli incidenti e l'individuazione delle debolezze e vulnerabilità nei propri sistemi informativi; c) una risposta conforme alle procedure stabilite e la comunicazione dei risultati ottenuti con la misura adottata; d) la valutazione della gravità dell'incidente, la documentazione delle conoscenze acquisite grazie all'analisi dell'incidente e la raccolta di informazioni pertinenti da utilizzare eventualmente come prova e per sostenere un processo di costante miglioramento"*.[51]

Il regolamento affronta anche la gestione della continuità operativa rispetto al ripristino dell'organizzazione dei servizi a livelli predefiniti in seguito ad un incidente, stabilendo che è necessaria: *a*) la definizione e l'uso di piani di emergenza basati sull'analisi dell'impatto sulle attività aziendali volti a garantire la continuità dei servizi erogati dai fornitori di servizi digitali e valutati e testati regolarmente, ad esempio mediante esercitazioni; *b*) la capacità di ripristino di emergenza, valutata e testata regolarmente, ad esempio mediante esercitazioni.

Il regolamento proprio in virtù della sua completezza indica anche quali sono i "*parametri da prendere in considerazione al fine di determinare se l'impatto di un incidente è rilevante*", previsto dall'art. 3 del Regolamento n.151/2018. È stabilito che, in base al numero di utenti interessati da un incidente il fornitore di servizi digitali è in grado di stimare: *a*) il numero di persone fisiche e giuridiche interessate con cui è stato concluso un contratto per la fornitura del servizio, o

[50] Regolamento n.151 del 30 gennaio 2018, art. 2.
[51] Regolamento n.151 del 30 gennaio 2018, art. 2.

b) il numero di utenti interessati che hanno utilizzato il servizio in particolare in base ai precedenti dati sul traffico. Il regolamento si sofferma anche sulla durata dell'incidente,[52] sulla diffusione geografica[53] e sulla portata della perturbazione del funzionamento del funzionamento del servizio.[54] Oltre ai citati parametri il Regolamento stabilisce altresì un elenco di situazioni che devono sussistere per far sì che "un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni" (art. 4): *a*) il servizio fornito da un fornitore di servizi digitali non è stato disponibile per oltre 5.000.000 di ore utente, dove per ore utente si intende il numero di utenti interessati nell'Unione per una durata di sessanta minuti; *b*) l'incidente ha provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo del fornitore di servizi digitali che ha interessato oltre 100.000 utenti nell'Unione; *c)* l'incidente ha generato un rischio per la sicurezza pubblica, l'incolumità pubblica o in termini di perdite di vite umane; *d*) l'incidente ha provocato danni materiali superiori a 1.000.000 di euro per almeno un utente nell'Unione.

5. Il Decreto legislativo n.65 del 2018 di attuazione della Direttiva NIS

Nel mese di maggio 2018 è stato approvato in Consiglio dei ministri il Decreto legislativo di attuazione alla Direttiva NIS (D.lgs. n.65/2018), entrato in vigore il 26 giugno.

[52] Regolamento n.151 del 30 gennaio 2018, art. 3, "*La durata dell'incidente di cui all'articolo 16, paragrafo 4, lettera b), della Direttiva (UE) n.1148/2016 è il periodo tra la perturbazione della regolare prestazione del servizio in termini di disponibilità, autenticità, integrità o riservatezza e il momento del ripristino*".

[53] Regolamento n.151 del 30 gennaio 2018, art. 3, "*Per quanto riguarda la diffusione geografica relativamente all'area interessata dall'incidente di cui all'articolo 16, paragrafo 4, lettera c), della direttiva (UE) 2016/1148, il fornitore di servizi digitali è in grado di stabilire se l'incidente influisce sulla fornitura dei suoi servizi in determinati Stati membri*".

[54] Regolamento n.151 del 30 gennaio 2018, art. 3, "*La portata della perturbazione del funzionamento del servizio di cui all'articolo 16, paragrafo 4, lettera d), della direttiva (UE) 2016/1148 è misurata per una o più delle seguenti caratteristiche compromesse dall'incidente: disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi correlati*".

L'approccio del decreto è *soft* nel senso che esso si limita ad "assorbire" quanto già stabilito dalla Direttiva senza andare ad aggiungere contenuti ulteriori.

La Direttiva europea, come abbiamo visto, lascia ampio margine di manovra agli Stati membri per ampliare l'ambito di applicazione delle disposizioni in essa contenute, possibilità che, come si dirà a breve, non è stata sfruttata dal governo italiano che ha deciso di limitarsi ad applicare la Direttiva solo ai settori già stabiliti in ambito europeo. I settori enunciati dalla Direttiva, lo ricordiamo, sono energia, trasporti, banche, mercati finanziari, sanità fornitura e distribuzione di acqua potabile e infrastrutture digitali, nonché motori di ricerca, servizi *cloud* e piattaforme di commercio elettronico. Ad avviso di chi scrive, sarebbe stato necessario, tramite il recepimento, estendere la normativa in esame anche al settore della pubblica amministrazione in considerazione della grande quantità di dati trattati, in maggioranza "sensibili", nonché per il ruolo fondamentale che ricopre a livello nazionale. Ad ogni buon conto, la pubblica amministrazione, nella funzione di erogatrice dei servizi ricompresi nei settori elencati, sarà comunque sottoposta all'applicazione della Direttiva NIS.

Il D.Lgs. n.65/2018 stabilisce, come enunciato dall'art. 1, misure volte a conseguire un elevato livello di sicurezza della rete e dei sistemi informativi in ambito nazionale, prevedendo, come richiesto dalla Direttiva NIS, una strategia nazionale, la designazione di autorità nazionali competenti, del punto di contatto unico, nonché di un **Gruppo di intervento per la sicurezza informatica** in caso di incidente in ambito nazionale (CSIRT). Come evidenziato nei paragrafi precedenti, la Direttiva NIS all'art. 4 adotta un elenco di termini e relative definizioni utili a definire il quadro di riferimento; siffatte definizioni sono riprese dal D.Lgs. n.65/2018, all'art. 3.

In merito all'identificazione degli operatori dei servizi essenziali, l'art. 4, comma 1, del D.Lgs. stabilisce che le autorità competenti NIS hanno il compito di identificare, per ciascun settore e sottosettore dell'Allegato II, gli operatori dei servizi essenziali che abbiano sede nel territorio nazionale. È istituito presso il Ministero dello sviluppo economico l'elenco nazionale degli operatori dei servizi

essenziali che è riesaminato ed aggiornato su base regolare dalle autorità NIS competenti, proprio come previsto dalla Direttiva, ogni 2 anni a partire dal 9 maggio 2018. È altresì previsto che il punto di contatto unico debba trasmettere alla Commissione europea le informazioni[55] sulla valutazione dell'attuazione della disciplina in ambito nazionale secondo un approccio coerente rispetto all'identificazione degli operatori dei servizi essenziali.

Rispettando pedissequamente quanto richiesto dall'art. 7 della Direttiva n.1148/2016, il D.Lgs. n.65/2018, all'art. 6, prevede l'adozione di una strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei Ministri. La strategia nazionale dovrà senz'altro partire dal presupposto di base di ideare programmi e iniziative volte alla formazione e alla sensibilizzazione in materia di sicurezza informatica, concepire un piano di valutazione dei rischi e di prevenzione degli stessi a fronte di incidenti informatici. Il Presidente del Consiglio dei Ministri, di fatto, adotta, sentito il CSIRT, una strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale (art. 6, comma 1) nella quale devono essere indicati gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi; il quadro di *governance* per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; i piani di ricerca e sviluppo; un piano di valutazione dei rischi; l'elenco dei vari attori coinvolti nell'attuazione (art. 6, comma 2). È affidato alla Presidenza del Consiglio dei Ministri il compito di trasmettere alla Commissione europea la

[55] Art. 4, comma 8, D.Lgs. n.65/2018. Siffatte informazioni riguardano "*a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali; b) l'elenco dei servizi di cui al comma 2; c) il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II ed un'indicazione della loro importanza in relazione a tale settore; d) le soglie, ove esistano, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 5, comma 1, lettera a), o all'importanza di tale particolare operatore di servizi essenziali di cui all'articolo 5, comma 1, lettera f)*".

strategia nazionale, entro 3 mesi dalla sua applicazione (sono esclusi dalla trasmissione alla Commissione europea le informazioni riguardo la sicurezza nazionale).

Come anticipato, gli istituti di credito, il settore bancario e quello finanziario sono sempre più esposti al *cyber risk* e pertanto si stanno muovendo nell'ottica di rafforzare la propria sicurezza informatica in vari modi. In linea con la Strategia nazionale di sicurezza cibernetica è nato, verso la fine del 2016 in accordo con Banca d'Italia e Associazione Bancaria Italiana (ABI), il CERTFin, un'iniziativa cooperativa pubblico-privata finalizzata ad aumentare la gestione del *cyber risk* degli operatori bancari e finanziari attraverso il supporto strategico ed operativo di attività di prevenzione, preparazione e risposta degli attacchi informatici o degli incidenti di sicurezza.[56]

Il CERTFin eroga, ai propri soci, essendo esso un'iniziativa cooperativa alla quale possono partecipare tutti gli operatori del settore bancario e finanziario italiano (previa la sottoscrizione di un modulo e il versamento di una quota di adesione), servizi di sicurezza informatica attraverso il centro per l'analisi e la condivisione delle informazioni (FinISAC); l'Osservatorio *Cyber Knowledge and Security Awareness*; e la centrale operativa per la gestione delle emergenze *cyber*. Il CERTFin collabora con molti soggetti pubblici e privati rappresentando quindi il punto di raccordo tra il settore finanziario e gli altri settori strategici in tema di *cyber security*.[57]

Il CERTFin è governato da ABI e Banca d'Italia, che ne condividono la presidenza, ed è gestito dal Consorzio ABI Lab. La sua *mission* è quella di facilitare lo scambio tempestivo di informazioni tra gli operatori del settore su potenziali minacce informatiche; costituire il punto di contatto privilegiato del settore finanziario con l'architettura istituzionale per la protezione cibernetica e la sicurezza informatica; facilitare la risposta a incidenti informatici su larga scala; supportare il processo di soluzione di crisi cibernetica; cooperare con

[56] Informazioni reperibili al sito del CERTFin, *www.certfin.it*.
[57] Informazioni reperibili al sito del CERTFin, *www.certfin.it*.

analoghe istituzioni nazionali e internazionali e con altri attori pubblici e privati coinvolti nella *cyber security*; e accrescere la consapevolezza e la cultura della sicurezza.[58]

L'organizzazione del CERTFin si articola su un livello decisionale-strategico, costituito dal Comitato Strategico, che indirizza il CERT e le linee di sviluppo del settore, e su un livello tattico-operativo, costituito dal Comitato Direttivo, che definisce e guida la gestione dei servizi offerti ai soci cooperatori, e dalla Direzione Operativa, che è responsabile delle attività operative del CERTFin e della gestione segretariale dei Comitati e amministrativa delle partecipazioni.

Tornando al D.Lgs. di recepimento della Direttiva NIS, il governo ha deciso di decentrare i compiti relativi alle autorità competenti per l'attuazione degli obiettivi della Direttiva e la relativa vigilanza ai Ministeri per lo sviluppo economico, per le infrastrutture e per i trasporti, per l'economia, per la salute e per l'ambiente i compiti relativi alle proprie aree di competenza. Con riguardo all'applicazione nazionale della direttiva, seguendo pertanto il dispositivo dell'art. 8, il D.Lgs. designa le Autorità competenti NIS, affidando per il settore bancario e finanziario questo compito al Ministero dell'economia e delle Finanze congiuntamente alle autorità di vigilanza del settore (Banca d'Italia e Consob), che devono collaborare e scambiarsi informazioni. Le Autorità competenti NIS sono responsabili dell'attuazione del D.Lgs. n.65/2018 rispetto ai propri settori di competenza e pertanto vigilano sull'applicazione delle norme nazionali attraverso poteri ispettivi e sanzionatori.

Il **punto di contatto unico**, ovvero il collegamento tra Unione europea e autorità compenti nazionali in materia di *cyber security* è individuato nel gruppo di cooperazione e nei CSIRT, il Dipartimento delle informazioni per la sicurezza (DIS). L'obbligo di comunicazione alla Commissione sulla designazione del **punto di contatto unico** e delle **Autorità Competenti NIS**, e sui loro compiti e/o modifiche, è assegnato alla Presidenza del Consiglio dei Ministri.[59]

[58] Informazioni reperibili al sito del CERTFin, *www.certfin.it*.
[59] Art. 7, comma 7, D.Lgs. n.65/2018.

Il disposto dell'art. 9 della Direttiva NIS impone altresì agli Stati membri di creare **Gruppi di intervento per la sicurezza informatica** in caso di incidente (CSIRT), applicato in Italia dal D.Lgs. n.65/2018 attraverso l'istituzione, presso la Presidenza del Consiglio dei Ministri, di un *Computer Security Incident Response Team* (CSIRT Italiano) con il compito non solo di prevenire e dare pronta risposta ad eventuali incidenti informatici, ma anche quello di cooperare con gli altri CSIRT Europei. Il CSIRT Italiano, attuando una fusione, andrà a sopprimere gli attuali CERT Nazionale del Ministero dello Sviluppo Economico e il CERT-PA dell'Agenzia per l'Italia Digitale. Siffatta fusione, ad ogni buon conto, non sarà di facile attuazione e pertanto i tempi per l'entrata in vigore effettiva del CSIRT Italiano potrebbe subire dei ritardi. Il CSIRT italiano sarà composto da 30 funzionari, di cui 15 scelti tra dipendenti delle amministrazioni pubbliche, e 15 da assumere in aggiunta. I principali compiti del CSIRT italiano sono specificati all'art 8, 5° e 6° comma, ovvero definisce le procedure per la prevenzione e la gestione degli incidenti informatici, garantisce la collaborazione effettiva, efficiente e sicura nella rete CSIRT. L'obbligo di comunicazione alla Commissione è anche in questo caso affidato alla Presidenza del Consiglio dei Ministri che deve comunicare il mandato del CSIRT nazionale e le modalità di trattamento degli incidenti a questo affidati (art. 8, comma 7).

L'unica innovazione rispetto alla Direttiva NIS apportata dal D.Lgs. di recepimento è quella di istituire, con il fine di ottenere una cooperazione nazionale adeguata, in aggiunta alla collaborazione congiunta delle Autorità Competenti NIS, del punto di contatto unico e del CSIRT italiano, presso la Presidenza del Consiglio dei Ministri, un Comitato Tecnico di Raccordo – composto da rappresentanti delle amministrazioni statali, regionali e delle province autonome.

6. Il Rapporto CLUSIT 2019

Un cenno va fatto altresì al ruolo del CLUSIT, **Associazione Italiana per la Sicurezza Informatica**, che da diversi anni si occupa della sicurezza informatica.

Nata nel 2000 sulla scorta delle esperienze di associazioni europee per la sicurezza informatica, si pone diversi obiettivi tra i quali quello di diffondere la cultura delle sicurezza informatica presso le aziende, la pubblica amministrazione e i cittadini; partecipare all'elaborazione di leggi, norme e regolamenti, sia a livello comunitario che nazionale, relativi alla scurezza informatica; contribuire ad organizzare percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della ICT; promuovere l'uso di metodologie e tecnologie che consentono di migliorare il livello di sicurezza delle varie realtà.

Ogni anno il CLUSIT pubblica un rapporto sulla sicurezza ICT in Italia. Il Rapporto CLUSIT 2019 parte dall'assunto che il 2018, senza ombra di dubbio, è stato l'anno peggiore per la *cyber security* poiché, come confermano i dati, vi è stata una evoluzione delle minacce *cyber*, sia dal punto di vista quantitativo sia dal punto di vista qualitativo, soprattutto nel settore finanziario (+ 33% nel 2018) dove si è assistito ad una crescita degli attacchi sia per gravità che per quantità.

A conferma di questo assunto di partenza vengono evidenziati i dati raccolti e analizzati dal pool di esperti che redigono il Rapporto stesso, facendo notare come vi siano stati 1.552 attacchi gravi negli ultimi 12 mesi, ben il 37,7% in più rispetto all'anno precedente, con una media di 129 attacchi gravi al mese, rispetto ad una media di 94 al mese nel 2017, e di 88 su 8 anni.[60] Il Rapporto CLUSIT 2019 è diviso in diverse aree, vi è una prima parte dove, come detto, vengono analizzati gli attacchi *cyber* del 2018 e le previsioni per il 2019, utilizzando contributi della Polizia Postale e delle Comunicazioni, del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza e del CERT Nazionale; la seconda denominata **Speciale FINANCE**, che ci interessa maggiormente e sulla quale ci soffermeremo nel proseguo, formata a sua volta da 4 contributi a cura dell'IBM, della *Communication Valley Reply*, della Banca d'Italia e della *Lutech*; la terza riguardo allo "Speciale GD.P.R.", poiché come sappiamo il 2018 è stato l'anno

[60] AA.VV., *Rapporto CLUSIT 2019*, Milano, 2019, pp. 7 e ss..

cruciale per la *Data Protection* in quanto il 25 maggio 2018 è entrato in vigore il GD.P.R.; la quarta sezione viene dedicata all'**Intelligenza Artificiale**; la quinta sezione alla **Blockchain**; ed infine l'ultima sezione del rapporto è dedicata all'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.

Come detto, soffermeremo la nostra attenzione sulla sezione **FINANCE**, composta da diversi contributi che ricostruiscono il panorama del *cyber crime* finanziario degli ultimi 12 mesi.

Secondo il Rapporto[61] anche a livello finanziario emerge con chiarezza come il 2018 sia stato un anno colmo di importanti sviluppi per il *cyber crime*, poiché numerose sono le novità sia con riferimento ai *malware* utilizzati che per il *modus operandi* attuato dai gruppi *cyber* criminali.[62]

Molti sono stati gli attacchi tramite *malware* usati per rubare numeri e dati di carte di credito, per accedere a banche in Francia, Polonia, Austria,[63] Turchia, per colpire piattaforme di cripto valute e utenti di banche *online* del Regno Unito. Anche l'Italia, evidenzia il Rapporto, è stata colpita da attacchi di *malware* di diverse specie che hanno creato non pochi disagi agli utenti colpiti. Il Rapporto evidenzia come l'elemento che più ha accresciuto lo sviluppo di questi *malware* è sicuramente la compartecipazione della vittima che inavvertitamente fornisce le credenziali d'accesso ai propri conti cliccando su *link* contenuti in mail che, solo all'apparenza, sono simili a quelle che si possono ritenere provenienti da siti accreditati di *internet banking*. Oltretutto, negli ultimi mesi del 2018, si è sviluppato un nuovo *modus operandi* che agisce non più sulle credenziali dell'utente, ma solo nel momento dell'effettiva operazione dispositiva,

[61] Gli autori dei contributi all'interno della sezione **Speciale FINANCE** del Rapporto CLUSIT 2019 sono per l'IBM, P.L. ROTONDO e D. RAGUSEO (a cura di), *Elementi sul cybercrime nel settore finanziario in Europa*; per *Valley Reply* L. ROCCO, *Analisi del cybercrime finanziario in Italia nel 2018*; per il CERT della Banca d'Italia P. DIGREGORIO e B. GIANNETTO, *Sviluppo di un sistema di cyber torea intelligence*; ed infine per Lutech L. SANGALLI e L. DINARDO (a cura di), *Carding – Scenario ed evoluzione dei canali di vendita nel 2018*.

[62] P.L. ROTONDO e D. RAGUSEO (a cura di), *Elementi sul cybercrime nel settore finanziario in Europa*, in AA.VV., *Rapporto CLUSIT 2019*, Milano, 2019, pp. 105 e ss..

[63] P.L. ROTONDO, e D. RAGUSEO, *op. cit.*, pp. 105 e ss..

sostituendo le coordinate bancarie del beneficiario; questo sistema quindi segue l'utente nelle operazioni di *login* e navigazione senza intervenire se non nel momento in cui si effettua l'operazione: tecnica nota con il nome di *webinject*.[64]

Quelle accennate sono solo alcune delle tecniche che gli *hacker* o i gruppi criminali mettono a punto per reperire dati sensibili e attuare frodi finanziarie, ma sui profili tecnici di queste vicende non possibile soffermarsi in questa sede.

Rileva però sottolineare, come conferma il Rapporto, l'idea secondo la quale le frodi finanziarie siano attuate, ormai da qualche anno, non più da singoli e solitari *hacker*, bensì da gruppi criminali organizzati che possiedono competenze tecniche avanzate e che permettano di aggiornare costantemente i *malware*, ogni qualvolta che vengano identificati dalle soluzioni di *advanced fraud protection* esistenti. Le *advanced fraud protection* sembrano essere promettenti poiché riescono a combinare numerosi fattori di rischio per identificare la sessione sospetta prima che venga ultimata la transazione.[65]

Per altro verso, l'evoluzione della *cyber security* induce a ritenere che molto presto le password andranno a scomparire a causa dei molteplici *data breach*,[66] ovvero una violazione di sicurezza che comporta, in modo accidentale o in modo illecito, la divulgazione non autorizzata o l'accesso a dati personali compromettendo pertanto la riservatezza, l'integrità o la disponibilità di dati personali. La progressiva scomparsa dell'utilizzo delle password, come oggi le intendiamo, sta dando il passo all'utilizzo dell'impronta digitale che, secondo il *Future of Identity Study* 2018,[67] risulta essere più sicura anche se tuttavia già sembrano sussistere dei *data breach* relativi all'autentificazione biometrica. La *Multi-Factor Authentication* (MFA), l'identificazione a più fattori, è sicuramente il futuro della protezione per le credenziali di accesso poiché la MFA combina più

[64] P.L. ROTONDO e D. RAGUSEO, *op. cit.*, pp. 111 e ss..
[65] P.L. ROTONDO e D. RAGUSEO, *op. cit.*, pp. 114 e ss..
[66] Vasto è il campo del Data Breach, si v. *ex multis*, il sito del Garante per la protezione dei dati personali.
[67] P.L. ROTONDO, *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand*, reperibile sul sito *www.SecurityIntelligence.com*, Gennaio 2019.

elementi di identificazione in modo da rendere più complessa l'intromissione all'interno del sistema contenente dati sensibili da parte di malintenzionati.[68]

Tuttavia, nonostante le soluzioni proposte dai fornitori di servizi essenziali, così come intesi dalla Direttiva NIS e dagli atti normativi cui sono susseguiti, e quindi anche dai fornitori di servizi finanziari, siffatte soluzioni devono essere continuamente aggiornate e implementate proprio come vengono migliorati i *malware* e gli altri sistemi utilizzati dai gruppi criminali informatici, in quanto in un contesto così dinamico le soluzioni individuate diventano rapidamente obsolete.[69]

Oggi il panorama nazionale, europeo e mondiale è costantemente rivolto alla digitalizzazione dei sistemi e dei servizi pertanto è maggiormente esposto agli attacchi dei *cyber* criminali che come visto prendono continuamente di mira i sistemi per accedere a dati sensibili, soprattutto a livello bancario-finanziario. Difatti, proprio le organizzazioni criminali continuano ad alimentare il mercato del *malware as a service* per rubare credenziali ed attuare frodi bancarie.[70]

Pertanto, possiamo affermare che il furto di credenziali attuato tramite l'uso di *malware* resta una minaccia che non deve essere sottovalutata, soprattutto dalle banche che forniscono servizi di *internet banking*.

Per far fronte ai numerosi attacchi cibernetici contro gli istituti finanziari, in particolare banche e banche centrali, occorre che si passi dal *risk management* alla prevenzione della minaccia[71] poiché gli attacchi alle istituzioni finanziarie generalmente sono rivolti a reperire dati sensibili e strategici che posso anche compromettere infrastrutture critiche, come quelle dei sistemi di pagamento transnazionali e le piattaforme finanziarie.[72] L'evoluzione normativa nel settore

[68] P.L. ROTONDO e D. RAGUSEO, *op. cit.*, pp. 114 ss. e P.L. ROTONDO, *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand, op. cit.*.
[69] P.L. ROTONDO e D. RAGUSEO, *op. cit.*, pp. 115 e ss..
[70] L. ROCCO, *Analisi del cybercrime finanziario in Italia nel 2018*, in AA.VV., *Rapporto CLUSIT 2019*, Milano, 2019, pp. 129 e ss..
[71] P. DIGREGORIO e B. GIANNETTO, *Sviluppo di un sistema di cyber torea intelligence*, in AA.VV., *Rapporto CLUSIT 2019*, Milano, 2019, pp. 137 e ss..
[72] P. DIGREGORIO e B. GIANNETTO, *op cit.*, pp. 137 e ss..

sicuramente avrà un impatto positivo, si vedano soprattutto le Direttive europee quali la GD.P.R. e la stessa Direttiva NIS, poiché imporrano alle imprese e alle pubbliche amministrazioni di predisporre dei *budget ad hoc* funzionali allo sviluppo della *compliance* e della sicurezza dei dati e delle informazioni.

7. Conclusioni

L'innovazione tecnologica nel settore bancario, da un lato, ha avuto un impatto fortemente positivo, in quanto ha fatto nascere "un nuovo modo di fare banca", dove il cliente è più autonomo nelle decisioni e meno legato alla banca quale entità fisica, dall'altro è contraddistinta da profili di opacità e criticità che portano ad incorrere nel cosiddetto *cyber risk*. L'aumento del *cyber risk*, soprattutto nel settore bancario, ha fatto emergere come quanto fatto finora in un'ottica di prevenzione non sia stato sufficiente. Come abbiamo visto, soprattutto a livello europeo con la Direttiva NIS, e conseguentemente a livello nazionale, con il D.Lgs. n.65/2018, si è inteso agire per migliorare la *cyber resilience* del settore bancario-finanziario adottando strategie e regole più incisive. Nonostante la messa a punto di tali regole, la creazione di Autorità nazionali competenti per settore e l'implementazione della cooperazione si ritiene che vi sia ancora molto da fare, soprattutto nel settore bancario-finanziario, per arginare il *cyber risk*. Difatti, oltre alle iniziative già poste in essere, si ritiene necessario che le banche rafforzino la *cyber security* fornendosi di personale qualificato e specializzato in materie informatiche e di sistemi di sicurezza più difficili da eludere.

L'evoluzione tecnologica del settore bancario-finanziario è sicuramente un'innovazione importante, ma per far sì che gli istituti fruiscano realmente di questa innovazione è necessario che sussista una parallela evoluzione della sicurezza cibernetica in quanto solo in questo modo possono continuare a detenere una posizione rilevante nell'economia e nel mercato, essendo proprio la sicurezza dei dati e dei clienti uno dei criteri che i consumatori/investitori utilizzano nella scelta dell'istituto di riferimento. Per questi motivi, gli intermediari bancari-finanziari dovranno puntare sull'affidabilità e la sicurezza quali

condizioni essenziali per mantenere un rapporto di fiducia con la clientela duraturo nel tempo.