Volume 13 (2023)
ISSN 2612-6966

OJH

Open Journal of Humanities

Open Journal of Humanities
Electronic Scientific Journal in Open Access
ISSN 2612-6966

Homepage
www.doaj.org/toc/2612-6966

Publisher
Universitas Studiorum S.r.l. - Casa Editrice Scientifica
via Sottoriva, 9 - 46100 Mantova (MN), Italy - www.universitas-studiorum.it

Open Journal of Humanities (OJH) is a peer-reviewed electronic Scientific Journal, which is devoted to the field of Humanities. OJH is published three times a year, and is distributed online with a full Gold Open Access policy, without any embargo period, through a Creative Commons License (CC-by 4.0).
Peer-reviewing process for OJH is operated on a "double blind" basis, for each proposed article; it is conducted by at least two external referees, and is monitored by members of OJH's Scientific Committee and by the Publisher's Editor. Both the reviewers and author identities are concealed from the reviewers, and vice versa, throughout the review process. Received articles are made anonymous by our Editors, before Peer-reviewing process begins. Selection is based only on intellectual and scientific value and content, with no regards to authors' identity, origins, political or religious orientations. Proposed papers must be unpublished and fully original, and OJH Editorial Board will condemn and report any plagiarism or semi-plagiarism case. Every single Author accepts his own full responsability for the originality and paternity of the published text.
Accepted topics of OJH include the whole field of Humanities, and namely: Anthropology, Archaeology, Arts (Visual Arts, Architecture), Classics, Philology, Philosophy, Law and Politics, Linguistics, Literature, Sociology, Economics. Corrispondent scientific classification in Italy covers the following fields (cf. D.M. 855/2015): Area 10 "Scienze dell'antichità, filologico-letterarie e storico-artistiche"; Area 11 "Scienze storiche, filosofiche, pedagogiche, psicologiche"; Area 12 "Scienze giuridiche"; Area 13 "Scienze econo-miche e statistiche"; Area 14 "Scienze politiche e sociali".

Open Journal of Humanities, 13 (2023)
issn 2612-6966

Network Information Security in Europa: la cybersecurity al confronto con il diritto vivente

Matteo Buffa
Università degli Studi di Genova

Abstract
European Union Law proposes important and profound revision of the Directive on network and information security considering the need for a new, and better, standardization of Member States' national law about cybersecurity. Such reform appears to be necessary looking at the last developments of recent years, as well as at the various crisis factors at international level, even in terms of critical infrastructures and their interdependence. The subject of interest looks, fitting between different traditions and regulatory cultures, to innovative perspectives, both in terms of Law and possible educational developments. Legal informatics and living law propose new challenges and comparisons for essential and important subjects, looking at the set of obligations that will be required to them in collaborating and contributing to ensuring a higher level of security inside and outside the borders of Europe.

Keywords: cybersecurity, network information security, European Union, Critical infrastructures protection, legal informatics, didactics of law.

1. *Network Information Security* (NIS) II. Rifusione nel diritto vivente

Come suggerito dal titolo di questo lavoro, 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 Euro-

pea. Il testo normativo mostra 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 Decreto legislativo 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.

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. Essa è in linea con le priorità della Commissione volte a rendere l'Europa pronta ad affrontare l'era digitale e costruire un'economia adatta alle sfide del futuro e che sia idonea a porsi al servizio dei cittadini. La sicurezza cibernetica, inoltre, è una delle priorità nella risposta della Commissione alla crisi dovuta alla diffusione del virus COVID-19. Il pacchetto comprende una nuova strategia per la *cyber*-sicurezza mirata a rafforzare l'autonomia strategica dell'Unione per migliorarne la resilienza e la risposta collettiva e creare una rete Internet globale e aperta. La riforma contiene, infine, una proposta di una direttiva sulla resilienza degli operatori critici di servizi essenziali, che mira a ridurre le minacce fisiche nei confronti degli stessi.

Come noto la forma direttiva[2] è atto e fonte di diritto derivato dell'UE e viene, tipicamente, adottata per consentire il perseguimento e il raggiungimento di obiettivi comuni tra gli Stati Membri dell'ordinamento europeo, lasciando "liberi"[3] gli ordinamenti nazionali rispetto alle forme con cui dare seguito ed applicazione alla disciplina, pur entro un termine determinato. 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 di-

2. Gli atti di diritto secondario – differenti da quelli di diritto primario europeo, cioè a dire i trattati – di cui le istituzioni dell'Unione possono avvalersi nell'esercizio delle loro competenze sono enumerati nell'art. 288 del Trattato sul funzionamento dell'Unione europea (TFUE): regolamenti, direttive, decisioni, raccomandazioni e pareri. Si tratta dei cd. atti tipici in quanto definiti secondo modelli predeterminati nelle fonti di diritto primario. È proprio, in effetti, il diritto primario, ex art. 288 TFUE a distinguere gli atti vincolanti, e quindi suscettibili di costituire fonti formali di norme giuridiche, i regolamenti, le direttive e le decisioni, da quelli che tali non sono, le raccomandazioni e i pareri. Il complesso degli atti vincolanti dà luogo al cd. diritto derivato, formalmente subordinato alle norme primarie contenute nei trattati istitutivi.

3. Secondo la dottrina prevalente, che trova conferma nell'opinione dell'Agenzia dell'Unione Europea per la *cybersecurity*, la direttiva NIS, quale atto di diritto secondario, è stata adottata in tale forma per tenere conto delle circostanze nazionali e, inoltre, per consentire di "riutilizzare" o, comunque, ridefinire le strutture organizzative esistenti o per allinearsi alla legislazione nazionale esistente, eventualmente anche tramite adeguamenti ed emendamenti al diritto già in vigore.

sciplina 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 necessaria considerazione delle ricadute importanti della *cybersecurity* in materia di diritti fondamentali dei cittadini e delle cittadine dell'UE,[4] nonché in relazione alla evidente e sempre maggiore interconnessione tra le infrastrutture critiche dei diversi Stati membri, come si avrà modo di meglio approfondire *infra*.

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 meto-

4. 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.

do 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 appena intervenuta approvazione del testo normativo oggetto di indagine sino al suo effettivo recepimento nei diversi Stati membri). Inoltre, considerando il contenuto altamente innovativo della disciplina[5] 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

5. "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*, ma anche, come si vedrà più in dettaglio di seguito, digital divide – che genera interrogativi radicali, sul piano filosofico, ma che ha anche un preciso impatto sull'operatività di chi si trova a svolgere professioni forensi o occupazioni che con il diritto hanno un legame diretto e inaggirabile (si pensi ai vari comparti della pubblica amministrazione ma anche ai vari mondi del sistema economico e produttivo). Ciò pone inevitabilmente, poi, questioni pratiche e operative anche a chi per funzione ha il compito di insegnare ad insegnare una disciplina come quella giuridica che conosce costantemente nuove forme e configurazioni del suo stesso oggetto. L'esperienza giuridica è infatti oggi pervasivamente attraversata e connotata dalle tecnologie informatiche" in Marzocco, Zullo e Casadei 2021: 159. Sullo stesso tema e per un più ampio approfondimento si rinvia anche all'opera collettanea Casadei e Pietropaoli 2021.

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 decreto legislativo 10 ottobre 2022 n. 151.[6]
L'ambizione del presente contributo vede, inoltre, grazie all'incontro di realtà importanti[7] impegnate nella formazione degli operatori di settore, l'occasione di ripensare all'innova-

6. "Norme sull'ufficio per il processo in attuazione della legge 26 novembre 2021, n. 206, e della legge 27 settembre 2021, n. 134".

7. Quali, oltre all'Università degli Studi di Genova con il Master di II livello *in cyber security and critical infrastractures protection* e il Centro di competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche Start 4.0, lo Studio Legale associato B-RIGHT *Lawyers* di Genova e Sababa security con un percorso di formazione e (e-)*training* che si rivolge alla *cybersecurity* e alle certificazioni, alle misure di sicurezza implementate a partire dal recepimento nazionale della direttiva NIS e, infine, al perimetro nazionale di sicurezza. Tale percorso, – tra gli altri – ha il pregio di unire contenuti tecnico-specialistici fondamentali, anche giuridici, proposti con una formulazione semplice e accessibile grazie ad una visualizzazione efficace garantita dalla piattaforma in cui il corso si svolge e si struttura. È forse proprio la caratteristica e la capacità di allontanarsi dal dato normativo "puro" *à la* Kelsen, insieme all'uso di metodologie didattiche innovative e digitali – pur senza poter prescindere dalla rilevanza della "lettera della norma" – a rendere fruibile a un pubblico vasto ed eterogeno (come è quello impegnato e interessato dalla *cybersecurity*) tale modello formativo.

zione formativa rivolta al mondo delle professioni legali, ingegneristiche, afferenti al complesso delle ICT.
Intuitiva sembra a chi scrive l'influenza della revisione della disciplina NIS, che qui è oggetto di analisi principale, sul futuro di tale modello formativo. Mi sembra, però, opportuno richiamare sempre in questa sede la necessità di 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.[8] Per quanto la proposta di tale modello "altro" sembri e suoni, in qualche misura, come una proposta innovativa, l'identità del diritto vivente come alternativa a quella del diritto formale come oggetto di studio e insegnamento (che, come si vedrà, ha avuto un ruolo fondamentale nella nascita 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

8. 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 Buffa 2022.

> tradizionali (anche nel caso in cui tali ideologie erano divenute prescrizioni) ma anche il criterio in base al quale quelle critiche venivano svolte.[9]

Ricordo, inoltre, che è stato sostenuto che non si possa parlare di realismo giuridico americano senza ricordare una distinzione tra due correnti nell'ambito di questo movimento: una prima corrente costituita da quegli autori scettici rispetto alle regole e una seconda costituita da un atteggiamento critico rispetto alla determinazione dei fatti alla base delle regole o da esse qualificati.[10]

9. Tarello 1962: 3. Per una più ampia disamina di queste origini segnalo il volume curato da Fanlo Cortés e Ferrari 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.

10. Si veda, ancora, a questo proposito, Tarello 1962: 8-9 e ss., ove si ricorda che: «[...] Il primo sottogruppo può venire identificato sulla base delle caratteristiche seguenti: a) una esigenza di certezza giuridica, che si manifesta nella convinzione che sia socialmente desiderabile che gli avvocati possano predire ai loro clienti l'esito che una controversia avrebbe ove venisse portata innanzi ai tribunali; b) la convinzione che, allo stato attuale ciò non avvenga; c) l'opinione secondo cui le 'regole giuridiche formali' enunciate nelle decisioni giudiziarie – chiamate talvolta regole di carta – troppo spesso si rivelano insicure in quanto guida alla previsione; d) la convinzione di poter stabilire al di là delle regole di carta, alcune regole reali descrittive di uniformità o regolarità del comportamento giudiziale, e l'opinione che tali regole reali possano servire come effettivo strumento di previsione dei risultati di controversie future». Il secondo gruppo, muovendosi oltre la critica alle cd regole di carta, invece, nella ripresa operata da Tarello delle considerazioni di Frank sul punto: «[...] si distinguono dagli altri, secondo il Frank, perché ritengono che comunque precise o definite possano essere le regole giuridiche formali, [...] qualunque uniformità possano venire scoperte al di là di queste regole formali, nulladimeno è impossibile, e sarò sempre impossibile, predire l'esito di cause future

Entrambe le correnti, però, sono concordi nel ritenere la necessità di una trasformazione profonda della nozione di diritto rispetto a quella staticità che lo contraddistingue nella concezione formalista, sostituendo alla prospettiva dei diritti "di carta", quella del diritto vivente. Con tale formulazione i realisti guardano 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 così un connotato dinamico e, soprattutto, in parte imprevedibile. Altri autori si sono misurati con la definizione di diritto vivente. Nel 1913, E. Ehrlich propone una definizione provocatoria:

> Il diritto vivente è il diritto che, non formulato in proposizioni giuridiche, regola tuttavia la vita sociale. La fonte di conoscenza di questo diritto è, in primo luogo, il moderno documento giuridico; in secondo luogo, l'osservazione diretta della vita sociale, degli scambi, delle consuetudini, degli usi di tutti i gruppi, non solo di quelli riconosciuti giuridicamente, ma anche di quelli ignorati o trascurati dal diritto, e perfino di quelli da esso condannati.

Nella formulazione di Ehrlich il diritto vivente si manifesta come "non diritto", o comunque in un "altro diritto"[11] inse-

poiché i fatti su cui le decisioni si basano rendono impossibile il calcolo dato che i fatti non sono precostituiti, ma vengono determinati nel corso del processo. [...] La certezza del diritto non è un valore perché è – a dirla col Frank – un mito».

11. Tali concetti trovano più di una corrispondenza con il pensiero di N. Llewellyn che in uno scritto rivolto a Pound sostiene che: «Il significato del diritto senza i suoi effetti è praticamente nullo: ignorare i suoi effetti significa ignorare il suo significato e conoscerli senza studiare le persone su cui influisce è impossibile». Castignone, Faralli e Ripoli 2002: 211.

rendosi in quella distanza fra diritto e prassi, fra teoria e pratica, una distanza che si rende ancora più evidente in materia di *cybersecurity* ed infrastrutture critiche. Una "esplosione di parole nuove", ma anche di altrettante competenze: l'occasione di nuove sfide formative, didattiche, così come di ricerca e, prima di tutto, di comprensione. Anche in questo frangente le considerazioni svolte da Thomas Casadei in un recente manuale dedicato alla didattica del diritto mi sembrano rilevanti per guardare ai plurimi significati del diritto in azione, nella complessità delle interazioni tra docenti, studenti e contesto. 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.

> La didattica del diritto non è il diritto stesso. Essa non può tradursi (e ridursi) in "addestramento" al diritto e alle sue regole: le nozioni sono sicuramente un aspetto importante dell'apprendimento, ma se impartite esclusivamente in forma meccanica diventano sterili o, peggio ancora, indigeste per gli studenti e controproducenti ai fini di una buona didassi.

È necessario, invece, guardare al diritto come prodotto della regolazione sociale, della storia e delle culture, dell'argomentazione, dell'interpretazione, delle funzioni che esso è chiamato ad assolvere, per poter immaginare le future generazioni di cittadine/i come soggetti capaci di agire nel, e attraverso, il diritto. Ancora, su questo punto:

> La specificità della didattica delle discipline giuridiche non può pertanto non muovere dall'adozione di un approccio integrato di nozioni di didattica generale, di conoscenze riguardanti i modelli pedagogici

> e da una precisa cognizione delle differenti metodologie che, sul piano dell'insegnamento, possono adottarsi. Per altro verso, tuttavia, un approccio alla didattica del diritto ha bisogno di una adeguata considerazione delle specificità che contraddistinguono, complessivamente, il campo dell'esperienza giuridica, al di là della pluralità delle sue configurazioni sul piano del diritto positivo[12]

da cui, *a fortiori*, l'essenzialità di un approccio siffatto nell'intersezione tra le discipline giuridiche e informatiche.

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 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 fase di redazione della disciplina c.d. NIS II, ciò sembra ancora più importante ai fini della definizione del contesto. Rispetto a quest'ultimo non potranno, in effetti, trascurarsi gli usi non solo dei gruppi che il diritto

12. Marzocco, Zullo e Casadei 2021: 96 e 107.

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,[13] dall'altro) e, persino, condanna, nel definire minacce, vulnerabilità,[14] 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.

13. Tale circostanza porta con sé, secondo alcuni autori, alcune possibili derive problematiche, come osservato da E. Maestri riferendosi a J.R. Reidenberg: la "visione *border-centric* della legislazione e della giurisdizione rischia di determinare la soccombenza del principio di legalità (il diritto come *Rule of law*) a favore del principio di effettività (il diritto come *Problem solving*). In tal senso le tutele apprestate dalle giurisdizioni nazionali e sovranazionali rischiano di affievolirsi per difetto di sovranità, diventando tutele dimezzate a causa del continuo mutamento delle norme tecniche di *soft law* che regolano il *cyberspazio*". L'autore, guardando alle relazioni tra attori azioni e diritto in via orizzontale e animate secondo logiche "dal basso" guarda al 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. Maestri 2015: 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 Maestri 2015, dove nel capitolo quarto si propone un passaggio "dal Panopticon al Synopticon" in cui le tecnologie attuali avrebbero prodotto un effetto, se si vuole, piuttosto paradossale nell'elaborazione di un nuovo paradigma di sorveglianza, in cui pochi sono osservati (e osservabili) da molti e in cui anche gli osservatori possono essere, a loro volta osservati. Ciò, potenzialmente, riguarda – se non tutti – la maggior parte degli utenti del web, circostanza piuttosto allarmante se rapportata alla connotazione malevola di questa "osservazione" e dei suoi intenti. Si veda, infine, Orrù 2021: 203 e ss.

14. 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 Vantin 2021.

2. Contesto della riforma tra coordinamento, consapevolezza e alleanze pubblico-private

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*. Una tale struttura mi sembra già indicativa di lacune significative riscontrate nel breve 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. Di particolare interesse, una possibile tassonomia dei fattori determinanti della necessità di una revisione della normativa cui corrisponde, piuttosto specularmente, la necessità di migliore coordinamento, partenariato e consapevolezza in tema di sicurezza informatica, che qui si propone senza pretesa di esaustività:

1) Crescenti attacchi informatici (in particolare l'attacco all'Ema – *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[15] in uso in UE nel 2024 – che estende le necessità di tutela sempre più anche alle e ai cittadine/i dell'UE, quindi non solo con esclusivo riferimento alle persone giuridiche);
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[16] 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*.[17]

15. 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 Zanuzzi 2017: 99 e ss.

16. Nell'opinione delle istituzioni europee il regime di vigilanza e esecuzione della direttiva NIS non è stato efficace. Gli Stati membri avrebbero mostrato molta riluttanza nell'applicazione delle sanzioni ai soggetti che omettevano di adottare requisiti di sicurezza o di segnalare incidenti. Ciò può avere conseguenze negative per la resilienza dei singoli soggetti rilevanti e, inoltre, a livello del mercato interno dell'Unione Europea nel suo complesso.

17. "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

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 im-

ulteriore terreno (virtuale) di scontro, e per la sua frequenza appare ormai come una costante fisiologica delle vicende internazionali. Mentre gli Stati (e i loro cittadini) appaiono sempre più bisognosi di tutele dinanzi al proliferare di nuove minacce, ancora una volta la politica e il diritto faticano a tenere il passo di un'evoluzione tecnologica che procede secondo logiche e ritmi estremamente più rapidi. In tale contesto, in una prospettiva giuridica appare particolarmente urgente interrogarsi sulle risposte fornite dall'ordinamento internazionale alle sfide del cyberspazio [...] frequentemente associata al termine "cyberwarfare" ("guerra cibernetica") definibile come un insieme di "azioni compiute da una nazione per penetrare nei computer o nelle reti di un'altra nazione al fine di causare un danno o un'interruzione di un servizio" e in tempi recenti intesa anche in accezioni più ampie comprensive degli atti di soggetti non statali. 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 Ferruglio 2018: 91-93. Sul rapporto tra sicurezza informatica, *cybercrime* e *cyberwarfare* si veda anche l'ultimo capitolo del lavoro monografico di D'Avanzo 2020: 245 e ss. Ancora, per una mappatura legata anche alla definizione del perimetro nazionale di sicurezza cibernetica, Aterno 202: 207 e ss.

prese avrebbero sofferto, nel 2021, di un attacco ogni 11 secondi (era un attacco ogni 40 nel 2016).
È, per altro, 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[18] si sono rivelate *target* preferenzia-

18. Come si è evidenziato nel corso delle lezioni del Master universitario di II livello *in cybersecurity and critical infrastructures protection* dell'Università degli Studi di Genova 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. Guardando non solo al contesto continentale eurocentrico diversi soggetti hanno tentato una possibile classificazione. Oltre oceano il Dipartimento per la sicurezza interna degli Stati Uniti (DHS) ha stabilito che: "Le infrastrutture critiche della nazione forniscono i servizi essenziali che sono alla base della società statunitense e servono da spina dorsale dell'economia, della sicurezza e della salute della nostra nazione". Il DHS elenca 16 settori "così vitali per gli Stati Uniti che il loro malfunzionamento o distruzione avrebbe un effetto debilitante sulla sicurezza, l'economia nazionale, la salute o la sicurezza pubblica nazionale, o qualsiasi combinazione di questi elementi". 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

le, con aggravamento dovuto ai c.d. sistemi interconnessi[19] (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).

Rinaldi, Peerenboom e Kelly,[20] hanno descritto queste interdipendenze sulla base di sei dimensioni possibili.

1. Ambiente/contesto: struttura entro la quale soggetti proprietari e operatori di sistema stabiliscono finalità e obiettivi, costruiscono sistemi di valori per definire il loro *business*. Lo stato operativo e le caratteristiche dell'infrastruttura influenzano l'ambiente e a sua volta l'ambiente influenza l'infrastruttura.
2. Tipi di interdipendenza: per gli autori possiamo trovarci in presenza di un'interdipendenza di tipo fisico, *cyber*, geografico (un'eventuale catastrofe o evento ambientale può comportare cambiamenti allo stato di altre infrastrutture, quando si condivide lo stesso luogo fisico, ma anche un ponte, una stanza) o, ancora, logico (se lo stato di ognuna delle infrastrutture dipende dallo stato dell'altra con un meccanismo che non è nessuno dei precedenti, uno stato tipicamente legato a scambi di servizi tra infrastrutture, fenomeni socio culturali, vincoli legislativi, le decisioni umane sono tipicamente centrali nella creazione di questi vincoli e legami).

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 Setola 2011: 10 e ss.

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

20. Rinaldi, Peerenboom e Kelly 2002: 12 e ss.

Sempre secondo gli autori la classificazione può essere estesa a cause di tipo "sociologico", cioè riconducibili al comportamento di operatori umani quali, ad es., la saturazione della linea telefonica per una situazione che determina la connessione contemporanea di molti soggetti, ovvero la scelta di disattendere compiti determinati per motivazioni "etiche".

3. Stato operativo: secondo gli autori esso descriverebbe il funzionamento dell'infrastruttura; il normale funzionamento o situazioni anomale hanno diverse ricadute sugli altri soggetti, è importante, per tale ragione, comprendere anche gli effetti e le tempistiche dello stato di ripristino a seguito di un eventuale guasto o mancato funzionamento.
4. Caratteristiche dell'infrastruttura: nel modello proposto troviamo elementi ben definiti, in particolare la scala spaziale, da intendersi come lo spazio in cui è collocata l'infrastruttura in cui si stabilisce una gerarchia:
   a) Parte: la componente più piccola dell'analisi che è possibile unire in
   b) Unità: come insieme di parti correlate funzionalmente da un
   c) Sottosistema, come linea di unità che compongono un
   d) Sistema, raggruppamento di sottosistemi (ad es. una centrale nucleare) e, infine:
   e) Infrastruttura, come un insieme completo di sistemi simili. Come noto essi possono riferirsi ad un'identità nazionale, sovranazionale, internazionale.

È anche possibile adottare una scala temporale che descriva l'orizzonte di interesse o il tempo di vita dell'infrastruttura; anche il ciclo e il tempo di vita dell'infrastruttura sono variabi-

li, tipicamente, anche in unità di misura: passiamo da secondi (sistema energetico) a ore (forniture di acqua, gas, trasporti) o persino ad anni (se guardiamo al miglioramento o aumento delle capacità della infrastruttura). Le interdipendenze di tipo logico sono qui più importanti.

Abbiamo poi fattori operativi che riguardano la possibile reazione delle infrastrutture a fattori o elementi di stress o perturbazione/turbamento. Fattori di carattere organizzativo, determinati dal comportamento delle infrastrutture.

1) Nell'analisi di questi autori non meno importante è l'analisi che riguarda il tipo di guasto e le interdipendenze tra le infrastrutture che possono costituire il mezzo attraverso il quale un guasto può propagarsi:
   a) a cascata, quando il guasto della prima provoca il guasto nella seconda, poi nella terza, con effetto domino;
   b) quando il malfunzionamento dell'infrastruttura rende più gravoso un malfunzionamento nella seconda infrastruttura, indipendente dal primo;
   c) a causa comune quando due o più infrastrutture subiscono guasto per lo stesso motivo e nello stesso momento.
2) Infine, rilevante è anche il c.d. "livello di accoppiamento". Esso, che può distinguersi tra stretto o lasco, influisce sul tempo di propagazione insieme al comportamento nella risposta. Se stretto, quando le infrastrutture sono fortemente interdipendenti, le interazioni che potranno essere di tipo lineare o complesso, avranno un effetto più veloce sul tempo e sull'intensità della propagazione. Se, invece, siamo in presenza di un accoppiamento lasco – agenti o strutture sono relativamente dipendenti – allora vi sarà poca relazione e correlazione nella interdipendenza degli stati.

Alla base di tutti i tentativi di revisione della normativa di settore, la consapevolezza dei meccanismi funzionali dell'interdipendenza e dell'interconnessione tra le infrastrutture che sino a qui si sono menzionate sembra avere avuto alterna fortuna, da cui la sottesa opportunità di richiamarle, in questa sede, seppure in sintesi.

Nel 2004 il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche istituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri, nel suo rapporto conclusivo sulla situazione italiana definisce le infrastrutture critiche come quel: "Complesso di reti e sistemi che includono industrie, istituzioni, e strutture di distribuzione che operando in modo sinergico producono un flusso continuato di merci e servizi essenziali per l'organizzazione, la funzionalità e la stabilità economica di un moderno paese industrializzato e la cui distruzione o temporanea indisponibilità può indurre un impatto debilitante sull'economia, la vita quotidiana o le capacità di difesa di un paese".

A questa apertura e alla necessità di una definizione comune volta all'avvicinamento della normativa di settore degli Stati membri, nella consapevolezza della sempre maggiore interconnessione dei sistemi è intervenuto il diritto dell'Unione europea. L'8 dicembre 2008 il Consiglio dell'Unione ha emanato la direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione. Seppur relativa alle infrastrutture critiche europee, nonché parziale, in quanto focalizzata soltanto su quelle dei settori dell'energia e trasporti, il punto a) dell'art. 2 fornisce una

definizione di infrastruttura critica per cui si intende: "un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni".

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).[21]

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, renden-

21. 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)".

do così possibile il passaggio dalla c. d. *Business impact assessment* (BIA) alla c. d. *citizen impact asssessment* (CIA). L'ENISA[22] ha monitorato ed evidenziato la sempre maggiore so-

22. *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. Istituita nel 2004 e rafforzata dalla legge dell'UE sulla cybersecurity, l'Agenzia dell'Unione Europea per la Cybersicurezza contribuisce alla politica informatica dell'UE, rafforza l'affidabilità dei prodotti, dei servizi e dei processi TIC con i sistemi di certificazione della sicurezza *cyber*, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi alle sfide informatiche di domani. Attraverso la condivisione delle conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, rafforzare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, mantenere la società e i cittadini europei sicuri dal punto di vista digitale. Si veda il sito istituzionale per migliori e maggiori dettagli sul mandato e sull'operato di tale organo. Per quanto qui di interesse si rinvia, inoltre, alla pagina dedicata alla direttiva NIS: https://www.enisa.europa.eu/topics/nis-directive ove si legge che la direttiva NIS (cfr. UE 2016/1148) è il primo atto legislativo dell'UE in materia di *cybersecurity*. L'obiettivo principale è quello di migliorare la *cybersecurity* in tutta l'UE. La direttiva NIS è stata adottata nel 2016 e successivamente ogni Stato membro dell'UE ha iniziato a adottare una legislazione nazionale, che segue o "recepisce" la direttiva. La direttiva NIS si compone di tre parti: 1. Capacità nazionali. 2. Collaborazione. 3. Vigilanza nazionale dei settori critici: gli Stati membri dell'UE devono supervisionare la *cybersecurity* degli operatori di mercato critici nel loro paese: vigilanza ex ante nei settori critici (energia, trasporti, acqua, sanità, infrastrutture digitali e settore finanziario), supervisione ex post per i fornitori di servizi digitali critici (mercati online, cloud e motori di ricerca online). Sulla distinzione tra settori critici e fornitori di servizi digitali si rimanda al prosieguo di questa trattazione che guarderà, specificamente, alle novità introdotte dalla direttiva c.d. NIS II nella distinzione tra soggetti essenziali ed importanti. Per una panoramica del recepimento

fisticazione, 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.[23]
Diversi indici di resilienza nell'ambito della *cybersecurity* delle persone giuridiche tra gli Stati membri hanno avuto ricadute

della normativa di cui alla direttiva NIS I si rimanda, infine, alla sezione accessibile al collegamento: https://digital-strategy.ec.europa.eu/en/policies/nis-transposition da cui è possibile accedere ai dati comunicati da ogni Stato membro anche in relazione alla strategia nazionale di sicurezza *cyber*, punto di contatto, autorità competente per i soggetti e settori critici e per quanto attiene i fornitori di servizi digitali critici.

23. Il tema in argomento, oggetto di approfondimento specifico in diversi moduli del Master di II livello in *Cybersecurity and critical infrastructures protection* dell'Università degli Studi di Genova, è connotato dalla convivenza, da un lato, di una certa complessità "sistemica" che tiene conto dell'unicità dei soggetti e delle specifiche caratteristiche idonei a connotarli al fine e, dall'altro, da diversi tentativi di standardizzazione. 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".

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 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*.[24]

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 mi-

24. "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". Panzani 2017: 1231 e ss.

gliore 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. Analisi di impatto

Il percorso di implementazione e recepimento della direttiva NIS ha chiesto alla Commissione di riesaminare il funzionamento della disciplina introdotta. Nell'ambito del suo obiettivo chiave, cioè quello di rendere "l'Europa adatta all'era digitale" e in linea con gli obiettivi dell'Unione della sicurezza, la Commissione ha annunciato – nel suo programma di lavoro 2020 – che avrebbe condotto il riesame della direttiva NIS entro la fine del 2020. Per questa ragione, il 25 giugno 2020, la Commissione ha pubblicato una *road map* combinata per la valutazione di impatto iniziale sulla revisione della direttiva NIS, in base alla quale si prevedeva di «valutare il funzionamento della direttiva NIS avendo a riguardo il livello di sicurezza delle reti e dei sistemi informativi negli Stati membri».
La Commissione ha sottolineato che la revisione era "ulteriormente giustificata dall'improvviso aumento della dipendenza dalle tecnologie dell'informazione durante la crisi Covid-19", dichiarando inoltre che "A seconda dei risultati della valutazione del funzionamento della direttiva NIS, un pubblico aperto consultazione e valutazione d'impatto, la Commissione potrebbe proporre misure volte a migliorare il livello di sicurezza cibernetica all'interno dell'Unione".

La valutazione della Commissione ha analizzato, pertanto, la direttiva NIS rispetto a rilevanza, coerenza, efficacia ed efficienza. Le sue principali conclusioni hanno messo in luce che l'ambito di applicazione della direttiva NIS è apparso troppo limitato in termini di settori coinvolti, principalmente a causa di:

i) Una sempre crescente digitalizzazione e un parimenti maggiore grado di interconnessione, nei termini che sopra si sono meglio descritti, tra soggetti rilevanti, anche di rilevanza transazionale;
ii) l'ambito di applicazione della direttiva NIS non riflette più tutti settori digitalizzati che forniscono servizi chiave all'economia e alla società nel suo complesso.

Inoltre, la valutazione ha concluso che la direttiva NIS non ha fornito sufficiente chiarezza per quanto riguarda i criteri di soglia per gli OSE e la competenza nazionale delle *authority* sui fornitori di servizi digitali. Questo ha portato a una situazione in cui alcuni tipi di entità non sono stati identificati come soggetti rilevanti per l'applicazione della disciplina in alcuni Stati membri e non sono quindi stati tenuti ad adottare e mettere in atto misure di sicurezza e segnalare incidenti. A titolo esemplificativo, allo stato attuale, alcuni grandi ospedali in un determinato Stato membro non rientrano nell'ambito di applicazione della direttiva NIS e, quindi, non sono tenuti ad attuare le misure di sicurezza che ne discendono, mentre in un altro Stato Membro ogni singolo operatore sanitario è interessato dai requisiti di sicurezza NIS con gli obblighi che ne discendono.

La direttiva NIS nella sua prima formulazione del 2016 ha in effetti conferito agli Stati Membri, come già sottolineato, un

ampio potere discrezionale nel definire la sicurezza, gli incidenti da ritenersi "rilevanti", gli obblighi di segnalazione per gli OSE. Per questo la valutazione condotta in termini di impatto ha mostrato che, in alcuni casi, gli ordinamenti nazionali hanno implementato questi requisiti in modi significativamente diversi, creando per altro oneri aggiuntivi (e spesso dissonanti) per società e imprese operanti in più di uno Stato membro.
Per il complesso di tali elementi il regime di supervisione e di applicazione della direttiva NIS è risultato, in parte, inefficace. Le risorse finanziarie e umane accantonate e individuate dagli Stati membri per l'assolvimento dei loro compiti (come l'identificazione degli OSE e ai fini del monitoraggio e della loro supervisione), e di conseguenza, i diversi livelli di competenza nell'affrontare i rischi per la *cyber* sicurezza, variano notevolmente.

- Ciò aggrava ulteriormente le differenze nella *cyber* resilienza tra gli Stati membri (*awareness*).
- Gli Stati membri non condividono sistematicamente[25] le informazioni tra loro, con dati negativi conseguenze in partico-

25. Sulla necessità di una riflessione nell'azione, consapevole della ineludibilità di capacità adattive che risiedono sul piano delle competenze e della loro possibilità di apprendimento costante, anche ai fini dell'evidenziazione della dimensione etimologica dal connotato collettivo di termine "competenza" come *cum petere*, cioè a dire chiedersi insieme, sembra interessante ricordare, con un riferimento alla letteratura "atecnica", ma interessante nella prospettiva del paragone con il c.d. *law in action*, che: «Quando i bravi musicisti jazz improvvisano insieme, manifestano anche un "sentimento" per il loro materiale e apportano modifiche "sul posto" ai suoni che sentono. Ascoltandosi l'un l'altro e ascoltando sé stessi, sentono dove sta andando la musica e adattano il loro modo di suonare di conseguenza. Possono farlo, prima di tutto, perché il loro sforzo collettivo di invenzione musicale si avvale di uno schema – uno schema metrico,

lare per l'efficacia delle misure di sicurezza *cyber* e il livello di consapevolezza situazionale a livello dell'UE (*coordination*).
- A mancare, inoltre, è anche la condivisione delle informazioni tra soggetti individuali e per l'impegno tra le strutture di cooperazione a livello dell'UE e gli enti privati (*public-private partnership*).

4. Stati membri: verso una consapevolezza situazionale comune

L'obiettivo del riesame della direttiva NIS, guardando al contesto e all'analisi di impatto che precede, può essere sintetizzato come quello atto ad aumentare il livello di *cyber resilience* di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori pertinenti, ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva e, infine, migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta in caso di violazioni della sicurezza *cyber*.

A tale obiettivo di ordine generale e molto legato alle politiche in tema di mercato e libera concorrenza si aggiungono, inoltre, obiettivi maggiormente specifici che si legano a problemi puntuali:

melodico e armonico familiare a tutti i partecipanti – che dà un ordine prevedibile al pezzo. Inoltre, ciascuno dei musicisti ha a disposizione un repertorio di figure musicali che può fornire al momento opportuno. L'improvvisazione consiste nel variare, combinare e ricombinare un insieme di figure all'interno dello schema che delimita e dà coerenza alla performance. Quando i musicisti ascoltano la direzione della musica che si sta sviluppando dai loro contributi intrecciati, ne danno un nuovo senso e adattano la loro performance a questo nuovo senso creato. Stanno riflettendo nell'azione sulla musica che stanno suonando collettivamente e sui loro contributi individuali ad essa, pensando a ciò che stanno facendo e, nel processo, migliorando il loro modo di farlo». Schön 1983: 55.

a) Per affrontare il tema del basso livello di *cyber* resilienza delle imprese che operano nell'Unione europea, l'obiettivo specifico è quello di garantire che i soggetti in tutti i settori che dipendono dai sistemi informatici e di rete e che forniscono servizi chiave all'economia e alla società nel suo complesso siano tenuti a adottare misure di sicurezza *cyber* e a segnalare gli incidenti al fine di aumentare il livello globale di capacità di resilienza e risposta in tutto il mercato interno. La sottolineatura relativa al mercato in luogo dell'ordinamento non sembra, a chi scrive, indifferente.
b) Per affrontare il problema del livello differente di resilienza tra Stati membri e tra settori, l'obiettivo specifico è quello di garantire che tutti i soggetti attivi in settori disciplinati dal quadro giuridico della NIS, di dimensioni simili e aventi un ruolo comparabile, siano soggetti allo stesso regime normativo cioè a dire che esso sia uniforme indipendentemente dalla giurisdizione e dall'ordinamento cui sono sottoposte nell'Unione europea.
c) Al fine di garantire che tutti i soggetti attivi nei settori disciplinati dal quadro giuridico della NIS siano tenuti a rispettare gli stessi obblighi basati sul concetto di gestione del rischio per quanto riguarda le misure di sicurezza e a segnalare tutti gli incidenti sulla base di un insieme uniforme di criteri, gli obiettivi specifici sono volti a garantire che le autorità competenti applichino in modo più efficace le norme stabilite dal livello giuridico attraverso misure allineate di vigilanza e applicazione e garantire un livello comparabile di risorse tra gli Stati membri assegnate alle autorità competenti che consentano loro di svolgere i compiti fondamentali definiti dal quadro della NIS.

d) Per affrontare il nodo della consapevolezza situazionale comune e della mancanza di una risposta comune alle crisi, l'obiettivo specifico è di garantire lo scambio di informazioni essenziali tra gli Stati membri introducendo obblighi di condivisione di informazioni e di cooperazione chiari per le autorità competenti in relazione a minacce e incidenti informatici e sviluppando una capacità operativa comune di risposta dell'Unione alle crisi.

5. *Cybersecurity* e *cyber reselience*: essenzialità e importanza di nuovi soggetti rilevanti

L'approccio del diritto vivente, con attenzione ai contenuti "minimi" che lo abitano in termini di giurisprudenza, dottrina e prassi amministrative, chiede di guardare – come si è già evidenziato in precedenza – anche agli usi dei gruppi sociali e dei soggetti che abitano l'ordinamento, tanto più in una fase come quella attualmente in essere, cioè a dire di transizione verso la disciplina in via di adozione da parte delle istituzioni degli Stati membri. 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 ("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) coinvolti 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.[26] 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.[27]

26. 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.

27. 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".

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 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 e, inoltre, l'one-

re che potrebbe discendere dai requisiti della nuova direttiva, in particolare dal punto di vista della vigilanza, sarebbe anche bilanciato sia per i nuovi soggetti da comprendere nell'ambito di applicazione sia per le autorità competenti. 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".

Complessivamente, la proposta prevede efficienti compromessi e sinergie, con migliori potenzialità tra tutte le opzioni strategiche analizzate per garantire un livello di *cyber* sicurezza superiore e coerente dei soggetti chiave all'interno dell'Unione, con risparmi di costi sia per le imprese che per la società.

Se guardiamo al piano delle risorse, per le imprese che, ferma l'incognita e la conseguente necessità di una valutazione puntuale delle diverse forme e modalità di recepimento nel merito da parte degli Stati membri nell'applicazione del quadro NIS, si stima che per i primi anni successivi all'introduzione del nuovo assetto normativo sarebbe necessario un aumento massimo del 22 % della spesa corrente per la sicurezza delle TIC (tecnologie per l'informazione e la comunicazione, secondo l'acronimo italiano) tale aumento sarebbe del 12 % per le imprese già rientranti nell'ambito di applicazione della direttiva NIS vigente. Tuttavia, questo aumento medio della spesa per la sicurezza delle TIC porterebbe ad un vantaggio proporzionale di tali investimenti, dovuto in particolare a una considerevole riduzione dei costi degli incidenti di sicurezza cibernetica stimata a 118 miliardi di euro entro dieci anni.

Nelle intenzioni dichiarate del legislatore europeo le piccole imprese e le microimprese non rientreranno nell'ambito di applicazione del quadro NIS II, se non in relazione al possibile loro coinvolgimento e attenzionamento nel contesto della *supply chain*. Anche per le medie imprese è possibile prevedere un aumento del livello di spesa per la sicurezza delle TIC nei primi anni successivi all'introduzione della riforma. Allo stesso tempo, l'aumento del livello dei requisiti di sicurezza per tali soggetti incentiverebbe anche le loro capacità di *cyber security* e contribuirebbe a migliorare la loro gestione del rischio. Non trascurabile, poi, l'impatto sui bilanci e sulle amministrazioni nazionali: si prevede, con l'implementazione di queste disposizioni, un aumento stimato di circa il 20-30% delle risorse a breve e medio termine nei settori di interesse di competenza della normativa in analisi.

Dal punto di vista economico finanziario non sono previsti e prevedibili, allo stato, altri impatti significativi. La proposta dovrebbe determinare funzionalità di sicurezza più solide e, di conseguenza, avrebbe un impatto attenuante più sostanziale sul numero e sulla gravità degli incidenti, comprese le violazioni di dati, con conseguente aumento della sostenibilità degli investimenti necessari, contenimento dei danni patiti e patendi da parte delle imprese coinvolte e, in termini generali, di un risparmio a lungo termine di risorse. 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 *cyber security* e con riguardo ai soggetti coinvolti, pur evidenziando come 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.

6. NIS II: Base giuridica e *ratio* di una riforma attesa

La base giuridica della direttiva NIS II è riconducibile all'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE) il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Conformemente alla sentenza della Corte di giustizia dell'UE nella causa C58/08, Vodafone Ltd e altri, il ricorso all'articolo 114 TFUE è giustificato in caso di divergenze tra le normative nazionali qualora queste incidano direttamente sul funzionamento del mercato interno. Analogamente, la Corte ha ritenuto che qualora un atto fondato sull'articolo 114 TFUE abbia già eliminato qualsiasi ostacolo agli scambi nel settore da esso armonizzato, il legislatore dell'Unione non può essere privato della possibilità di adeguare tale atto a qualsivoglia modificazione delle circostanze o evoluzione delle conoscenze, in considerazione del compito affidatogli di vigilare alla protezione degli interessi generali riconosciuti dal trattato. Infine, secondo il Giudice europeo le misure relative al ravvicinamento previste dall'articolo 114 TFUE intendono consentire, in funzione del contesto generale e delle circostanze specifiche della materia da armonizzare, un margine di discrezionalità in merito alla tecnica di ravvicinamento più appropriata per ottenere il risultato auspicato. L'atto giuridico proposto favorirebbe e migliorerebbe l'instaurazione e il funzionamento del mercato interno per i soggetti essenziali e importanti stabilendo norme chiare e generalmente applicabili relative all'ambito di applicazione della

direttiva NIS e armonizzando le norme applicabili nel settore della gestione del rischio *cyber* e della segnalazione di incidenti. Le attuali disparità in questo settore, sia a livello legislativo che di vigilanza, nonché a livello nazionale e dell'Unione, sono state ritenute così importanti da costituire ostacoli per il mercato interno. I soggetti impegnati in attività transfrontaliere si trovano a fare fronte a obblighi normativi diversi, con possibili sovrapposizioni, e/o una diversa applicazione degli stessi a scapito dell'esercizio della loro libertà di stabilimento e della libera prestazione di servizi. Norme diverse hanno anche un impatto negativo sulle condizioni della concorrenza nel mercato interno quando si tratta di soggetti dello stesso tipo in Stati membri differenti.

Vicina alla base giuridica di questo intervento legislativo e interessante oggetto di analisi sembra anche la *ratio* della norma in commento che, a questo punto, possiamo sintetizzare come volta a conseguire specifici obiettivi di contenimento e riduzione delle spese che hanno visto, in questi ultimi anni, una crescita esponenziale e poco prevedibile, in particolare al fine di:

- Affrontare il problema attualmente persistente dell'insufficienza del livello di preparazione in materia di *cybersecurity* degli Stati membri e di società e altre organizzazioni per ottenere un miglioramento in termini di efficienza e riduzione dei costi supplementari derivanti da incidenti in ambito *network&information security*.
- Per i soggetti essenziali e importanti, l'aumento del livello di preparazione in materia di *cyber risk* e *security* potrebbe attenuare la potenziale perdita di entrate a causa di perturbazioni, dovute anche allo spionaggio industriale, riducendo

altresì le ingenti spese destinate alla mitigazione *ad hoc* delle minacce. Tali vantaggi dovrebbero superare i costi d'investimento necessari. La riduzione della frammentazione del mercato interno migliorerebbe anche la parità di condizioni tra operatori.

- Per gli Stati membri tali miglioramenti "strutturali" potrebbero ulteriormente ridurre il rischio di un aumento delle spese di bilancio destinate alla mitigazione *ad hoc* delle minacce e i costi supplementari in caso di emergenze legate a incidenti classificabili nel piano della sicurezza informatica e delle comunicazioni.
- Per le cittadine e i cittadini dell'Unione, affrontare il problema degli incidenti di *cybersecurity* si tradurrà prevedibilmente in una riduzione delle perdite di reddito dovute a perturbazioni economiche legate a questo nuovo tipo di minacce per la propria incolumità, sia dal punto di vista personale che patrimoniale.

Se guardiamo all'ambito di applicazione della direttiva NIS II esso sembra di fatto sovrapponibile e in continuità a quello della direttiva NIS nella sua prima formulazione, ancorché con alcuni punti di distinzione, in particolare ove essa:

a) stabilisce obblighi per gli Stati membri al fine di adottare una strategia nazionale per la *cybersecurity*, designare autorità nazionali competenti, punti di contatto unici e CSIRT;[28]

28. Dal sito https://www.csirt.gov.it/ è possibile apprendere che il CSIRT in Italia è istituito presso l'Agenzia per la *cyber* sicurezza nazionale (ACN). I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 art. 4. Essi includono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di

b) prevede che gli Stati membri stabiliscano obblighi di gestione e segnalazione dei rischi di sicurezza *cyber* per i soggetti indicati come soggetti essenziali nell'allegato I e come soggetti importanti nell'allegato II;
c) prescrive che gli Stati membri stabiliscano obblighi in materia di condivisione delle informazioni sulla "*cyber* sicurezza".

Le microimprese e le piccole imprese, ai sensi della raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, sono escluse dall'ambito di applicazione della direttiva, ad eccezione dei fornitori di reti di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, dei prestatori di servizi fiduciari, dei registri dei nomi di dominio di primo livello (*top-level domain, here and after*, TLD) e della pubblica amministrazione, nonché di alcuni altri soggetti, come l'unico fornitore di un servizio in uno Stato membro.

Se guardiamo, in particolare, a quest'ultima previsione è facile intuire come, di fatto, si tratti di una clausola aperta cui sarà necessario dare applicazione in ogni Stato membro con possibilità di ampliamento del novero dei soggetti interessati anche tra le piccole e medie imprese e, non di meno, il rischio di discrezionalità e disparità nei diversi contesti che potrebbero riguardare sia la caratteristica dell'unicità del soggetto in rapporto ad un servizio settore altrimenti escluso da quelli essenziali

incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT. Il CSIRT stabilisce relazioni di cooperazione con il settore privato. Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni. Il profilo completo dello CSIRT Italia è contenuto nel documento disponibile all'indirizzo: https://www.csirt.gov.it/rfc2350.txt

ed importanti, ovvero la noverazione tra soggetti importanti ed essenziali di funzioni non attinenti ai settori individuati come strategici e critici per la *cybersecurity* e, in fondo, per la sicurezza nazionale.

7. Attraversare la riforma: quadri, cooperazione, condivisione, gestione e obblighi di 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 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 Incidente 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[29] sulla fornitura dei loro servizi.
I registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per tali livelli dovranno raccogliere e mantenere dati di registrazione dei nomi di dominio che siano accurati e completi. Infine, per consentire un'effettiva utilità a tali prescrizioni, i soggetti interessati saranno tenuti a fornire un accesso efficiente ai dati di registrazione del dominio per coloro che richiederanno legittimamente l'accesso. Di norma, i soggetti essenziali e importanti saranno da ritenersi come sottoposti alla giurisdizione dello Stato membro in cui

29. Si vedrà *infra* l'ampliamento di questa definizione aperta secondo criteri concorrenti.

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*,[30] 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.

Con ultimo riguardo al tema della condivisione delle informazioni, come si è già avuto modo di evidenziare, essa è tratto necessario e trasversale ai tre assi fondamentali su cui la direttiva NIS II si struttura. Per tale ragione gli Stati membri sono chiamati, in applicazione e recepimento della disciplina, ad adotta-

30. 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 Moro e Sarra 2017: 179, dove l'autore, analizzati i diversi possibili inquadramenti contrattuali, si concentra anche sui maggiori problemi legati alla tutela dei dati e della sicurezza, ricordando gli interventi che da vari fronti (sia da parte del Garante privacy italiano che da parte dell'ENISA) mirano ad un accrescimento della consapevolezza da parte degli utenti. La necessità di questo "miglioramento continuo", tipica delle tecniche di *business management*, riguarda anche una tipizzazione delle possibili vulnerabilità e minacce, nonché una rinnovata responsabilità in considerazione della difficile possibilità di copertura contro tali rischi nell'*outsourcing* del *risk management* attraverso polizze assicurative di sorta considerata la sempre maggiore indisponibilità delle compagnie assicurative in questa direzione.

re norme che consentano ai soggetti di partecipare alla condivisione di informazioni relative alla *cybersecurity* nel quadro di specifici accordi di condivisione di informazioni in materia, in conformità all'articolo 101 TFUE. Al medesimo fine, gli Stati membri dovranno consentire ai soggetti che non rientrano nell'ambito di applicazione della direttiva NIS II di segnalare, su base volontaria, incidenti significativi, minacce informatiche o "quasi incidenti" che siano da considerarsi rilevanti.
Completa il quadro di sintesi delle disposizioni e previsioni della riforma il riferimento del legislatore europeo ad una sezione dedicata alla vigilanza e al monitoraggio dell'applicazione della norma nei diversi contesti, nazionali e sovranazionale. 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.[31]

31. Si legge, nel considerando n. 127 del testo della direttiva c. d. NIS II, che: "Al fine di rendere efficace l'esecuzione, è opportuno stabilire un elenco minimo di sanzioni amministrative in caso di violazione degli obblighi di gestione e segnalazione dei rischi di sicurezza *cyber* previsti dalla presente direttiva, istituendo un quadro chiaro e coerente per tali sanzioni in tutta l'Unione. Occorre tenere debitamente conto della natura, della gravità e della durata dell'infrazione, del danno effettivamente causato o delle perdite effettivamente subite o del danno o delle perdite potenziali che si sarebbero potuti verificare, del carattere doloso o colposo della violazione, delle azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite, del grado di responsabilità o di eventuali violazioni precedenti pertinenti, del grado di cooperazione con l'autorità competente e di qualsiasi altro fattore aggravante o attenuante. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie, dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva

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[32] che un soggetto im-

tutela giurisdizionale e il giusto processo". Nel non escludere persino profili di responsabilità penale, il considerando n. 133 afferma, ancora, che: "Al fine di rafforzare ulteriormente l'efficacia e il carattere dissuasivo delle sanzioni applicabili alle violazioni degli obblighi stabiliti a norma della presente direttiva, le autorità competenti dovrebbero avere la facoltà di applicare sanzioni consistenti nella sospensione di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi forniti da un soggetto essenziale e nell'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di una persona fisica. Data la loro gravità e l'impatto sulle attività dei soggetti e, in ultima analisi, sui consumatori, tali sanzioni dovrebbero essere applicate solo in proporzione alla gravità della violazione e tenere conto delle circostanze specifiche di ciascun caso, tra cui il carattere doloso o colposo della violazione e le azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite. Tali sanzioni dovrebbero essere applicate solo come ultima *ratio*, vale a dire solo una volta esaurite le altre pertinenti misure di esecuzione previste dalla presente direttiva, e solo fino a quando i soggetti ai quali si applicano non adottino le misure necessarie per rimediare alle carenze o per conformarsi alle prescrizioni dell'autorità competente per cui tali sanzioni sono state applicate. L'imposizione di tali sanzioni dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale, il giusto processo, la presunzione di innocenza e i diritti della difesa".

32. 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*.

portante 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.[33] A 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.

8. NIS II: Oltre i confini dell'Unione?

In apertura di questo contributo si sono già evidenziate le ragioni di una rilevanza transnazionale ed extraeuropea della disciplina oggetto di recente approvazione. Essa ricorda, ove opportuno, che l'Unione sarà chiamata a concludere accordi internazionali, in conformità all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali che consentano la loro partecipazione ad alcune delle attività del gruppo di coopera-

33. "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 per l'esercizio precedente dell'impresa cui il soggetto essenziale o importante appartiene, se tale importo è superiore" ex art. 34 c. 4 della 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.

zione e della rete di CSIRT. Tali accordi sono intesi a garantire un'adeguata protezione dei dati e una copertura maggiore delle variabili e delle ipotesi verificabili in uno spazio, quale quello *cyber*, dove i confini nazionali e sovranazionali sembrano perdere di rilevanza, a beneficio dell'istituzione di perimetri di sicurezza che, necessariamente, si interfacciano con minacce, sfide e vulnerabilità globali e, pertanto, della difficile riconduzione a contesti meramente locali-continentali. Gli Stati membri, a questo fine, dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di *cybersecurity* dell'UE attraverso le reti di cooperazione esistenti, in particolare la già ricordata rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)[34] la rete di CSIRT e il gruppo di cooperazione.

In ultimo, a riprova della forte rilevanza internazionalistica delle disposizioni in commento oltre i confini dell'Unione con ricadute sul diritto pubblico internazionale, per la gestione delle crisi a livello europeo si prevede che le parti debbano potersi affidare alle indicazioni dei dispositivi integrati per la risposta politica alle crisi (IPCR). A tal fine la Commissione è chiamata a fare ricorso al processo di coordinamento intersettoriale delle "crisi ad alto livello" del sistema ARGUS. Se la crisi implicherà un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) dovrà essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna (SEAE).

34. Il regolamento interno di EU-CyCLONe dovrà specificare ulteriormente, in sede di sua redazione e adozione, le modalità di funzionamento della rete comprendendo, tra l'altro, i ruoli, le modalità di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione in utilizzo.

9. Notifiche, segnalazioni e cooperazione: un nuovo sistema integrato

Sempre in tema di collaborazione tra le autorità nazionali e sovranazionali la disciplina in commento prevede che, se diverse tra loro, le autorità competenti, il punto di contatto unico e i CSIRT di uno stesso Stato membro saranno chiamati a cooperare tra loro. L'opportunità di una cooperazione è da intendersi valida, in particolare, per quanto concerne l'adempimento degli obblighi previsti dalla direttiva in tema di notifiche, che coinvolgeranno un complesso di soggetti eterogenei. Nello specifico gli Stati membri sono tenuti a provvedere affinché tutti gli organi rilevanti ricevano le notifiche in merito agli incidenti, alle minacce informatiche significative e ai quasi incidenti (c.d. *near miss)*. Tali obblighi trovano opportuno rafforzamento cooperativo grazie alla previsione per cui, nella misura necessaria per l'efficace adempimento dei compiti e degli obblighi stabiliti dalla direttiva all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra le autorità competenti e i punti di contatto unici e le autorità di contrasto, le autorità di protezione dei dati, le autorità responsabili delle infrastrutture critiche.
Con specifico riguardo agli obblighi di segnalazione introdotti dalla direttiva NIS II gli Stati membri provvederanno affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT eventuali incidenti che abbiano un impatto significativo sulla fornitura dei loro servizi. Se opportuno,[35] tali soggetti notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti che possono

35. La valutazione di opportunità sembra, al momento, non orientata da criteri uniformi e potrebbe, pertanto, dare luogo a difformità di applicazione, pur dovendosi necessariamente riferire alla nozione di impatto significativo.

ripercuotersi negativamente sulla fornitura di tali servizi. Gli Stati membri provvederanno, altresì, affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta alle autorità competenti o al CSIRT di determinare l'eventuale impatto transfrontaliero dell'incidente.

> Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT qualunque minaccia informatica significativa che, secondo tali soggetti, avrebbe potuto causare un incidente significativo.[36]

Sempre "se opportuno", tali soggetti notificheranno senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che è possibile adottare in risposta a tale minaccia (nonché la minaccia stessa). La rassicurazione per cui tale notifica non esporrà il soggetto che la effettua a una maggiore responsabilità, sembra essere disposta allo scopo di favorire la più ampia condivisione e incoraggiare la promozione e adozione di una migliore trasparenza nelle prassi applicative di diritto vivente.

In particolare, gli Stati membri sono chiamati a provvedere affinché, ai fini della notifica, i soggetti interessati trasmettano alle autorità competenti o al CSIRT:

a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, una notifica iniziale che indichi se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola;
b) su richiesta di un'autorità competente o di un CSIRT, una relazione intermedia sui pertinenti aggiornamenti della situazione;

36. Confermando così l'ottica fortemente preventiva della tutela prevista.

c) una relazione finale entro un mese dalla trasmissione della notifica di cui alla lettera a), che comprenda almeno:
   i) una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto;
   ii) il tipo di minaccia o la causa che ha innescato l'incidente;
   iii) le misure di attenuazione adottate e in corso di adozione.

La previsione per cui gli Stati membri dispongono che, in casi debitamente giustificati e con l'accordo delle autorità competenti o del CSIRT, il soggetto interessato possa derogare alle scadenze di cui alle lettere a) e c), pur nella consapevolezza della necessità di mantenere alcuni margini di discrezionalità, desta qualche perplessità in chi scrive rispetto agli obiettivi di uniformità degli ordinamenti nazionali.

10. La nozione di 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, nella attuale formulazione, 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 guar-

dare 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.

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.[37]

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

37. 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.

le sue responsabilità, anche quella di trasmettere mensilmente all'ENISA una 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.

11. Le misure di sicurezza tra quadri e strategie

Come già evidenziato in apertura di questo contributo, la disciplina di revisione della direttiva NIS ha disposto in tema della necessità, per ogni Stato membro, dell'elaborazione e adozione di una strategia nazionale per la *cybersecurity*, come cornice fondamentale idonea all'individuazione e applicazione delle misure di sicurezza più efficaci in tale ambito. In

particolare, ogni Stato membro dovrà adottare una strategia nazionale per la *cybersecurity* che definisca obiettivi strategici e adeguate misure strategiche e normative[38] al fine di raggiungere e mantenere un livello elevato di sicurezza *cyber*. La strategia nazionale per la *cyber* sicurezza comprenderà, secondo la lettera della norma, gli elementi seguenti:

a) una definizione degli obiettivi e delle priorità della strategia per la *cybersecurity* dello Stato membro;
b) un quadro di *governance* per la realizzazione di tali obiettivi e priorità, individuando misure strategiche, ruoli e responsabilità degli enti e degli organismi pubblici, nonché di altri attori pertinenti;
c) una valutazione volta a individuare le risorse e rischi di *cybersecurity* pertinenti nello Stato membro;
d) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti, la collaborazione tra i settori pubblico e privato.[39]

Nell'ambito della strategia nazionale per la sicurezza *cyber*, gli Stati membri saranno, inoltre, chiamati a realizzare:

a) misure relative alla *cybersecurity* nella catena di approvvigionamento dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione (TIC) utilizzati da soggetti essenziali e importanti per la fornitura dei loro servizi;

38. Sulla particolare categoria delle misure normative sembra opportuno richiamare l'attenzione per evidenziare che le sole misure tecniche rischiano spesso di essere insufficienti alla generale *compliance* in tema di *cybersecurity*.

39. Anche in questo caso ritorna, in maniera evidente, l'impostazione del modello del ciclo di Deming insieme alle assonanze che ne discendono rispetto all'impostazione di un *Information Security Management System* (ISMS) e di un *Business Security Management System* (BSMS) con attenzione alla continuità operativa.

b) orientamenti relativi all'inclusione e alla definizione di requisiti relativi alla *cybersecurity* per i prodotti e i servizi TIC negli appalti pubblici;
c) misure volte a promuovere e a facilitare la divulgazione coordinata delle vulnerabilità;
d) misure relative al sostegno della disponibilità generale e dell'integrità del carattere fondamentale pubblico di una rete Internet aperta;
e) misure volte a promuovere e sviluppare competenze, attività di sensibilizzazione e iniziative di ricerca e sviluppo in materia di sicurezza *cyber*;
f) misure per sostenere gli istituti accademici e di ricerca nello sviluppo di strumenti di *cybersecurity* e di infrastrutture di rete sicure;[40]
g) misure, procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni tra imprese, nel rispetto del diritto dell'Unione;
h) misure volte a rispondere alle esigenze specifiche delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, relativamente a orientamenti e sostegno per rafforzare la loro resilienza alle minacce alla sicurezza *cyber*.

Aspetto della rilevanza tutt'altro che relativa è ancora quello legato alla gestione delle eventuali crisi che dovessero discendere da incidenti significativi e di una certa estensione. Da questo punto di vista ogni Stato membro designerà una o più autorità competenti responsabili della gestione delle crisi e degli inciden-

40. Si noti che nella forma entrata in vigore e pubblicata in Gazzetta Ufficiale gli istituti accademici e di ricerca sono formalmente inclusi tra gli altri settori critici come da allegato II.

ti su vasta scala. Gli ordinamenti nazionali, a questo fine, saranno responsabili affinché le autorità competenti dispongano di risorse adeguate a svolgere i compiti loro assegnati in modo efficace ed efficiente in relazione a queste particolari circostanze. Ogni Stato membro individuerà, pertanto, le capacità, le risorse e le procedure che potranno essere impiegate in caso di crisi ai fini della nuova disciplina NIS II e, al medesimo scopo, dovrà elaborare e adottare un piano nazionale di risposta agli incidenti e alle crisi di *cybersecurity* in cui siano stabiliti gli obiettivi e le modalità della gestione delle crisi e degli incidenti di sicurezza *cyber* su vasta scala. La norma si cura di stabilire anche i contenuti necessari del piano in parola, individuando, in particolare:

a) gli obiettivi delle misure e delle attività nazionali di preparazione;
b) i compiti e le responsabilità delle autorità nazionali competenti;
c) le procedure di gestione delle crisi e i canali di scambio delle informazioni;
d) le misure di preparazione, comprese le esercitazioni e le attività di formazione;
e) le parti afferenti al settore pubblico e privato e le infrastrutture coinvolte;
f) le procedure nazionali e gli accordi tra organismi e autorità nazionali al fine di garantire il sostegno efficace dello Stato membro alla gestione coordinata delle crisi e degli incidenti di *cybersecurity* su vasta scala a livello dell'Unione e la sua effettiva partecipazione a tale gestione.

Definito il piano, sulla base di questi contenuti minimi, gli Stati membri comunicheranno alla Commissione le autorità com-

petenti designate alla gestione degli eventi di crisi e trasmetteranno i propri piani nazionali di risposta agli incidenti e alle crisi di *cybersecurity* entro tre mesi. Quale clausola di riserva conclusiva, il diritto dell'Unione si premura di specificare che gli Stati membri potranno omettere dal piano informazioni specifiche se, e nella misura in cui, ciò sia strettamente necessario ai fini della sicurezza nazionale.

12. Misure di gestione dei rischi di *cybersecurity* in Europa

Ai fini della gestione dei rischi di *cybersecurity*, la direttiva NIS II invita gli Stati membri a provvedere affinché i soggetti essenziali e importanti adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che essi utilizzano nella fornitura dei loro servizi. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicureranno un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio[41] esistente. Le misure comprenderanno almeno[42] i seguenti elementi:

a) analisi dei rischi e politiche di sicurezza dei sistemi informatici;
b) gestione degli incidenti (prevenzione e rilevamento degli incidenti e risposta agli stessi);
c) continuità operativa e gestione delle crisi;

41. In stretta corrispondenza alla nozione di incidente significativo e i criteri stabiliti per identificarlo, la norma afferma che: «Ai fini della presente direttiva, il termine "rischio" dovrebbe riferirsi alla potenziale perdita o perturbazione causata da un incidente di *cybersecurity* e dovrebbe essere espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi tale incidente».

42. Confermando, quindi, che il catalogo seguente è da intendersi come dedicato alle misure "minime".

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi fornitori o fornitori di servizi, quali quelli relativi alla conservazione ed elaborazione dei dati o di servizi di sicurezza;[43]
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure (test e audit) per valutare l'efficacia delle misure di gestione dei rischi di *cybersecurity*;
g) uso della crittografia e della cifratura.

13. Per concludere? Alcune questioni aperte

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 all'approvazione e adozione definitiva (ed esatta) 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

43. Guardando al considerando n. 85 si comprende che affrontare i rischi di *cybersecurity* derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono rimasti vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti dovrebbero pertanto valutare e tenere in considerazione la qualità complessiva dei prodotti e delle pratiche di sicurezza *cyber* dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

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.[44]

44. Ci troviamo nell'ambito delle tre direttrici 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

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?

Altro tema di interesse è quello che si lega alle possibili valutazioni qualitative in termini di proporzionalità, effettività ed efficacia. Nelle intenzioni del legislatore europeo le norme proposte nella direttiva non si muovono oltre a quanto è necessario per raggiungere in modo soddisfacente gli obiettivi specifici. D'altra parte, bisogna ricordare che la necessità di un allineamento e di una razionalizzazione in tema di misure di sicurezza e degli obblighi di segnalazione sono da considerarsi, in parte, anche un riscontro alle richieste degli Stati membri e delle imprese ivi stabilite per migliorare il quadro attuale. La proposta, tenendo conto delle pratiche già esistenti negli Stati membri, mira ad ottenere così un livello maggiore di protezione conseguito grazie a misure razionalizzate e coordinate, come quelle sin qui esaminate, proporzionale ai rischi sempre più elevati affrontati, compresi quelli che presentano un elemento transfrontaliero. Esse saranno effettivamente ritenute ragionevoli

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)». Brighi 2021: 147.

e corrisponderanno agli interessi dei soggetti coinvolti nel garantire la continuità e la qualità dei loro servizi? 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*?
Concludendo quindi questa analisi guardando ad 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 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. La proposta sostituisce, inoltre, il complesso sistema di identificazione degli operatori di servizi essenziali con obblighi generali, introducendo – opportunamente – un livello più elevato di armonizzazione degli obblighi di sicurezza e di segnalazione, che sembrerebbe quindi capace di ridurre gli oneri spesso elevati della conformità, in particolare per i soggetti che forniscono servizi transfrontalieri. La proposta tenta, altresì, una riduzione al minimo dei costi di conformità per le PMI,

in quanto i soggetti rilevanti saranno tenuti ad adottare solo le misure necessarie a garantire un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio presentato.
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.

Riferimenti bibliografici

Aterno, S. 2022. *Sicurezza informatica. Aspetti giuridici e tecnici*. Pisa: Pacini Editore.

Buffa, M. 2022. "Didattica del diritto e cultura giuridica nell'educazione (in)attuale. Note a margine di un recente manuale." *Materiali per una storia della cultura giuridica* 1.

Casadei, T. e Pietropaoli, S. eds. 2021. *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*. Padova: Cedam giuridica.

Castignone, S., Faralli, C. e Ripoli, M. eds. 2002. *Il diritto come profezia. Il realismo americano: antologia di scritti*. Torino: Giappichelli.

Contaldo, A. e Peluso, F. 2018. *Cybersecurity: la nuova disciplina italiana ed europea alla luce della direttiva NIS*. Pisa: Pacini giuridica.

D'Avanzo, W. 2020. *Il diritto di fronte alle sfide del futuro. Studi di informatica giuridica e dritto dell'informatica*. Mantova: Universitas Studiorum.

Fanlo Cortés, I. e Ferrari, D. eds. 2020. *I soggetti vulnerabili nei processi migratori, la protezione internazionale tra teoria e prassi*. Torino: Giappichelli.

Ferruglio, M. 2018. "Cyber operation e responsabilità internazionale degli stati: uno sguardo d'insieme." In Ivaldi, P. e Carrea, S. eds. *Lo spazio cibernetico. Rapporti giuridici pubblici e privati nella dimensione nazionale e transfrontaliera*. Genova: Genova University Press.

Guastini, R. 2013. "Il realismo giuridico ridefinito." *Revus, European Constitutionality Review* 10/1.

Ivaldi, P. e Carrea, S. eds. 2018. *Lo spazio cibernetico. Rapporti giuridici pubblici e privati nella dimensione nazionale e transfrontaliera*. Genova: Genova University Press.

Maestri, E. 2015. *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*. Napoli: Edizioni Scientifiche Italiane.

Marzocco, V., Zullo, S. e Casadei, T. 2021. *La didattica del diritto. Metodi, strumenti e prospettive*. Pisa: Pacini.

Moro, P. e Sarra, C. eds. 2017. *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*. Milano: FrancoAngeli.

Panzani, L. 2017. "Forum shopping e abuso del diritto." *Il nuovo diritto delle società* 10. Torino: Giappichelli.

Rinaldi, S.M., Peerenboom, J.P. e Kelly, T.K. 2002. "Identifying understanding and analyzing critical infrastructures interdependencies." *IEEE Control Systems Magazine*.

Schön, D.A. 1983. *The reflective practitioner. How professionals think in action*. New York: Basic books.

Setola, R. 2011. *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*. Rapporto di ricerca. Centro Militare di Studi Strategici.

Shackelford, S.J. e Andres, R.B. 2011. "State responsibility for cyber-attacks: competing standards for a growing problem." *Georgetown journal of International Law*.

Tarello, G. 1962. *Il realismo giuridico americano*. Milano: Giuffré.

Vantin, S. 2021. *Il diritto antiscriminatorio nell'era digitale. Potenzialità e rischi per le persone, la pubblica amministrazione, le imprese*. Milano: Wolters Kluwer Italia.

Siti consultati

https://www.csirt.gov.it/

https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Nuove-norme-sulla-protezione-delle-infrastrutture-critiche-nellUE_it

https://www.enisa.europa.eu/topics/nis-directive

Nota editoriale

Il presente contributo include riflessioni più ampie di quelle che l'autore ha svolto, sullo stesso tema, in Buffa M., *La direttiva NIS II. Cybersecurity in Europa: tra innovazione, formazione e diritto vivente*, in "Democrazia e diritti sociali, Rivista telematica di Filosofia del diritto", I/2023, e-ISSN 2610-9166, pubblicato in pari data.