LA DIRETTIVA NIS II CYBERSECURITY IN EUROPA: TRA INNOVAZIONE, FORMAZIONE E DIRITTO VIVENTE

Abstract

Il presente contributo guarda alla recente approvazione della direttiva NIS II quale riforma rilevante per la *cybesecurity* in Europa. Essa si misurerà con le intersezioni tra innovazione, nuove necessità formative e le sfide del diritto vivente. La direttiva, basata su tre assi fondamentali (coordinamento, consapevolezza, collaborazione tra settore pubblico e privato), distingue soggetti essenziali e soggetti importanti tra le infrastrutture rilevanti per settori e infrastrutture critiche e strategiche dell'Unione europea. Consente, inoltre, di immaginare nuovi scenari tanto nella didattica quanto nella ricerca di settore, all'incontro con un nuovo complesso di strategie e adempimenti che si rendono necessari per affrontare l'era digitale in Europa e fuori dai suoi confini.

This contribution looks at the recent approval of NIS II directive as a relevant reform for cybersecurity in Europe, which will be confronted with the intersections between innovation, new training needs and the challenges of the so-called living Law. The directive, based on three key elements (i.e., coordination, awareness, and collaboration between public and private partners), distinguishes essential subjects and important subjects among relevant infrastructures for critical and strategic sectors and infrastructures of the European Union. Furthermore, it allows to imagine new scenarios both in teaching and research, meeting a new set of strategies and obligations that seem to be necessary to face the digital era in Europe and beyond its borders.

Keywords: Cybersecurity, Network&information Security, NIS II, EU/Directive/2022/2555, Compliance.

1. *Network Information Security* (NIS) II: prospettive plurali su una riforma

Il presente contributo intende mettere in luce le intersezioni tra innovazione, formazione e diritto a partire dalla direttiva UE 2022/2555, c.d. NIS II (*Network Information Security*) da ultimo approvata dalle istituzioni europee e pubblicata nella gazzetta ufficiale dell'Unione. Si tratta di una direttiva del Parlamento europeo e del Consiglio rivolta alla necessità di raggiungere un livello comune elevato di *cybersecurity* in Unione Europea. Il testo normativo mette in luce evidenti potenziali ricadute anche al di fuori dei confini dell'ordinamento sovranazionale. La riforma in esame prevede l'abrogazione della c.d. "direttiva NIS" cioè a dire della direttiva UE 2016/1148 del 6 luglio 2016 recante misure per garantire un livello elevato – e comune tra gli Stati Membri – di

sicurezza delle reti e dei sistemi informativi dell'Unione[1], la modifica del regolamento UE 910/2014 e della direttiva UE 2018/1972. In Italia, la direttiva NIS è stata recepita con d.lgs. n. 65 del 18 maggio 2018. Questa norma ha introdotto significative misure a modificazione dell'ordinamento giuridico nazionale a tutela dei valori e al raggiungimento degli obiettivi comuni fissati dalla normativa europea in argomento, insieme alla più recente legge n. 109 del 4 agosto 2021 intervenuta in tema di *cyber*-sicurezza e per consentire l'istituzione di un'agenzia nazionale.

La direttiva NIS, nella sua prima versione, è stata approvata ormai sei anni fa e pubblicata in GUUE n. 194 del 19 luglio del 2016, prevedendo un termine per il recepimento da parte degli Stati Membri di 18 mesi (nella specie entro il 9 maggio del 2018). La direttiva NIS II dovrà essere recepita dagli Stati membri dell'Unione entro il 18 ottobre 2024.

L'adozione di questa particolare forma di manifestazione del diritto derivato dell'Unione Europea, nella revisione della disciplina in materia di sicurezza delle reti e delle informazioni, potrà risultare produttiva di effetti positivi accompagnati, però, dallo stesso ordine di criticità emerse nella sua applicazione precedente risultata difforme nei differenti ordinamenti giuridici nazionali che l'hanno recepita. Proprio a tali difformità e disparità – e ai loro effetti deteriori – NIS II tenta, almeno in parte, di porre rimedio, in continuità con le misure adottate in passato. Se chi scrive ritiene condivisibile l'orientamento delle recenti politiche dell'Unione in materia volto a consentire un apprezzabile margine di discrezionalità degli Stati nazionali in considerazione della rilevante eterogeneità dei contesti e delle soggettività giuridiche coinvolte dalla (e nella) *cybersecurity*, l'obiettivo dell'uniformità delle legislazioni nazionali avrebbe certamente potuto essere perseguito con migliore e maggiore efficacia grazie all'adozione di un regolamento (direttamente applicabile senza la necessità di una normativa nazionale di recepimento). Ciò a partire dalla necessità di considerare le ricadute importanti della *cybersecurity* in materia di diritti fondamentali dei cittadini dell'UE[2], nonché in relazione alla evidente e sempre maggiore interconnessione tra le infrastrutture critiche dei diversi Stati membri.

[1] La direttiva rientra in un pacchetto di misure volte a migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso nel campo della *cybersecurity* e della protezione delle infrastrutture critiche, pur individuate con una differente denominazione.

[2] Come avvenuto, a titolo esemplificativo, anche in occasione dell'approvazione del regolamento UE 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e in abrogazione della precedente direttiva 95/46/CE.

Se l'oggetto di analisi principale di questo contributo resta la riforma della direttiva in tema di *network* e *information security* pare opportuno, ancora in sede di introduzione, segnalare che la metodologia di analisi utilizzata, ormai tipica del metodo di insegnamento e ricerca nelle scienze sociali all'incontro con le scienze giuridiche e l'informatica giuridica, tenterà di muovere oltre le previsioni del diritto formale (approccio che si ritiene tanto più utile in questa sede e in queste circostanze in considerazione della recentissima approvazione del testo normativo oggetto di indagine sino al suo effettivo recepimento nei diversi Stati membri). Inoltre, considerando il contenuto altamente innovativo della disciplina[3] e, più in generale, del contesto cui essa si riferisce, il formalismo giuridico sembra un approccio decisamente inadeguato a descrivere la portata autentica di tale riforma anche in relazione alle sue potenzialità applicative, ad oggi, passibili solo di un'opera di meta-previsione.

Tale inadeguatezza, cioè a dire quella per cui per conoscere e interpretare il diritto sarebbe sufficiente conoscere il dato normativo puro è per parte della dottrina riconducibile a quell'approccio che alcune e alcuni esponenti rilevanti delle scienze giuridiche hanno ricondotto all'etichetta di giuspositivismo "ingenuo". Ciò, in particolare, anche nel rivolgersi a operatori di settori specialistici legati alla *cybersecurity* quali, certamente, quelle professioni e professionalità – in parte ancora in via di definizione – che, sempre più, si troveranno ad avere a che fare con le complessità che discendono dall'incontro tra scienze giuridiche e scienze informatiche. Nel guardare a questi operatori del diritto "tra le discipline" non possono dimenticarsi anche le professionalità afferenti all'Ufficio per il processo (UPP) istituto innovativo che ha attratto interessi di approfondimento e ricerca anche a fronte delle recenti riforme introdotte con d.lgs. 10 ottobre 2022, n. 151[4]. Resta allora fondamentale proporre un'alternativa al diritto formale quale oggetto prevalente di studio e di formazione e (con)ricerca, guardando alla più recente esperienza della didattica giuridica[5]. Per quanto la proposta

[3] «Quello che è venuta profilandosi è una vera e propria esplosione di *parole nuove – e-Health, data privacy, autonomous driving, net neutrality, critical data studies, neurodiritto, blockchain, smart contract, cyberwarfare* […]. L'esperienza giuridica è infatti oggi pervasivamente attraversata e connotata dalle tecnologie informatiche» in V. MARZOCCO, S. ZULLO, T. CASADEI, *La didattica del diritto. Metodi, strumenti e prospettive*, Pisa, 2021[2], p. 159. Sullo stesso tema e per un più ampio approfondimento si rinvia anche all'opera collettanea T. CASADEI, S. PIETROPAOLI, (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, 2021.

[4] «Norme sull'ufficio per il processo in attuazione della legge 26 novembre 2021, n. 206, e della legge 27 settembre 2021, n. 134».

[5] Su questo tema mi permetto di segnalare un mio recente contributo che si concentra sulla tematica dell'(in)attualità della didassi giuridica e della didattica del diritto come insegnamento autonomo guardando all'educazione e alla cultura giuridica e regolativa nazionale ed europea. Si veda M. BUFFA, *Didattica del diritto e cultura giuridica nell'educazione (in)attuale. Note a margine di un recente manuale*, in *Materiali per una storia della cultura giuridica*, 1, 2022.

di tale modello "altro" sembri e suoni, in qualche misura, come innovativa, l'identità del diritto vivente come alternativa a quella del diritto formale come oggetto di studio e insegnamento (che ha avuto un ruolo fondamentale nella diffusione di metodologie didattiche clinico-legali) è, in realtà, piuttosto risalente. Tra i movimenti e le "scuole" di pensiero cui è necessario fare riferimento figura, innanzitutto, il realismo giuridico americano, particolarmente influente nella nascita della *clinical legal education*, con un'origine del tutto particolare, ben riassunta nelle parole di Giovanni Tarello: «Negli anni attorno al 1930, un gruppo di giuristi americani particolarmente occupati a sottoporre sia dottrine sia norme tradizionalmente accettate (o di cui si supponeva l'accettazione da parte dei tradizionalisti) ad una critica dal punto di vista del loro realismo (cioè della loro capacità descrittiva) si dissero "realisti" […] ed ecco che, per gradi insensibili, quella che era una semplice locuzione del linguaggio ordinario venne ad assumere il valore di una designazione tecnica per indicare non solo lo svolgimento di motivi critici nei confronti di ideologie tradizionali (anche nel caso in cui tali ideologie erano divenute prescrizioni) ma anche il criterio in base al quale quelle critiche venivano svolte»[6].

Il realismo guarda al diritto e ai diritti come a una macchina, come a un processo, all'insieme di meccanismi e procedure che possiamo comprendere solo quando sono in movimento. Solo così sarebbe possibile coglierne funzioni, efficienza, necessità di nuove direzioni. Il diritto, guardato e trattato come un organismo vivente, riacquista un connotato dinamico e, soprattutto, in parte imprevedibile. Questo continuo rapporto con il soggetto di diritto e l'esercizio – meglio se consapevole – della cittadinanza (nazionale ed europea, aspetto ormai centrale anche non riguardo al tema della *cyber* sicurezza) si pone certamente come uno spunto adeguato ad approfondimenti didattici rispetto alle funzioni del diritto e, soprattutto, alle sue pratiche.

Innegabile, in conclusione di questo paragrafo introduttivo, sembra a chi scrive la necessità di guardare, con Ehrlich, ad una prospettiva altamente anti-formalista, che consenta di dare nuova e più importante rappresentazione al diritto vivente, per concedere spazio al «moderno documento giuridico» e, soprattutto, alle consuetudini e agli usi di tutti i gruppi sociali. Con ciò diviene, inoltre, possibile immaginare nuove forme clinico-legali di insegnamento del diritto che, sull'esempio del

[6] G. TARELLO, *Il realismo giuridico americano*, Milano, 1962, p. 3. Per una più ampia disamina di queste origini mi permetto di segnalare il volume curato da I. FANLO CORTÉS, D. FERRARI, *I soggetti vulnerabili nei processi migratori, la protezione internazionale tra teoria e prassi*, Torino, 2020, che ospita tra gli altri un mio contributo dedicato all'esperienza delle cliniche legali nell'insegnamento del diritto (vivente) all'incontro con vulnerabilità e soggetti vulnerabili.

realismo giuridico americano, ma anche di autorevoli esponenti italiani, come Carnelutti, guardino alle scienze mediche come possibile modello per una formazione connotata, oltreché dal superamento del formalismo, dall'interdisciplinarità, al perseguimento di obiettivi di giustizia sociale. Tratti resi possibili dall'incontro con umane e umani, per "toccare" il diritto vivente, e il suo effetto sulle vite delle conosciate e dei consociati, anche e soprattutto nel loro incontro con l'era digitale. Se l'attenzione agli «usi di tutti i gruppi sociali» *à la* Ehrlich, per altro verso, sembra adattarsi in modo perfetto alle fasi di consultazione europea che hanno preceduto la redazione della disciplina NIS II, ciò sembra ancora più importante ai fini della definizione del contesto. Rispetto a quest'ultimo non potranno trascurarsi gli usi non solo dei gruppi che il diritto riconosce (infrastrutture critiche e soggetti definiti, cittadine e cittadini dell'Unione) ma sarà necessario guardare anche agli usi dei gruppi che il diritto trascura (anche a titolo di *soft law*, da un lato, e oltre i confini dell'Unione[7], dall'altro) e, persino, condanna, nel definire minacce, vulnerabilità[8], soggetti perpetratori di attacchi informatici nella costruzione di nuovi criteri per identificare la condotta deviante e, forse, spunti per elaborare una nuova sociologia giuridico-informatica della devianza.

2. Contesto: (inter)connessioni vulnerabili

La proposta di revisione della normativa europea in materia di *network* e *information security* arriva, a ben vedere, già a conclusione del 2020. Diverse analisi di contesto hanno inciso sulla necessità di ripensare le strategie europee (e nazionali) in tema di sicurezza informativa e di rete guardando ad una strutturazione a tre pilastri: *a) coordination*; *b) awareness*; *c) partnership public-private*. Tale struttura mi sembra già indicativa di lacune significative riscontrate nel breve

[7] Tale circostanza porta con sé, secondo alcuni autori, alcune possibili derive problematiche, come osservato da E. Maestri che, guardando alle relazioni tra attori azioni e diritto in via orizzontale e animate secondo logiche "dal basso", descrive il mondo in rete come caratterizzato da una lotta per il dominio in cui le tematiche affrontate in tema di *network* e *information security* sembrano centrali. E. MAESTRI, *Lex informatica e soft law. Le architetture normative del cyberspazio*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, cit., p. 157 e ss. Ricordo, inoltre, anche quanto la sicurezza informatica abbia dato luogo a interessanti riflessioni in tema di sorveglianza panoptica o, se si vuole, sinoptica, come nella restituzione di E. MAESTRI, *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*, Napoli, 2015, dove nel capitolo quarto si propone un passaggio «dal Panopticon al Synopticon». Si veda, infine, E. ORRÙ, *Verso un nuovo Panottico? La sorveglianza digitale*, in T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, 2021, p. 203 e ss.

[8] Per una mappatura dei rischi possibili, anche in tema di nuove vulnerabilità, nel contesto delle nuove tecnologie all'incontro con il diritto antidiscriminatorio di matrice europea rinvio a S. VANTIN, *Il diritto antidiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*, Milano, 2021.

periodo che va dall'entrata in vigore della direttiva NIS I (a partire dal recepimento nei diversi Stati membri) sino ai primordi della crisi pandemica e sindemica da Covid-19. In effetti, manchevoli sarebbero risultati proprio gli aspetti relativi al coordinamento, alla consapevolezza, alla necessità di "alleanze" tra il settore pubblico e quello privato nella gestione della sicurezza e della rete, guardando ai sempre più crescenti e nuovi aspetti di vulnerabilità e alle corrispettive nuove forme di minaccia che ne sono discese. I fattori determinanti della necessità di una revisione della normativa possono sintetizzarsi come di seguito:

1) Crescenti attacchi informatici (in particolare l'attacco all'*European Medicines Agency* con esposizione di dati sensibili sul vaccino prodotto dalla BioNTech-Pfizer);

2) Nuove sfide per il mercato interno dell'UE dettate dalla crescente digitalizzazione (*e-commerce*, *cashless payments*, *IoT*: si prevendono 22.3 miliardi di dispositivi IoT[9] in uso in UE nel 2024);

3) Ruolo sempre più importante e da attenzionare della *supply chain* (con conseguenti ricadute di rilevanza anche per le piccole e medie imprese);

4) Consapevolezza della necessità di armonizzazione di requisiti, controlli, sanzioni sui territori e negli ordinamenti degli Stati membri;

5) Nuova tecnologia 5G e nuove sfide per il mercato e gli operatori che vi operano;

6) Crisi pandemica per la diffusione del virus Covid-19;

7) Conflitto tra Russia e Ucraina, con il sempre maggiore "coinvolgimento" dell'UE nell'assetto geopolitico mondiale in relazione al posizionamento anche rispetto alla *cyberwarfare*[10].

---

[9] Per un approfondimento nella relazione tra internet delle cose e *data security*, nel contesto di una sempre maggiore perdita del potere di controllo dei dati e la nascita di nuove vulnerabilità anche in relazione alle problematiche relative all'effettività del consenso degli utenti si veda il contributo di A.C. ZANUZZI, *Internet of things e privacy. Sicurezza e autodeterminazione informative*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 99 ss.

[10] «Negli ultimi anni il fenomeno dei c.d. cyberattacchi (o attacchi cibernetici, o attacchi informatici) è rapidamente cresciuto di importanza, fino ad essere percepito come una delle principali minacce alla sicurezza degli Stati e della Comunità internazionale. Il fenomeno travalica i confini dei conflitti armati, nei quali pure il cyberspazio costituisce sempre più un ulteriore terreno (virtuale) di scontro, e per la sua frequenza appare ormai come una costante fisiologica delle vicende internazionali». In queste righe, oltre ad un approfondimento legato agli attacchi informatici e alla guerra cibernetica, interessante sembra il riferimento ai *non stative agents* nella perpetrazione di tali minacce, che l'autore riconduce a S. J. SHACKELFORD e R. B. ANDRES nel contributo *State responsibility for cyber attacks: competing standards for a growing problem*, pubblicato nel *Georgetown journal of International Law* nel 2011, a riprova della sempre maggiore rilevanza di questo tema non solo per le scienze informatiche, ma per le scienze giuridiche internazionalistiche e alle intersezioni disciplinari con le prime. Si veda M. FERRUGLIO, *Cyber operation e responsabilità internazionale degli stati: uno sguardo d'insieme*, in P. IVALDI, S. CARREA (a cura di), *Lo spazio cibernetico. Rapporti giuridici pubblici e privati nella dimensione nazionale e transfrontaliera*, Genova, 2018, pp. 91-93. Sul rapporto tra sicurezza informatica, *cybercrime* e *cyberwarfare* si veda anche l'ultimo capitolo del lavoro monografico di

Se guardiamo agli anni immediatamente successivi alla pubblicazione della direttiva NIS I non possiamo non renderci conto di una evoluzione preoccupante del quadro della sicurezza informatica, con la conseguente nascita di nuove vulnerabilità, minacce e la corrispettiva necessità di misure per farvi fronte sia nel contesto della tutela dei diritti delle persone fisiche che per quanto attiene le persone giuridiche.

Nel 2017 diverse indagini relative alla sicurezza informatica concordavano nel sostenere e prevedere che in Europa le imprese avrebbero sofferto, nel 2021, di un attacco ogni 11 secondi (era un attacco ogni 40 nel 2016).

È, peraltro, pacifico che l'aumento esponenziale degli attacchi al settore bancario e finanziario rendono sempre più vulnerabili ed esposte/i ad attacchi di sorta non solo gli istituti di credito e gli enti finanziari, ma in via sempre più diretta anche cittadini/e dell'Unione, spesso *target* di frodi informatiche attraverso differenti tecniche (quali, a mero titolo esemplificativo, il *phishing* attraverso mezzi informatici e di telecomunicazione). Le infrastrutture critiche[11] si sono rivelate *target* preferenziale, con aggravamento dovuto ai sistemi interconnessi[12] (caratteristica divenuta palese, in modo particolare, a partire dalla pandemia, ma di fatto già sistemica prima delle minacce epidemiologiche che hanno interessato l'ultimo triennio, cui è necessario però riconoscere il "merito" di aver reso innegabili alcune dipendenze funzionali). In passato Rinaldi, Peerenboom e Kelly[13], hanno descritto queste interdipendenze sulla base di diverse dimensioni possibili. Non meno importante è anche l'analisi che riguarda il tipo di guasto e le interdipendenze tra le infrastrutture che possono costituire il mezzo attraverso il quale un danno può propagarsi.

W. D'AVANZO, *Il diritto di fronte alle sfide del futuro. Studi di informatica giuridica e dritto dell'informatica*, Mantova, 2020, pp. 245 e ss. Ancora, per una mappatura legata anche alla definizione del perimetro nazionale di sicurezza cibernetica, S. ATERNO, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pisa, 2022, pp. 207 ss.

[11] L'individuazione di una definizione univoca di infrastruttura critica è un'operazione non semplice e, pertanto, ne deriva una categoria ancora "aperta" e, in qualche misura flessibile. Nel rapporto di ricerca *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici* il prof. R. Setola afferma che: «Di per sé ognuna delle infrastrutture critiche è un sistema complesso (*complex network*) distribuito geograficamente, caratterizzato da un comportamento dinamico fortemente non lineare (ovvero che in situazioni particolari, anche piccoli eventi che in condizioni nominali sarebbero assorbiti senza conseguenze palesi, possono provocare una forte alterazione nelle funzionalità del sistema) e che interagisce sia con le altre infrastrutture critiche sia con diversi soggetti: gestori, utenti, ecc. Per molte di queste infrastrutture non esiste nessuna singola entità che abbia il completo controllo o anche solo la completa conoscenza del sistema, né esiste alcuna entità in grado di monitorare globalmente il sistema, né di gestirlo in modo centralizzato». Si veda R. SETOLA, *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*, Rapporto di ricerca 2011, Centro Militare di Studi Strategici, pp. 10 ss.

[12] Si analizzeranno nel prosieguo di questo contributo alcune possibili letture di tale caratteristica delle infrastrutture critiche e strategiche.

[13] S.M. RINALDI, J.P. PEERENBOOM, T.K. KELLY, *Identifying understanding and analyzing critical infrastructures interdependencies*, in *IEEE Control Systems Magazine*, I, 2002, pp. 12 ss.

Se certamente interessante resta il contributo della prima formulazione della direttiva NIS del 2016 nella distinzione tra settori critici e fornitori di servizi essenziali in ragione della criticità che li contraddistingue, oltre alla direttiva NIS II qui in esame, la Commissione Europea ha adottato di recente un nuovo progetto di iniziativa legislativa (volto all'adozione di una nuova direttiva in tema di infrastrutture critiche[14]) Alle opportunità legate alle tecnologie digitali sono corrisposte, pertanto, nuove esposizioni economiche e sociali a minacce *cyber*, con ripercussioni rilevanti su cittadine/i e alti costi economici e sociali in termini di impatto, rendendo così possibile il passaggio dalla c. d. *Business impact assessment* (BIA) alla c. d. *citizen impact asssessment* (CIA).

L'ENISA[15] ha monitorato ed evidenziato la sempre maggiore sofisticazione, circoscrizione ed estensione degli attacchi informatici. Verizon ha stabilito che l'86% delle violazioni nel 2019 erano motivate da ragioni economico-finanziare e solo il 10% circa per spionaggio (45% *hacking*, 17 % *malware*, 22% *phishing*).

Un tema che, pertanto, sembra essere necessario affrontare nel contesto che ha determinato la necessità di una revisione della disciplina NIS è altresì, senza dubbio, quello della resilienza, intesa etimologicamente, da *resilio*, come la capacità delle imbarcazioni di sapersi capovolgere dopo un evento di naufragio, risalire, in senso figurato, per tornare allo *status quo ante* e garantire la continuità operativa[16].

Diversi indici di resilienza nell'ambito della *cybersecurity* delle persone giuridiche tra gli Stati membri hanno avuto ricadute su cittadine/i dell'Unione, anche guardando alla già evocata disciplina del trattamento dei dati delle persone fisiche come da GDPR. Non sono state assenti dissonanze e mancate uniformità tra le legislazioni degli Stati membri anche rispetto ai settori identificati

[14] Come si legge nella pagina dedicata (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Nuove-norme-sulla-protezione-delle-infrastrutture-critiche-nellUE_it) «Per "infrastruttura critica" si intende qualunque sistema essenziale per il mantenimento delle funzioni cruciali della società e dell'economia: la sanità, l'alimentazione, la sicurezza, i trasporti, l'energia, i sistemi informatici, i servizi finanziari, ecc. L'iniziativa mira a proteggere meglio questi sistemi dalle catastrofi naturali e dalle minacce di origine antropica (come il terrorismo, gli attacchi informatici, la disinformazione, la scalata ostile da parte di soggetti stranieri). Terrà conto dei seguenti aspetti: i crescenti collegamenti tra i settori; le nuove minacce (ad esempio cambiamenti climatici e pandemie)».

[15] *European Union Agency for Cybersecurity*, Agenzia dell'Unione Europea per la Cybersicurezza. Si tratta dell'agenzia dell'Unione dedicata al conseguimento di un elevato livello comune di *cybersecurity* in tutta Europa.

[16] Rispetto a quest'ultima prospettiva, AGID, Agenzia per l'Italia Digitale che fa capo alla Presidenza del Consiglio dei ministri, ricorda che «Esistono standard internazionali che fanno riferimento alla continuità operativa. È di particolare rilevanza lo standard UNI CEI ISO/IEC 27001:2014 "Tecnologia delle informazioni - Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni - Requisiti" che, pur trattando della sicurezza informatica, identifica nella continuità operativa un elemento essenziale».

e identificabili – a proposito di usi dei gruppi sociali – come OSE (operatori servizi essenziali) e FSD (fornitori di servizi digitali) dando così vita a disparità e potenziale *forum shopping*[17].

Il quadro ha visto poi l'intervento di alcune complicazioni a partire dalla difficoltà dovuta alla assenza di un coordinamento effettivo e di una capacità di dare risposta comune (anche tra gli Stati Membri) nella gestione, segnalazione degli incidenti e nella *business continuity* tra infrastrutture critiche collegate.

Per l'insieme di queste ultime criticità, evocate dalle testimonianze condivise nelle consultazioni condotte dalla Commissione europea e dalle altre istituzioni e agenzie dell'Unione, la direttiva NIS II mira a eliminare le divergenze, anche in potenza, con l'obiettivo principale di un maggiore e migliore coordinamento, anche ai fini di una più efficiente cooperazione tra le autorità nazionali degli Stati membri, per l'aggiornamento della disciplina in tema di *cybersecurity*, al fine di garantire l'effettività del diritto dell'Unione europea e l'uniformità delle legislazioni nazionali in tema di soggetti rilevanti e destinatari della normativa, mezzi di tutela giurisdizionale e sanzioni.

3. Soggetti essenziali e importanti: tra *cybersecurity* e *cyber reselience*

L'approccio del diritto vivente, con attenzione ai contenuti "minimi" che lo abitano in termini di giurisprudenza, dottrina e prassi amministrative, chiede di guardare anche agli usi dei gruppi sociali e dei soggetti che abitano l'ordinamento. A partire proprio da tale presupposto, all'intersezione con le eterogenee definizioni e funzioni delle infrastrutture critiche, la direttiva NIS II innova il piano dei soggetti destinatari della nuova disciplina per rendere uniformi gli ordinamenti (e, a seguire, gli usi) dei diversi Stati membri. Se NIS I distingue tra OSE come Operatori di Servizi Essenziali e FSD come Fornitori di Servizi Digitali, NIS II, invece, supera la distinzione tra queste entità proponendo le categorie di soggetti essenziali («settori ad alta criticità») e soggetti importanti

[17] «Secondo la giurisprudenza della Corte di giustizia l'abuso del diritto consiste nel ricorso ad una facoltà prevista dalla legge per uno scopo diverso da quello voluto dal legislatore con l'intenzione di trarne vantaggio. La Corte ha ritenuto che sussista l'abuso del diritto quando sono presenti un elemento oggettivo, rappresentato dal fatto che, nonostante il formale rispetto delle norme comunitarie, non viene raggiunto lo scopo per cui queste norme sono state emanate, ed un elemento soggettivo, costituito dall'intenzione di trarre vantaggio dalla disciplina dell'Unione creando artificialmente le condizioni per la loro applicazione. Nella sentenza *Kofoed* la Corte ha fatto espressamente riferimento al divieto di abuso del diritto come ad un principio generale del diritto dell'Unione, si può affermare pertanto che tale principio valga anche con riguardo alla materia disciplinata dal regolamento (CE) n. 1346/2000 e dal regolamento (UE) 2015/848». L. PANZANI, *Forum shopping e abuso del diritto*, in *Il nuovo diritto delle società*, X, 2017, pp. 1231 ss.

(«altri soggetti critici»). La distinzione non è solo formale e relativa alla denominazione in uso anche in considerazione di un interessante cambio di prospettiva. I soggetti essenziali e importanti, infatti, non saranno più individuati su indicazione delle competenti autorità nazionali in base all'incontro di criteri di soglia, ma sulla base dell'identità dei settori "rilevanti" definiti negli allegati della riforma con esclusione, come meglio si specificherà *infra*, delle piccole e medie imprese (PMI) ancorché potenzialmente chiamate in causa dalla *supply chain*. Da ciò deriverà un ampliamento quantitativo e qualitativo importante dei soggetti (essenziali e importanti) chiamati a nuovi adempimenti, con interessanti ricadute anche dal punto di vista del mercato interno.

In effetti, sono da considerare, tra gli altri, soggetti essenziali il settore bancario e finanziario, quello delle infrastrutture e dei trasporti, la P.A. l'energia, la salute[18]. Rientrano invece nella definizione di soggetti importanti il settore alimentare, quello della gestione dei servizi pubblici quali quelli dei servizi postali, la gestione dei rifiuti che, come i settori seguenti, hanno avuto un'importanza crescente a partire dall'epidemia Covid-19, quali il settore dell'industria chimica e farmaceutica[19].

Proprio la prospettiva anti-formalista consente di osservare gli effetti che muovono oltre la definizione legislativa:

- In particolare, la OPC (*open public consultation*) che ha preceduto la redazione della norma in termini di proposta a seguito della posizione del Parlamento europeo (risoluzione 12 marzo 2019) e le conclusioni del Consiglio del 20 ottobre 2020, ha coinvolto i ventisette Stati membri per evidenziare inconsistenze nella applicazione della norma nella identificazione di OSE e FSE ha evidenziato incoerenze non solo formali, ma sostanziali, nell'applicazione della norma, nei rapporti tra gli ordinamenti, anche in relazione al mercato interno.

- Più specificamente rispetto a tali dissonanze, un soggetto poteva essere identificato come OSE in uno SM, ma come FSE in un altro, o ancora come *service provider*, venendo così escluso dall'ambito di applicazione della direttiva NIS in uno stato membro ancora diverso. Tali disparità

[18] Nello specifico, la direttiva e il suo allegato I si riferiscono ad energia (elettrica, tele-riscaldamento, raffreddamento, petrolio, gas); trasporti (idrogeno, areo, ferroviario, su acqua, su strada); settore bancario; infrastrutture dei mercati finanziari; settore sanitario, acqua potabile; acque reflue; infrastrutture digitali; gestione dei servizi TIC; pubblica amministrazione, spazio.

[19] Qui, come da allegato II, la direttiva individua, in sintesi servizi postali e di corriere; gestione dei rifiuti; fabbricazione, produzione e distribuzione di sostanze chimiche; produzione, trasformazione e distribuzione di alimenti; settore della fabbricazione (dispositivi medici e medico diagnostici *in vitro*, computer prodotti di elettronica e ottica, apparecchiature elettriche, autoveicoli rimorchi e semirimorchi, altri mezzi di trasporto); fornitori di servizi digitali (mercati *online*, motori di ricerca online, *social networks*) e ricerca, riferendosi in modo aperto a «organizzazioni di ricerca».

di trattamento, in disparte la necessità di un'applicazione uniforme del diritto europeo, sempre auspicabile, mostravano possibili scenari capaci di rendere le entità ancora più vulnerabili ad attacchi e minacce *cyber* transnazionali.

Come si è avuto modo di mettere in luce, in sede di analisi dell'implementazione della disciplina della direttiva NIS I sono emerse significative disparità anche nel novero quantitativo di istituzioni individuate tra gli OSE. La misura in commento, per altro fronte, dovrebbe apportare vantaggi significativi: le stime indicano che la riforma potrebbe portare a una riduzione fino a 11,3 miliardi di euro dei costi degli incidenti di *cyber* sicurezza. L'ambito di applicazione settoriale sarebbe notevolmente ampliato nel quadro della NIS. Ciò si deve al fatto che il nuovo quadro NIS II definisce un approccio a due livelli, incentrato su soggetti chiave e di grandi dimensioni e su una differenziazione del regime di vigilanza che consenta la supervisione solo *ex post* per un ampio numero di tali soggetti, in particolare quelli considerati importanti, ma non essenziali.

È, inoltre, almeno probabile che la direttiva avrà un impatto positivo nel garantire un avvicinamento di condizioni tra gli Stati membri di tutti i soggetti rientranti nell'ambito di applicazione della direttiva riducendo le asimmetrie inerenti alle informazioni sulla *cybersecurity* e con riguardo ai soggetti coinvolti, seppure una fonte regolamentare di diritto secondario avrebbe migliorato con maggiore certezza l'attuale piano di dissonanze tra gli ordinamenti e le conseguenze che ne sono discese.

4. Struttura e sintesi della riforma tra quadri, cooperazione, condivisione, gestione e segnalazione

Possiamo ritenere la direttiva NIS II come fondata su tre assi principali che riguardano le innovazioni apportate alla sicurezza delle reti e informazioni: un primo asse dedicato all'ambito di applicazione e ai soggetti destinatari che si è prima analizzato, un secondo asse dedicato alle misure, un terzo e ultimo asse dedicato alle notifiche, che comprende l'identificazione dei soggetti obbligati, delle autorità destinatarie delle segnalazioni, i termini di notifica. In seguito, si analizzerà la struttura della riforma guardando agli elementi trasversali a tali assi.

Nel contesto della direttiva gli Stati membri sono tenuti, innanzitutto, ad adottare una strategia nazionale per la *cyber* sicurezza che definisca gli obiettivi strategici e le misure politico-normative appropriate volte a raggiungere e mantenere un livello elevato di tutela. La fonte stabilisce, inoltre, un "quadro" per la divulgazione coordinata delle vulnerabilità e impone agli Stati membri

di designare CSIRT che agiscano da intermediari fidati e facilitino l'interazione tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti e servizi TIC. L'ENISA è tenuta a istituire e mantenere un registro europeo delle vulnerabilità che guarderà a quanto individuato e comunicato nei diversi ordinamenti nazionali. Gli Stati membri sono chiamati a mettere in atto tali quadri nazionali di gestione delle crisi di *cyber* sicurezza, tra l'altro designando le autorità nazionali competenti responsabili della gestione di incidenti e crisi su vasta scala. Gli ordinamenti nazionali sono, inoltre, tenuti a designare una o più autorità nazionali competenti in materia di *cyber* sicurezza per i compiti di vigilanza previsti dalla presente direttiva e un punto di contatto unico nazionale in materia (SPOC: *Single Point of Contact*) che eserciti una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri e a designare i CSIRT (*Computer Security Incident Response Team*).

Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri, sviluppare fiducia e scambio di buone pratiche, la direttiva istituisce un gruppo di cooperazione, nonché una rete di contatto tra CSIRT, allo scopo di contribuire allo sviluppo di una condivisione attiva e trasparente di informazioni. Tali misure sono intese a promuovere, primariamente, una cooperazione operativa, rapida ed efficace tra i diversi soggetti coinvolti. È a questo fine che si propone l'istituzione di una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) per sostenere la gestione coordinata di incidenti e crisi di *cyber*-sicurezza su vasta scala e garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'UE, a riconferma di quanto tale dimensione sia ormai strategica e irrinunciabile nelle politiche sovranazionali. L'ENISA resta soggetto fondamentale e, in questo quadro cooperativo, sarà tenuta a presentare, in collaborazione con la Commissione, una relazione annuale sullo stato della *cybersecurity* dell'Unione. A questo fine la Commissione è chiamata a istituire un sistema di revisione tra pari che consenta di effettuare revisioni periodiche dell'efficacia delle politiche di *cyber* sicurezza adottate dagli Stati membri. La direttiva impone agli Stati membri di prevedere che gli organi di gestione di tutti i soggetti che rientrano nell'ambito di applicazione della norma, quali soggetti e, conseguentemente, settori essenziali e importanti per l'Unione, approvino misure di gestione dei rischi di *cybersecurity* e, a riprova della necessità di un approccio condiviso e innovativo in tema di formazione, seguano un *training* specifico in materia.

Gli Stati membri, pertanto, saranno tenuti a garantire che i soggetti che rientrano nell'ambito di applicazione della disciplina adottino misure tecniche e organizzative adeguate e proporzionate

per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete, in applicazione dei principi di adeguatezza e proporzionalità che, insieme a quello di sussidiarietà, restano principi fondamentali e ispiratori del diritto dell'Unione europea anche in questo settore. Sugli Stati graverà anche l'obbligo di garantire che i soggetti notifichino alle autorità nazionali competenti, o ai CSIRT, qualsiasi incidente di *cyber* sicurezza che abbia un impatto significativo[20] sulla fornitura dei loro servizi.

Di norma, i soggetti essenziali e importanti saranno da ritenersi come sottoposti alla giurisdizione dello Stato membro in cui prestano i propri servizi. Tuttavia, alcuni tipi di soggetti (quali, a titolo esemplificativo, i fornitori di servizi DNS, i gestori di registri dei nomi di dominio di primo livello, ancora i fornitori di servizi di *cloud computing*[21], i fornitori di servizi di *data center* e fornitori di reti di distribuzione dei contenuti, nonché alcuni fornitori di servizi digitali) saranno sottoposti alla giurisdizione dello Stato membro in cui sono principalmente stabiliti nell'Unione. In questo modo, in effetti, si garantisce che tali soggetti non si confrontino con una miriade di prescrizioni giuridiche eterogenee nella fornitura di servizi transfrontalieri a un livello particolarmente elevato. L'ENISA, a questo scopo, è chiamata dalla direttiva a creare e mantenere un registro dei soggetti che rientrino in questa particolare categoria. Le autorità competenti saranno tenute a esercitare la vigilanza sui soggetti che rientrano nell'ambito di applicazione della direttiva e, in particolare, a garantirne la conformità ai requisiti di sicurezza (tramite l'applicazione delle misure) e di notifica degli incidenti nonché ad un sistema di sanzioni.

La direttiva distingue, opportunamente, tra un regime di vigilanza *ex ante* per i soggetti essenziali e un regime di vigilanza *ex post* per i soggetti importanti. Quest'ultimo impone alle autorità competenti di adottare provvedimenti qualora esse ricevano elementi di prova o indicazioni[22] che un soggetto importante non soddisfa i requisiti di sicurezza e di segnalazione degli incidenti. La direttiva obbligherà, inoltre, gli Stati membri a imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti, definendo alcuni importi massimi in caso di inadempimenti[23]. A

[20] Si vedrà *infra* l'ampliamento di questa definizione aperta secondo criteri concorrenti.

[21] Si rinvia per un approfondimento alle questioni emergenti in tema di *cloud computing* all'incontro con la filosofia del diritto al contributo di P. SOMMAGIO, *Dalla scrivania alla nuvola e ritorno. Riflessioni filosofico-giuridiche sul cloud computing*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, cit., p. 179.

[22] In considerazione della grande apertura delle espressioni in uso, in termini di «elementi di prova e indicazioni» quale presupposto sufficiente all'adozione di provvedimenti da parte delle autorità competenti, si intuisce che la previsione di un regime di vigilanza e controllo *ex post* non è da intendersi come privo di una finalità preventiva "nell'azione" del suo dispiegamento confermando, inoltre, la rilevanza attribuita a tali soggetti nel contesto della *cybersecurity*.

[23] «Gli Stati membri provvedono affinché le violazioni degli obblighi […] siano soggette a sanzioni pecuniarie amministrative pari a un massimo di almeno 10.000.000 EUR o fino al 2% del totale del fatturato mondiale annuo

partire da tali previsioni a chiusura del sistema di vigilanza e monitoraggio, considerando tra l'altro la severità del quadro sanzionatorio, è possibile prevedere che gli Stati membri e i soggetti coinvolti saranno decisamente incentivati a cooperare e ad assistersi reciprocamente quando prestino servizi in più di uno Stato membro o quando lo stabilimento principale di un soggetto, ovvero il suo rappresentante, si trovi in un determinato Stato membro, ma i suoi sistemi informatici e di rete siano situati in uno o più altri Stati membri.

5. Incidente significativo

Aspetto interessante e trasversale alla riforma introdotta dalla direttiva NIS II è la nuova formulazione della nozione di «incidente significativo». Rilevante sembra, in questa sede, un richiamo alla lettera della norma che, all'art. 23, dispone che: «Un incidente è considerato significativo se:

a) ha causato o può causare una perturbazione operativa o perdite finanziarie sostanziali per il soggetto interessato;

b) si è ripercosso o può ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli».

Le condizioni di cui alle lettere a e b sembrerebbero dover coesistere per sostanziare questa categoria giuridica interpretativa innovativa che, per altro, in estensione rispetto a quanto previamente previsto dalla direttiva NIS I, si fonda su un'ottica preventiva di tutela nel guardare a situazioni potenziali di perturbazioni operative, perdite finanziarie sostanziali e, ancora, a ripercussioni su persone fisiche o giuridiche da cui possano discendere danni materiali o immateriali considerevoli. Si noti, però, che ciascuna di queste circostanze che riguardano il piano delle conseguenze degli incidenti, e non la sua eziologia, sembrano potenzialmente suscettibili di difformità interpretative e applicative nel diritto vivente. In particolare, oltre alla giurisprudenza e alla dottrina, ad avviso di chi scrive, rivestiranno importanza fondamentale le prassi applicative volte a stabilire la verificazione concorrente delle due ipotesi di cui alle lettere *a)* e *b)*, nonché il recepimento di tali condizioni nei diversi contesti nazionali entro i ventuno mesi a disposizione.

---

per l'esercizio precedente dell'impresa cui il soggetto essenziale o importante appartiene, se tale importo è superiore» *ex* art. 34, comma 4, direttiva NIS II per quanto attiene le sanzioni applicabili ai soggetti essenziali e importanti. Si noti che, nella formulazione approvata, l'articolo seguente non inasprisce le sanzioni applicabili ove gli inadempimenti comportino una violazione dei dati personali.

In presenza di un incidente significativo, nel termine di 24 ore dal ricevimento della notifica iniziale, le autorità nazionali competenti o il CSIRT dovranno fornire una risposta al soggetto notificante, che comprenda un riscontro iniziale sull'incidente e, su richiesta del soggetto, orientamenti sull'attuazione di possibili misure di attenuazione. Se il CSIRT non dovesse ricevere tale notifica, gli orientamenti sopraddetti saranno forniti dall'autorità competente, ma sempre mantenendo ferma la clausola «in collaborazione con il CSIRT».

Sempre su richiesta del soggetto interessato – previsione che a chi scrive pare interessante attribuzione di centralità e responsabilità conseguenti – il CSIRT dovrà fornire «ulteriore supporto tecnico».

A questo punto la riforma entra nell'eziologia della verificazione dell'incidente, prevendendo che qualora si sospetti che l'incidente abbia carattere criminale, le autorità nazionali competenti ovvero, in alternativa, il CSIRT saranno chiamati a fornire anche orientamenti (al soggetto richiedente) sulla segnalazione dell'incidente alle autorità di contrasto. Se opportuno, e in particolare se l'incidente in argomento dovesse interessare due o più Stati membri, l'autorità competente o il CSIRT dovranno informare gli altri Stati membri interessati e l'ENISA. Nel farlo i soggetti incaricati di tali obblighi, in conformità al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, dovranno tutelare la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite[24].

La riforma prevede, ancora, operando un opportuno bilanciamento preventivo, che qualora dovesse rendersi necessario sensibilizzare il pubblico per evitare un incidente o affrontare un incidente in corso, ovvero se la divulgazione dell'incidente corrisponda ad un interesse pubblico, dopo aver consultato il soggetto interessato l'autorità competente o il CSIRT e, se opportuno, le autorità o i CSIRT degli altri Stati membri interessati, sarà possibile informare il pubblico riguardo all'incidente o imporre al soggetto di farlo. Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico inoltrerà le notifiche ricevute ai punti di contatto unici degli altri Stati membri interessati. A fini di monitoraggio e valutazione costante di quanto in argomento il punto di contatto unico vedrà, tra le sue responsabilità, anche quella di trasmettere mensilmente all'ENISA una

[24] In questo senso colpisce la tutela della riservatezza delle informazioni fornite che sembra, però, volta a consentire l'eliminazione di ogni potenziale ostacolo alla più libera e trasparente condivisione delle informazioni rilevanti, pur nella generale e necessaria conformità con il diritto dell'Unione e, più in generale, delle legislazioni nazionali a questo conformi che, nei bilanciamenti possibili, dovranno necessariamente tenere conto del piano dei diritti fondamentali delle cittadine e dei cittadini dell'Unione europea. Nel paragrafo successivo, in effetti, si individuano limiti alla tutela di questa ampia riservatezza sulle informazioni fornite e sulle relative fonti e circostanze.

relazione di sintesi che comprenda dati anonimizzati e aggregati sugli incidenti, sulle minacce informatiche significative e sui quasi incidenti notificati conformemente alle disposizioni. Al fine di contribuire alla fornitura di informazioni e dati comparabili, l'ENISA potrà pubblicare orientamenti tecnici sui parametri delle informazioni incluse nella relazione di sintesi.

Le autorità competenti forniranno alle autorità designate le informazioni sugli incidenti e sulle minacce informatiche notificate conformemente dai soggetti essenziali identificati come soggetti critici o come soggetti equivalenti ai soggetti critici. La Commissione, in ultimo, potrà adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica. Si tratta di una procedura che potrà avere un effetto molto utile nell'avvicinamento delle misure in via di adozione. La Commissione, sempre a titolo di miglioramento continuo delle misure adottande, e in piena conformità al ciclo di Deming *Plan, Do, Check, Act* (PDCA) potrà emanare, altresì, atti di esecuzione al fine di specificare ulteriormente i casi in cui un incidente debba essere considerato significativo.

6. Gli interrogativi aperti

Esaurito l'esame degli aspetti più rilevanti e dell'impianto della direttiva NIS II pare opportuno mettere in luce alcuni interrogativi ancora aperti in relazione agli orizzonti successivi di implementazione. Oltre alla variabile temporale legata al recepimento della riforma in argomento nei ventuno mesi a disposizione per gli Stati membri, un primo interrogativo rilevante riguarda l'applicazione del principio di sussidiarietà in materia di *cybersecurity* e tutela delle infrastrutture critiche. È chiaro, infatti, che la resilienza all'interno dell'Unione non possa essere efficace se affrontata in modo diverso nei vari contesti nazionali o regionali, ma è altrettanto vero che, considerando le caratteristiche molto differenti degli ordinamenti giuridici nazionali degli Stati membri, un margine di discrezionalità, anche in relazione alla forma normativa di direttiva adottata, sembra ineludibile. La direttiva NIS I ha parzialmente ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia, il suo recepimento e la sua attuazione hanno portato alla luce carenze e limiti intrinseci di alcune disposizioni o approcci, come la poco chiara delimitazione del suo ambito di applicazione, che ha determinato differenze significative in termini di portata e intensità dell'intervento effettivo dell'UE nei "perimetri" degli Stati membri. Inoltre, con la crisi pandemica, di recente aggravata da quella energetica, l'economia

europea è diventata dipendente dai sistemi informatici e di rete come mai prima d'ora (così come sempre più vulnerabile alle crisi, interne ed esterne alla politica nazionale ed europea) mentre settori e servizi risultano sempre più interconnessi. L'intervento dell'Unione, guardando ai provvedimenti normativi adottati e addotandi in tema di NIS, può dirsi determinato principalmente da:

i) la natura sempre più transfrontaliera delle minacce e delle sfide legate alla sicurezza delle reti e delle informazioni;

ii) la fiducia negli interventi dell'Unione volti a migliorare e agevolare strategie nazionali efficaci e coordinate;

iii) il contributo degli interventi strategici concertati e collaborativi volti a un'efficace protezione dei dati e della vita privata[25].

La direttiva NIS II sarà quindi in grado di ovviare a tali problemi, nel rispetto del principio di sussidiarietà? Come sarà possibile interpretare gli eventuali obblighi nazionali più stringenti in tale *framework*? Quali gli strumenti per valutare le discipline di recepimento e l'entrata in vigore effettiva, potenzialmente in differita, nei diversi ordinamenti giuridici nazionali? La cooperazione tra i diversi Stati membri sarà effettivamente ispirata a meccanismi di condivisione, trasparenza e solidarietà, con attenzione alla libera concorrenza? I costi per garantire una cooperazione sistematica tra Stati membri saranno effettivamente minimi rispetto alle perdite e ai danni economici e sociali causati dagli incidenti di *cybersecurity*?

Operando una valutazione in potenza in tema di efficienza normativa e semplificazione, per quanto ad oggi possibile all'indomani dell'approvazione della norma e in assenza del suo effettivo recepimento, è possibile affermare e osservare che la proposta di un'esclusione generale di micro e piccoli soggetti dal campo di applicazione della direttiva NIS II vada riletta alla luce del possibile coinvolgimento di questi soggetti nella *supply chain* di soggetti essenziali e importanti. Ancora, si osserva l'adozione un regime di vigilanza *ex post* più "leggero" applicato a un gran numero di nuovi soggetti nell'ambito dell'ambito di applicazione (i cosiddetti soggetti importanti). Tali prescrizioni, pur ancora in attesa di misurarsi con il diritto vivente e, in particolare, con le prassi nazionali e

[25] Ci troviamo nell'ambito dell'azione di riforma europea centrata su tre direttrici riguardanti «(i) la resilienza, la sovranità tecnologica e la leadership europea; (ii) la costruzione e lo sviluppo di capacità operative per prevenire, dissuadere e rispondere ai crescenti attacchi informatici; e (iii) la promozione di un *cyberspazio* globale e aperto. Su questa spinta si è delineato il quadro giuridico all'interno del quale sono state presentate la proposta di revisione della direttiva NIS (NIS 2.0) e la proposta per una direttiva sulla resilienza degli operatori critici di servizi essenziali (CER Directive)». R. BRIGHI, *Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati*, in T. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Padova, 2021, p. 147.

locali, ma anche con l'elaborazione di strategie nazionali in tema di *cybersecurity* cui i diversi Stati membri sono invitati, mirano a ridurre al minimo ed equilibrare gli oneri che gravano sulle imprese e sulle pubbliche amministrazioni.

In tema di piani attuativi e modalità di monitoraggio, valutazione e informazione, la direttiva comprende un piano generale volto a monitorare e valutare l'impatto sugli obiettivi specifici posti, che richiederà alla Commissione di effettuare una revisione almeno 54 mesi dopo la data di entrata in vigore (cioè a quasi due anni dal recepimento da parte degli Stati membri che adempiranno nei termini) per informare poi il Parlamento europeo e il Consiglio sull'esito di tali rilievi. Il riesame, ancorché con termine piuttosto esteso, dovrà essere effettuato in linea con gli orientamenti della Commissione per «legiferare meglio» e, certamente, a seguito di un'altra *open public consultation* come avvenuto per l'elaborazione di NIS II. Tale intersezione sembra la più opportuna per dare spazio di confronto al diritto vivente ai fini del miglioramento continuo della disciplina, in un contesto in costante (e altrettanto imprevedibile) mutamento come quello legato alla *cybersecurity* e alla tutela delle infrastrutture critiche nella complessità delle loro interdipendenze: tra innovazione, (necessità di) formazione e diritto.

MATTEO BUFFA
Università degli Studi di Genova