ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

25 SETTEMBRE 2024

Giustizia digitale: sicurezza?

di Fabio Gaggero
Dottorando di ricerca in *Security Risk and Vulnerability*
Università degli studi di Genova

Giustizia digitale: sicurezza?*

di Fabio Gaggero
Dottorando di ricerca in *Security Risk and Vulnerability*
Università degli studi di Genova

Abstract [It]: Partendo dall'incipit della recente riforma della giustizia, il presente contributo vuole dare una lettura a caldo alla direttiva NIS2. L'approccio *digital by design* imposto dal legislatore a tale settore deve accompagnarsi ad una *security by design*. Nonostante il sistema NIS abbia visto un ampliamento del suo ambito di applicazione, la giustizia rimane ancora fra i settori esclusi.

Title: Digital justice: security?
Abstract [En]: This contribution aims to provide a critical analysis of the recent justice reform and its implications for the NIS2 directive. It argues that the digital by design approach imposed by the legislator on this sector must be accompanied by security by design. Despite the extension of the NIS system's scope, justice remains among the excluded sectors.

Parole chiave: cybersecurity, giustizia, NIS, servizi digitali, digitalizzazione
Keywords: cybersecurity, justice, NIS, digital services, digitization

1. Un'introduzione di contesto: cosa manca alla giustizia?

Ormai da diversi anni il concetto di digitalizzazione sta accompagnando il processo di rinnovamento della giustizia. Il dibattito interno fornisce molteplici spunti di trattazione, che toccano i diversi settori processuali. Seppur a diverse velocità, ciascuno di questi è stato plasmato dalla progressiva introduzione delle nuove tecnologie.

Anche se il pensiero va immediatamente alla riforma Cartabia, i cui esordi stanno dando i primi frutti[1], i primi segni di smaterializzazione dei documenti potevano essere riscontrati già nel Codice dell'Amministrazione Digitale, almeno sotto forma di principi.

* Articolo sottoposto a referaggio. This work was partially funded by the Next Generation EU project «Security and Rights in CyberSpace» (SERICS).

1 Vista la sede mi limito a rimandare a F. RUSSO, *Novità in tema di processo civile telematico*, in *Il giusto processo civile*, n. 1, 2023, pp. 85–113; M. GIALUZ, *Riforma Cartabia: modifiche strutturali al processo penale - Le disposizioni generali sulle impugnazioni e l'appello*, in *Giurisprudenza italiana*, n. 5, 2023, pp. 1209–11; P. TONINI, *Le nuove tecnologie e la riforma Cartabia*, in *Diritto penale e processo*, n. 3, 2022, pp. 293–97. Al momento in cui si scrive non mancano però i problemi di applicazione. Per una rassegna recente in ambito civile si veda I. FERRANTI, *Ma quale riforma della giustizia digitale civile, i tribunali sono ancora in ritardo*, in *Agenda Digitale*, 7 giugno 2023; I. FERRANTI, *Processo civile telematico Giudice di pace, il caos Cartabia*, in *Agenda Digitale*, 3 ottobre 2023.

Proprio su quelle prime componenti essenziali, costituite dalla normativa in materia di documenti digitali e di firme elettroniche, si regge il funzionamento del deposito telematico degli atti processuali.

Anzi è più corretto parlare al plurale di «processi telematici»[2] che sono stati via via introdotti, a riprova del fatto che di digitalizzazione del processo si è sempre parlato.

Bisogna poi tenere in considerazione la forte accelerazione apportata dalla pandemia di COVID-19, che può essere letta in continuità con la successiva entrata in vigore della Cartabia.

Senza alcuna presunzione di completezza riguardo a tematiche giusprocessualistiche, la cui dignità richiederebbe una più attenta e completa disamina, è però opportuno cogliere quelli che sono i minimi comuni denominatori di quella complessiva direzione verso la quale la giustizia italiana si sta muovendo.

In primo luogo, digitalizzare significa smaterializzare gli atti alla base del processo. Non si tratta solo di abbandonare il formato cartaceo, ma di predisporre le condizioni per sfruttare le potenzialità di analisi rese possibili dal formato digitale, il quale deve essere leggibile attraverso strumenti automatizzati. Da una parte, implica la digitalizzazione del precedente patrimonio giudiziario, ancora detenuto su supporto fisico. Dall'altra l'intero processo telematico dovrà essere predisposto per accogliere by default una digitalizzazione compiuta, ordinata e moderna. Vi è l'occasione di ripensare la struttura degli atti giudiziari, secondo una logica rigida e schematica, che dovrebbe ricordare quella della Rule 74 del regolamento della Corte EDU[3]. Le ripercussioni sono molteplici, a partire dal modo di ragionare del giurista, che sarà destinato a cambiare, rinunciando agli eccessi e alle formule di stile che lo hanno da sempre contraddistinto. Tale passaggio «dai documenti ai dati»[4] è stato sancito dalla riforma Cartabia, la quale è intervenuta per introdurre il potere del Ministro della giustizia di definire mediante suo decreto «gli schemi informatici degli atti giudiziari con la strutturazione dei campi necessari per l'inserimento delle informazioni nei registri del processo»[5]. Si inaugura una nuova fase del processo, nella quale la decisione non è più il risultato degli atti delle parti, ma, più precisamente, delle informazioni in essi contenuti.

2 Il Sole 24 ORE aveva riassunto questa disordinata evoluzione della giustizia attraverso la costruzione di una cronistoria dei «processi telematici». Si rimanda a V. MAGLIONE e B.L. MAZZEI, *Processi telematici, 7 piattaforme: è la babele della giustizia online*, *Il Sole 24 ORE*, 8 aprile 2021. A partire dal 2014 con il processo civile telematico, si sono poi aggiunti il processo contabile nel 2016, il processo amministrativo nel 2017, quello tributario nel 2019 e quello penale nel 2020, attraverso la normativa di emergenza. Si aggiungono oggi anche il processo telematico di fronte alla Corte di Cassazione e il processo telematico di fronte alla Corte costituzionale, rispettivamente dal 31 marzo 2021 e dal 3 dicembre 2021. Si veda a questo proposito E. SAMMACICCIO, *La Corte e il processo telematico: valutazioni e prospettive dopo la pandemia*, in *Consulta Online*, n. 2, 2022, pp. 864–74.

3 Si rimanda ai ragionamenti di A. SANTOSUOSSO, *Una Giustizia "digital by design": ecco come realizzarla*, in *Agenda Digitale*, 21 giugno 2021.

4 Si rimanda a Amedeo Santosuosso, *Un cambio epocale nella giustizia italiana: dai documenti ai dati*, in *Agenda Digitale*, 15 giugno 2023.

5 Si confronti la nuova formulazione dell'art. 46 delle disposizioni di attuazione del codice di procedura civile. Il primo decreto è il D.M. 7 agosto 2023, n. 110, pubblicato in Gazzetta Ufficiale 11 agosto 2023, n. 187.

Lo scenario apre la strada all'utilizzo di strumenti basati sull'IA. Il tema è quello della cosiddetta decisione algoritmica, al quale è stata dedicata negli ultimi anni una discreta produzione scientifica, in particolare per quanto concerne la giustizia amministrativa. L'ambito è già stato esplorato sotto molteplici prospettive, dalla responsabilità dell'amministrazione[6] ai requisiti di trasparenza e spiegabilità dell'algoritmo[7]. Gli impatti non sono certamente secondari perché vengono messi in discussione sia il principio di legalità[8], che il diritto ad un equo processo[9].

Una seconda prospettiva implicita al fenomeno della digitalizzazione in ambito giudiziario è quindi quella strettamente legata alle procedure. La volontà del legislatore di perseguire un sistema che sia digital by *design* ha come prima conseguenza la necessità di un adattamento, che deve essere supportato dalla creazione di apposite piattaforme digitali.

L'attuale organizzazione, aspramente criticata dall'avvocatura, vede l'esistenza di più di sette piattaforme differenti per il deposito degli atti introduttivi, con la creazione di un eccessivo carico burocratico.

Nonostante l'opportunità costituita per l'Italia dai fondi del PNRR, a distanza di oltre due anni dall'approvazione del piano nazionale di ripresa e resilienza non si riscontrano risultati concreti per l'ammodernamento della giustizia. La stessa Commissione Giustizia presso la Camera dei Deputati aveva dato parere positivo ai progetti di riforma, apprezzando i forti stanziamenti dedicati, almeno sulla carta, alla prima missione in materia di digitalizzazione. Questa dovrebbe essere la risposta giusta per il perseguimento di un'accelerazione dei tempi della giustizia.

Fra i diversi punti figurava il completamento della digitalizzazione del processo civile e penale, ma la Commissione Giustizia aveva perfettamente colto le più profonde necessità di rinnovamento, auspicando un perfezionamento del processo di digitalizzazione in tutti i settori della giustizia. In particolare, veniva ipotizzata la «implementazione di una rete esclusivamente dedicata al sistema giustizia con elevati standard di sicurezza»[10].

6 M.C. CAVALLARO e G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, n. 16, 2019, p. 7.

7 Quella dell'esplicabilità e della motivazione a seguito dell'azione algoritmica è una delle questioni più ricorrenti e più battute. Vista la densità delle questioni che sono scaturite dal dibattito, che sarebbe fuori luogo in questa sede, si consenta il rinvio ai più. Si vedano A. CORRADO, *La trasparenza necessaria per infondere fiducia in una amministrazione algoritmica e antropocentrica*, in *Federalismi.it*, n. 5, 2023, pp. 175–215; C. COLAPIETRO, *Gli algoritmi tra trasparenza e protezione dei dati personali*, in *Federalismi.it*, n. 5, 2023, pp. 151–74; T. ALTÌ e M.C. BARBIERI, *La trasparenza amministrativa come strumento di potere e di democrazia*, in *Rivista trimestrale di diritto pubblico*, n. 2, 2023, pp. 809–31; S. ARDUINI, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal - Rivista di BioDiritto*, n. 2, 2021, pp. 453–70; G. SCHNEIDER, *Accesso all'algoritmo pubblico sviluppato da terzi e questioni di riservatezza nell'amministrazione digitale*, in *AIDA*, n. 2, 2021, pp. 920–34; E. TROISI, *Decisione algoritmica, "Black-Box" e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, in *Jus Civile*, n. 4, 2022, pp. 953–75.

8 P. OTRANTO, *Riflessioni in tema di decisione amministrativa, intelligenza artificiale e legalità*, *in Federalismi.it*, n. 7, 2021, pp. 187–204.

9 J. SACCOMANI, *L'impatto della giustizia algoritmica sul diritto all'equo processo*, in *Cassazione penale*, n. 2, 2023, pp. 628–45.

10 Camera dei Deputati, *Proposta di Piano Nazionale di ripresa e resilienza. Doc. XXVII, n. 18.*, 23 marzo 2021, 66–67.

Proprio quest'ultima osservazione della commissione consente di introdurre un tema tanto importante quanto ignorato, qual è quello della sicurezza. L'attenzione del dibattito viene spesso distratta da tematiche più strettamente inerenti all'ambito del diritto, perdendo di vista quello che ormai è una condizione necessaria, ma non sufficiente per l'esercizio dei diritti, soprattutto se di giustizia si tratta.

La creazione di una piattaforma unica e di una rete dedicata potranno certamente agevolare l'esercizio dei diritti, ma diventeranno anche un requisito imprescindibile. Il prezzo dell'innovazione è quello di doversi muovere alla sua velocità, nella consapevolezza che il suo utilizzo espone inevitabilmente ad una nuova serie di minacce.

Gli attacchi informatici contro il Consiglio Superiore della Magistratura e altre istituzioni centrali in concomitanza con la visita a Roma del presidente Ucraino ne sono la prova[11].

Il recente completamento del Perimetro di Cybersicurezza nazionale assieme alla creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) sono stati traguardi fondamentali sotto il profilo della semplificazione dell'esistente sistema per la cybersecurity[12]. Nell'ambito di questo si collocano anche tutti quei soggetti che abbiano il compito di assicurare la continuità dell'amministrazione della giustizia, poiché svolgono una funzione essenziale dello Stato[13]. Grazie a questo rinnovato contesto, il legislatore nazionale ha ora a disposizione nuovi strumenti per garantire la costruzione di un sistema digitale sicuro per l'ecosistema processuale, alla luce del principio di security by *design*.

Trascurando il ritardo che caratterizza l'attuazione del PNRR, i prossimi anni potrebbero essere un periodo particolarmente fecondo per il completamento della digitalizzazione del paese, per via di un'interessante convergenza d'intenti.

All'attenzione posta sul piano interno, corrisponde infatti la rinnovata attenzione da parte delle istituzioni europee, le quali stanno proseguendo con l'attuazione della strategia europea per la cybersicurezza.

Una nuova opportunità per incrementare la sicurezza delle procedure potrebbe derivare dalla nuova direttiva NIS2. Certamente il suo ambito di applicazione non interesserà la giustizia, nonostante il marcato

11 Redazione RHC, *Attacco informatico al Ministero dell'interno e al CSM da parte degli hacktivisti filorussi*, in *Red Hot Cyber* , 13 maggio 2023.

12 Il presente contributo tralascia l'analisi del quadro legislativo nazionale, che ha visto importanti cambiamenti negli ultimi anni. Si consenta il rinvio alle più complete trattazioni di I. FORGIONE, *Il Ruolo Strategico Dell'agenzia Nazionale per La Cybersecurity Nel Contesto Del Sistema Di Sicurezza Nazionale: Organizzazione e Funzioni, Tra Regolazione Europea e Interna*, in Diritto Amministrativo, n. 4, 2022, pp. 1113–43; E. RAFFIOTTA, *Cybersecurity Regulation in the European Union and the Issues of Constitutional Law*, in *Rivista AIC*, n. 4, 2022, pp. 10-13; F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, n. 12, 2022, pp. 244-268.

13 Anche se la lista di soggetti identificati per l'inserimento nel Perimetro nazionale non è soggetta a pubblicazione, in quanto contenuta in un DPCM secretato, è facile ipotizzare che chiunque gestista un'infrastruttura, una piattaforma o un componente, che rende possibile i servizi digitali della giustizia, sia, in gergo, un «soggetto perimetrato». Si confrontino gli articoli 3 e 4 del DPCM 30 luglio 2020, n. 131, letti in combinato disposto con le modifiche apportate dal d.l. 14 giugno 2021, n. 82, per via dell'istituzione dell'ACN.

ampliamento dell'ambito di applicazione[14]. Per quanto molte aperture nella direttiva lascino al legislatore la possibilità di nuove inclusioni, è giustificato che un settore delicato quale quello dell'amministrazione della giustizia goda di particolari attenzioni. Nonostante questo, il legislatore nazionale dovrebbe cogliere l'occasione della trasposizione della nuova normativa europea al fine di trarre utili principi di funzionamento da implementare in maniera sinergica anche nel settore della giustizia.

Vista l'ormai imprescindibile necessità di un dibattito riguardo alla sicurezza del sistema giudiziario, si propone un commento al testo della nuova direttiva, che il legislatore nazionale dovrà recepire entro il 17 ottobre 2024. Nei paragrafi che seguono verranno brevemente delineate le ragioni che hanno portato all'emendamento, partendo dai commenti e dalle impressioni raccolte dalla Commissione europea.

2. La strada verso la NIS2

Nonostante l'Unione europea nutrisse grandi speranze nel sistema NIS, a meno di un anno di distanza dalla scadenza data per l'implementazione, fissata per il 9 Maggio 2018, la Commissione cominciava a far trasparire i suoi dubbi. In un'analisi in corso d'opera veniva sottolineato come gli sforzi implementativi dovessero necessariamente andare al di là dei requisiti minimi imposti dalla direttiva per conseguire un approccio realmente olistico. La cybersecurity è un settore relativamente nuovo ed in rapida evoluzione. Di conseguenza vanno adottate decisioni ambiziose che consentano alle misure in materia di sicurezza di integrarsi e di diventare strutturali.

Gli Stati membri dovevano puntare a migliorare la propria reattività, ma la grande varietà di approcci e la spesso grande decentralizzazione adottata a livello nazionale rischiavano di vanificare gli sforzi. Il sistema dei punti di contatto meritava un potenziamento, mentre al contempo si consigliava un ampliamento dell'ambito di applicazione per coprire altri settori essenziali, in particolare quello della pubblica amministrazione.

Nonostante le raccomandazioni per un efficace recepimento, l'efficacia complessiva dell'intervento deve essere esaminata, senza minimizzarne i risultati positivi. Certamente deve essere riconosciuto come la direttiva avesse gettato le basi per delle solide capacità di cybersicurezza a livello nazionale, sia attraverso l'imposizione di strategie nazionali, che attraverso la creazione di autorità nazionali. La predisposizione di organismi competenti aveva semplificato la gestione dei rapporti sia all'interno dei singoli stati membri, che fra stati membri. Inoltre, sulla base di questa organizzazione comune erano stati creati due nuove

14 L'aspetto più innovativo della nuova normativa sta proprio nella rivisitazione dell'ambito di applicazione, come si avrà modo di analizzare. Tra i principali ampliamenti c'è la volontà di includere tutta la pubblica amministrazione centrale e regionale, individuata sulla base della definizione data dalla legge nazionale. La stessa definizione di pubblica amministrazione, dopo aver dato alcuni criteri identificativi, fa espressa eccezione rispetto al sistema giudiziario, al parlamento e alla banca centrale. Si confrontino l'articolo 2 par. 2 let. f) e l'articolo 6 n. 35 della direttiva (UE) 2022/2555.

organi di supporto a livello europeo, il Gruppo di Cooperazione e la rete di CSIRT, che avevano contribuito alla creazione e alla disseminazione di pratiche comuni.

In questo modo, si era migliorato il livello di armonizzazione e si era costituita una solida base per poter discutere di questioni legate alla regolamentazione della cybersecurity. Ad esempio, il gruppo di cooperazione aveva contribuito in maniera importante alla sicurezza del 5G, durante gli sviluppi del cosiddetto 5G *toolbox*. Sempre riguardo a nuovi organi europei, non vanno inoltre trascurate le attività del *Cyber Crises Liaison Organisation Network* («CyCLONe»), benché inizialmente avesse solo un ruolo informale, nell'ambito del più ampio disegno di un *blueprint* per la rapida risposta alle emergenze.

La valutazione finale di implementazione iniziava con il prendere atto del mutato scenario, caratterizzato da un'espansione delle minacce potenziali e da una rapida digitalizzazione, ulteriormente marcata a causa della domanda di servizi digitali dovuta alla recente esperienza pandemica del COVID-19. Da quel momento una gran parte della vita sociale e professionale si era spostata nel cyberspazio, creando nuovi ed immediati bisogni.

«Risposte politiche più avanzate nel campo della sicurezza informatica sono diventate una questione urgente, poiché il numero di attacchi informatici continua ad aumentare, con attacchi sempre più sofisticati provenienti da un'ampia gamma di fonti all'interno e all'esterno dell'UE»[15]. Quelli che inizialmente erano incidenti causati da cause naturali oppure da organizzazioni criminali si sono trasformati in veri e propri atti di cyber war, perpetrati da agenti statali.

La cybersecurity è diventata una delle priorità trasversali dell'Unione europea nell'ambito delle nuove strategie per il mercato unico digitale. Il parlamento europeo nel 2016, parallelamente agli interventi a supporto della digitalizzazione del mercato, auspicava un forte miglioramento della cyber-resilienza, attraverso un ruolo più incisivo dell'ENISA[16] e dei CERT nazionali[17], la cui creazione doveva essere accelerata. In generale, i discorsi in materia di resilienza erano accompagnati dal radicamento di un principio di security by *design* che mirava a rovesciare la tradizionale logica di un intervento ex post, in caso di riscontate vulnerabilità[18].

15 Traduzione libera. Si rimanda a European Commission, *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148*, 16 dicembre 2020 consultabile qui.

16 European Parliament, *European Parliament Resolution of 19 January 2016 on Towards a Digital Single Market Act*, 19 gennaio 2016, p. 21, consultabile qui.

17 European Parliament, *European Parliament Resolution of 3 October 2017 on the Fight against Cybercrime*, 3 ottobre 2017, p. 11, consultabile qui.

18 *Ibid.* p. 11.

Già nel 2019 la Commissione era stata invitata a valutare la necessità di allargare ulteriormente l'ambito di applicazione della direttiva NIS per coprire altri settori critici[19]. Quest'invito era stato tenuto in considerazione nell'elaborazione dei progetti su «*Shaping Europe's digital future*». «La sovranità tecnologica europea parte dalla garanzia dell'integrità e della resilienza delle nostre infrastrutture di dati, reti e comunicazioni. È necessario creare le condizioni giuste affinché l'Europa possa sviluppare e impiegare le proprie capacità chiave, riducendo così la nostra dipendenza da altre parti del mondo per le tecnologie più importanti»[20].

Per questo motivo, fra le altre iniziative, veniva auspicata una nuova strategia per la cybersicurezza[21], fra i cui obiettivi principali c'è proprio la riforma del sistema NIS.

Lo stesso ordine di priorità era condiviso anche dal Consiglio dell'Unione europea che aveva accolto con favore le posizioni della Commissione[22] auspicando un'accelerazione dello sviluppo sicuro delle infrastrutture di rete di ultima generazione[23] e una revisione delle altre normative settoriali, in particolar la predisposizione di un intervento per introdurre requisiti minimi di sicurezza dei dispositivi connessi alla rete[24].

2.1. La valutazione della prima direttiva NIS

Sulla base di questo coordinamento d'intenti, si erano esaminati con attenzione i risultati della prima direttiva, al fine di progettare i futuri interventi di riforma, come del resto previsto dall'articolo 23 della stessa direttiva NIS[25]. La valutazione portata avanti dalla Commissione e allegata alla nuova direttiva si era basata sulla somministrazione di questionari ai diversi stakeholders. Le risposte avevano fatto emergere alcune principali mancanze, ulteriormente raggruppate in alcune problematiche[26].

19 European Parliament, *European Parliament Resolution of 12 March 2019 on Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them (2019/2575(RSP))*, 12 marzo 2019, p. 4,consultabile qui.

20 European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future*, 19 febbraio 2020, p. 2, consultabile qui.

21 *Ibid.*, p. 7.

22 Council of the European Union, *Council Conclusions on Shaping Europe's Digital Future*, 16 giugno 2020, p. 6, consultabile qui.

23 Council of the European Union, *Special Meeting of the European Council (1 and 2 October 2020) – Conclusions*, 2 ottobre 2020, p. 4, consultabile qui.

24 Council of the European Union, *Council Conclusions on the Cybersecurity of Connected Devices - Council Conclusions Approved by Written Procedure*, 2 dicembre 2020, p. 6, consultabile qui.

25 Per un'analisi del quadro precedente si rimanda a M. SALAMONE E V. DI LUCA, *La Disciplina Del "Cyberspace" Alla Luce Della Direttiva Europea Sulla Sicurezza Delle Reti e Dell'informazione: Contesto Normativo Nazionale Di Riferimento, Ruolo Dell'"intelligence" e Prospettive "de Iure Condendo"*, in *Federalismi.it*, n. 23, 2017, pp. 7-25; A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, n. 4, 2021, pp. 538–548.

26 Delle considerazioni che seguono è possibile trovare riscontro in European Commission, *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Proposal for a Directive of the*

In primo luogo, si poteva evidenziare il basso livello di resilienza raggiunto dalle imprese e più in generale da tutti i soggetti coperti dalla normativa, che si attestava solo ad un livello medio[27]. Anche se molte aziende avevano fatto progressi notevoli in pochissimi anni, il livello di resilienza dell'Unione europea rimaneva complessivamente basso, soprattutto in confronto ad altri paesi più avanzati.

Questo era ulteriormente aggravato dal rapido cambiamento dello scenario digitale. La principale ragione dietro queste mancanze era da ricercare nel limitato numero di settori coperto dalla normativa, che si traduceva in un minor numero di operatori sottoposti agli obblighi minimi di sicurezza.

Di conseguenza molti paesi avevano autonomamente deciso di estendere l'ambito di applicazione della normativa. Ritagliare un ambito di applicazione efficace è cruciale, vista la forte interconnessione fra i soggetti, che provoca esternalità difficilmente controllabili. Molte compagnie potrebbero non avere l'interesse a migliorare la propria postura di sicurezza sapendo di poter contare sulle spese per l'implementazione di misure di sicurezza sopportate da altri. La conseguenza è che chi non è soggetto alla normativa e dipende da soggetti che sono invece obbligati ad investire in sicurezza, non è a sua volta incentivato ad investire allo stesso modo, beneficiando della miglior protezione senza spese.

Il secondo problema, in parte legato al primo, era quello dell'esistenza di diversi livelli di resilienza tra i diversi Stati membri e i diversi settori. In altre parole, non solo è critico poter definire quali settori sono coperti dalla normativa, ma soprattutto quali operatori in quei settori sono tenuti in concreto ad osservare le obbligazioni.

Vanno pertanto considerate le inconsistenze nella procedura di identificazione degli operatori di servizi essenziali all'interno dello stesso settore, che portavano una stessa categoria di soggetti ad essere o non essere coperta dalla normativa a seconda dello stato membro.

Nonostante le autorità competenti in tutta l'Unione avessero identificato migliaia di soggetti pubblici o privati, permanevano importanti discrepanze nell'implementazione delle norme in materia di identificazione, che si traducevano in differenze di trattamento, talvolta anche piuttosto marcate. Queste non solo comportavano livelli eterogenei di cybersicurezza, ma anche limitazioni al mercato interno in particolare per quei soggetti operanti prevalentemente in maniera transfrontaliera, che dovevano farsi carico del surplus burocratico dovuto ai differenti requisiti[28].

European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148, pp. 15–29.

27 *Ibid*, p. 17.

[28] L'eterogeneità dei livelli di sicurezza è il risultato di un'iniqua distribuzione dei "costi" della cybersecurity fra i diversi soggetti privati. Anche se non è questo il contesto per approfondire le logiche di un mercato tanto complesso, è noto che esso sia caratterizzato da esternalità marcate. Basti ricordare come i costi della sicurezza siano totalmente a carico degli utenti finali, mentre i produttori di software o dispositivi di sicurezza non subiscano gli effetti negativi di un *breach* di sicurezza. Una possibile soluzione al fine di affermare una più equa distribuzione dei costi potrebbe essere ricercata nella dottrina che equipara la cybersecurity ad un bene pubblico. Si veda R. Brighi e P.G. Chiara, *La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto UE*, in *Federalismi.it*, n. 21, 2021, pp. 18–

Sotto una certa prospettiva, si trattava di uno spreco di risorse, investite in *compliance* e non in un vero e proprio incremento del livello di sicurezza. Senza contare come il controllo da parte delle autorità non avesse raggiunto un livello soddisfacente, tale da riuscire ad imporre il rispetto delle misure. Anche se in parte il problema è da attribuire ad una scelta di *design* della direttiva, certamente le differenti metodologie adottate dagli stati membri avevano acuito il problema.

L'esistenza di un procedimento di identificazione poteva essere efficace per garantire la resilienza delle infrastrutture critiche contro minacce non digitali, ma l'eccessiva frammentazione conseguita rendeva impossibile garantire un adeguato livello di protezione cyber, a causa delle innegabili interconnessioni esistenti fra i diversi soggetti.

Ovviamente queste osservazioni valevano solo per gli operatori di servizi essenziali e non anche per i fornitori di servizi digitali, per i quali non era necessaria una previa identificazione. Per quest'ultimi la complicazione non è tanto nella loro identificazione, ma nell'identificazione della giurisdizione alla quale sono sottoposti. Da una parte i fornitori di servizi digitali in più paesi dell'Unione devono essere sottoposti alla giurisdizione del paese nel quale hanno il proprio stabilimento principale. Dall'altra, qualora si tratti di fornitori non basati nell'Unione europea, la direttiva richiede loro la nomina di un rappresentante in uno degli stati membri, in modo da essere sottoposti alla giurisdizione di questo.

Il problema è che i fornitori non hanno nessun obbligo di avvisare l'autorità nazionale competente della nomina di un rappresentante. Per di più, sia per fornitori UE che per fornitori extra-UE, le stesse autorità nazionali non hanno sufficienti poteri per poter verificare in autonomia quali di essi siano effettivamente sottoposti alla propria giurisdizione.

Al di là delle difficolta di identificazione dei soggetti sottoposti alla normativa, vi era anche una complessità dovuta alle misure che questi erano tenuti ad implementare, a causa della grande discrezionalità lasciata agli stati membri. Le misure di sicurezza variavano considerevolmente, come anche le soglie per valutare la sussistenza dei criteri per l'inoltro della notificazione di incidente all'autorità competente. Inoltre, anche le procedure di notificazione avevano delle variazioni importanti.

Non essendoci alcuno standard preciso al quale potersi attenere, le stesse autorità nazionali nell'esercitare il proprio controllo, adottavano misure piuttosto diversificate, a parità di violazioni riscontrate. Le sanzioni variavano considerevolmente sia nella tipologia, che nella loro entità, ma erano per lo più disapplicate dalla maggior parte delle autorità, che erano restie alla loro applicazione. Questo rispecchiava per lo più il diverso livello di capacità cyber sviluppate dagli stati membri, nei quali vi erano anche differenti priorità politiche e disponibilità economiche allocate alla sicurezza.

42. Altri autori, invece, pongono maggiormente l'accento sull'importanza di un approccio collaborativo fra pubblico e privato. Si rimanda ad esempio a L. PREVITI, *Pubblici Poteri e Cybersicurezza: Il Lungo Cammino Verso Un Approccio Collaborativo Alla Gestione Del Rischio Informatico*, in *Federalismi.it*, n. 25, 2022, pp. 81–92.

Infine, il terzo problema che emergeva era relativo allo scarso livello di consapevolezza della situazione e alle conseguenti limitate capacità di risposta. Gli stati membri, infatti, non scambiavano fra loro informazioni sullo stato della sicurezza cyber e non possedevano nemmeno report completi, perché non vi erano canali strutturati per la collaborazione con il settore privato.

Gli stessi organi europei avevano fallito nel loro obiettivo di favorire scambi più efficienti, che erano rimasti invece limitati e piuttosto sporadici. Si era ancora lontani dall'introduzione di un approccio sistematico. Né il gruppo di cooperazione, la rete di CSIRT e nemmeno la Commissione erano in grado di analizzare con successo gli attacchi a livello europeo per definire i settori più a rischio in maniera comparata fra i diversi paesi. La causa principale di questa inefficienza era da ricercare nella generalità delle disposizioni della direttiva in materia di cooperazione, che, per via della loro astrattezza, avevano portato ad interpretare la collaborazione semplicemente come volontaria.

Di conseguenza solo pochissimi stati avevano fatto uso della procedura di consultazione transfrontaliera. Comunque, anche ove questa era stata utilizzata, non vi erano stati effettivi risultati, a causa della mancanza di indicazioni più precise in merito al suo funzionamento. In particolare, sarebbe stata utile l'istituzione di una piattaforma per facilitare lo scambio di informazioni sensibili. Gli organi a livello europeo non possedevano informazioni complete riguardo alla sicurezza, perché l'intero impianto ruotava attorno alla sola notificazione degli incidenti, lasciando fuori altre informazioni, comunque di rilievo, quali ad esempio il livello di skills e di formazione del personale. Il tutto impediva la reale implementazione di un meccanismo di gestione delle crisi, perché la normativa si interessava solo alla fase di notificazione dell'incidente[29].

Tutte le mancanze evidenziate erano radicate nell'impianto normativo e sarebbero state difficili da eliminare in mancanza di un intervento. Al contrario, era da immaginarsi un peggioramento della situazione con un aumento degli incidenti, che avrebbe portato con sé una crescita dei costi legati alla sicurezza. Molti soggetti privati magari avrebbero potuto aumentare i propri investimenti, ma la resa complessiva sarebbe stata sempre eterogenea, soprattutto a causa delle marcate esternalità.

29 Il ciclo di gestione delle crisi di cybersecurity si compone generalmente di quattro fasi: *preparation*, *response*, *recovery* e *lessons learned*. Nella fase di preparazione, le organizzazioni valutano proattivamente le proprie vulnerabilità, sviluppano piani di risposta agli incidenti e implementano misure di sicurezza. Durante la fase di risposta, rilevano e rispondono a un incidente informatico, contengono la violazione, attenuano i danni e indagano sulle cause. La fase di recupero si concentra sul ripristino delle normali operazioni, sulla riparazione dei sistemi colpiti e sull'implementazione di misure di sicurezza più efficaci. Infine, la fase di *lessons learned* comporta la conduzione di valutazioni *post-mortem* per identificare i punti deboli, aggiornare i piani e i controlli e migliorare le future capacità di risposta agli incidenti. Per ulteriori approfondimenti si rimanda a G BILLOIS, *Cybersecurity Incident and Crisis Management*, in D. ANTONUCCI (a cura di), *The Cyber Risk Handbook*, Wiley, Hoboken, 2017, pp. 171–84.

3. Una lettura a caldo della nuova direttiva NIS2

Per tutti questi motivi il legislatore europeo, a seguito della sua valutazione d'impatto, aveva deciso di procedere con l'emendamento della direttiva NIS e la sua sostituzione. Il testo definitivo della cosiddetta NIS2 è stato approvato nel dicembre 2022 e dovrà essere trasposto entro il 17 ottobre 2024, in tempo per l'abrogazione della precedente direttiva[30].

Il fatto che la direttiva abbia mantenuto il fondamento di legittimità nell'articolo 114 TFUE prova il consueto forte legame dell'intervento con il mercato interno. Se «tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato interno [...]», «la cybersicurezza è un fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione»[31].

Come si è appena dimostrato, l'eccessiva discrezionalità lasciata agli stati membri aveva limitato gli effetti positivi dell'armonizzazione, impattando negativamente sulle logiche di mercato, a causa dei molti e diversi requisiti da implementare da parte degli operatori. Non solo, ma la frammentazione nelle misure si traduceva anche in un'insicurezza congenita, che poteva essere sfruttata da eventuali attaccanti[32].

3.1. L'ambito di applicazione

Questo spiega la particolare attenzione dedicata al nuovo ambito di applicazione. Anzitutto, tra i punti oggetto della materia figurano due aggiunte rilevanti, da una parte regole e obblighi per lo scambio di informazioni sulla cybersicurezza, dall'altra specifici obblighi per lo svolgimento di attività di supervisione e di enforcement. Si trattava di due importanti assenze, che erano state alcune fra le cause principali dell'inefficienza del sistema NIS, proprio perché ancora fondato sull'erronea convinzione dell'efficienza della volontaria collaborazione e implementazione.

Sotto il profilo dei soggetti, l'ambito di applicazione è modellato attraverso l'introduzione di criteri di individuazione oggettivi, in particolar modo la dimensione dell'impresa. In questo modo, nell'ambito dei settori individuati dall'allegato I[33], tutti i soggetti che abbiano i requisiti per essere considerati medie

30 Si rimanda fra gli altri ai commenti di F. BAVETTA, *Direttiva NIS 2: Verso Un Innalzamento Dei Livelli Di Cybersicurezza a Livello Europeo – NIS*, in *MediaLaws*, n. 3, 2022, pp. 405–414; F. DI GIANNI, *Un'Europa "Ciberresiliente": La Risposta Dell'Unione Europea Alle Minacce e Agli Attacchi Informatici*, in *Studi Sull'integrazione Europea*, n. 2, 2023, pp. 399–424.

31 Si confronti il considerando 3 della direttiva (UE) 2022/2555.

32 Si confronti il considerando 5 della direttiva (UE) 2022/2555.

33 I settori sono allineati con quelli della normativa in materia di infrastrutture critiche. I primi settori individuati sono quelli definiti come «settori ad alta criticità»: 1) energia; 2) trasporti; 3) settore bancario; 4) infrastrutture dei mercati finanziari; 5) settore sanitario; 6) acqua potabile; 7) acque reflue; 8) infrastrutture digitali; 9) gestione dei servizi TIC (B2B); 10) pubblica amministrazione; 11) spazio. In aggiunta, fra quelli che vengono definiti come «altri settori critici» figurano: 1) servizi postali e di corriere; 2) gestione dei rifiuti; 3) fabbricazione, produzione e distribuzione di sostanze chimiche; 4) produzione, trasformazione e distribuzione di alimenti; 5) fabbricazione; 6) fornitori di servizi digitali; 7) ricerca.

imprese rientrano nell'ambito di applicazione della normativa. Sulla base di questa selezione iniziale si innestano poi altre aggiunte, indipendentemente dalla dimensione del soggetto[34], sempre preservando la possibilità di alcune esclusioni giustificate dallo svolgimento di attività legate alla sicurezza nazionale o a funzioni essenziali dello Stato.

Per quanto non nuovo, emerge anche lo sforzo di coordinamento con altre normative europee, attraverso i richiami al regolamento DORA, in materia di resilienza nelle attività finanziarie, al GDPR, alla direttiva e-privacy e alla nuova direttiva in materia di infrastrutture critiche. Questa volta però vi è una maggiore attenzione, che si può leggere anche nel maggior spazio al quale alla tematica è dedicato spazio nei considerando.

Inoltre, l'articolo 4 si spinge fino ad introdurre dei criteri oggettivi per definire i rapporti con altre normative settoriali. Esattamente come per la prima direttiva la normativa più specifica deve prevalere, ove introduca obblighi almeno equivalenti. Questa equivalenza però viene precisata sotto il profilo delle misure minime di sicurezza e della notificazione degli incidenti. In breve, una normativa settoriale può prevalere solo ove imponga l'adozione di misure di sicurezza equivalenti negli effetti e gli obblighi di notificazione degli incidenti consentano l'accesso immediato alle notificazioni al CSIRT e alle altre autorità NIS. In caso contrario, la normativa settoriale dovrebbe essere disapplicata per lasciare spazio alle obbligazioni derivanti dal nuovo sistema NIS.

Per quanto riguarda più specificatamente i modi di definizione dell'ambito di applicazione, emerge il superamento della precedente distinzione fra operatori di servizi essenziali e fornitori di servizi digitali, poiché non più aderente alla società attuale. Il sistema rimane improntato su un doppio regime, ma fra soggetti essenziali e soggetti importanti, individuati all'interno dei settori identificati dagli allegati I e II. Si noti come, a differenza della prima direttiva, non ci sia un'opposizione netta fra allegati. Se in precedenza ai settori di un allegato corrispondeva unicamente una categoria di soggetti, quest'automatismo è stato rimosso per lasciare spazio a ragioni di opportunità[35].

Cercando ora di delineare in maniera essenziale il nuovo ambito di applicazione, si può osservare come il principio generale del criterio dimensionale garantisca una grande certezza. Non solo questo è utilizzato

34 Si pensi ai fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico, ai prestatori di servizi di fiducia, ai registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio. Ma le aggiunte più rilevanti sono sicuramente legate alle infrastrutture critiche e alla pubblica amministrazione, eventualmente anche locale, se deciso dallo stato membro. Inoltre, non è secondaria l'attenzione agli istituti di ricerca, ai quali, similmente, è possibile un'estensione della normativa. Si confronti l'articolo 2 par. 2 della direttiva (UE) 2022/2555.

35 Sulla base della NIS1, l'allegato II («TIPI DI SOGGETTI AI FINI DELL'ARTICOLO 4, PUNTO 4») e l'allegato III («TIPI DI SERVIZI DIGITALI AI FINI DELL'ARTICOLO 4, PUNTO 5») si concentrano espressamente sui soggetti, poiché vi era una precisa distinzione fra i soggetti dell'uno e dell'altro. La prova è nello stesso titolo degli allegati che rimandano alle disposizioni della direttiva rispettivamente in materia di fornitori di servizi essenziali e di fornitori di servizi digitali.

per definire i confini dell'applicazione, ma anche per porre alcune differenze fra le due categorie di soggetti, ossia soggetti essenziali e soggetti importanti. In breve, tutte quei soggetti che superino i massimali per poter essere considerati medie imprese devono automaticamente essere classificati come soggetti essenziali.

Dopo questa prima individuazione «orizzontale», l'articolo 3 qualifica come soggetti essenziali alcuni soggetti specifici, da considerare con particolare criticità indipendentemente dalla loro dimensione.

In primo luogo, vi sono quei soggetti la cui operatività è alla base del funzionamento dei servizi di rete. La struttura di Internet si regge sul riconoscimento di una fiducia reciproca, che è il requisito primo per il suo utilizzo. Si pensi semplicemente ad una query su di un motore di ricerca, a seguito della quale vengono proposti dei risultati sotto forma di URL. Questo processo, che caratterizza la quotidianità, richiede diversi intermediari, che rientrano nell'insieme dei soggetti essenziali.

Il fatto che ogni connessione avvenga attraverso un link implica l'esistenza di un nome a dominio registrato presso un registro di nomi a dominio di primo livello. Questo è solo condizione necessaria ma non sufficiente per l'instradamento di una connessione, siccome il funzionamento della Rete si basa su indirizzi secondo lo schema del protocollo di rete (*Internet Protocol*, o IP). Ogni dominio è una mera semplificazione per migliorare l'esperienza di navigazione, che sarebbe altrimenti assai ardua se fosse richiesto di ricordare e inserire degli indirizzi numerici, come interpretati da *client* e *server*.

Di conseguenza, ogni dominio deve essere associato ad uno specifico indirizzo, che ogni *domain owner* deve configurare presso un fornitore di servizi DNS (*Domain Name System*), che ha il ruolo di mantenere e diffondere l'associazione con ridondanza presso gli altri gestori DNS. Quest'informazione viene reperita dal client che inizia la connessione verso il dominio in maniera del tutto trasparente rispetto all'utente. Allo stesso tempo, avviene anche la verifica dell'autenticità del dominio stesso, ossia della sua corrispondenza ad una determinata persona fisica o giuridica. Questo è possibile attraverso l'esistenza di una serie di infrastrutture alla base del cosiddetto web of trust. Tralasciando i dettagli, è sufficiente fare riferimento ai prestatori di servizi fiduciari qualificati, i quali si occupano anche del rilascio e della verifica di certificati per l'autenticazione di siti web[36].

Riepilogando, attraverso tutti questi passaggi, che sono alla base di una semplice navigazione sul web, è possibile delineare un primo gruppo di soggetti essenziali: registri dei nomi di dominio di primo livello,

36 Si sono fatti diversi riferimenti tecnici al funzionamento di Internet, il quale si preferisce dare per scontato in questa sede. Senza tediare con ulteriori dettagli, che sarebbero inopportuni in questo contesto, si consenta di rimandare a H. JINGWEI e D.M. NICOL, *An anatomy of trust in public key infrastructure*, in *International Journal of Critical Infrastructures* 13, n. 2–3, 2017, pp. 238–58, J.A. AMORIM, J.M. DE SIQUEIRA ROCHA, e T. MAGAL-ROYO, *Cybersecurity in Europe: Digital Identification, Authentication, and Trust Services*, in K. SANDHU (a cura di), 2021, pp. 18–36.

prestatori di servizi DNS e prestatori di servizi fiduciari qualificati[37]. Quest'ultimi sono l'unica reale integrazione, siccome gli altri due erano già qualificati come fornitori di servizi essenziali. La volontà del legislatore europeo è quella di rendere la normativa NIS l'unica normativa di riferimento. Alla luce del fine di creare uno standard univoco per la cybersicurezza nell'Unione, tutti quei soggetti dapprima eccettuati dall'ambito di applicazione devono essere ricondotti al suo interno.

L'esistenza di una normativa speciale non è motivo di riduzione dell'ambito di applicazione in esame, il quale deve essere il più vasto possibile per poter supplire ad eventuali mancanze in termini di sicurezza. Come si è già accennato, qualora una normativa speciale non garantisse il perseguimento di uno standard di sicurezza almeno equivalente, la normativa NIS dovrebbe riespandersi.

Per garantire questa logica, vengono meno diverse eccezioni, tra le quali vanno sottolineate le infrastrutture critiche europee, anch'esse sottoposte ad un recente processo di riforma[38]. Non va poi tralasciata la componente fisica dell'Internet, composta da fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, che in passato rappresentavano un'altra eccezione. Questi però non vengono considerati in toto, ma solamente nella misura in cui raggiungano la dimensione di media impresa.

Come anticipato nell'introduzione, la novità più importante è costituita dalla scelta di includere anche il settore della pubblica amministrazione[39]. Sia l'amministrazione centrale, che quella regionale dovranno essere sottoposte agli obblighi scaturenti dalla direttiva, per quanto venga lasciata un'importante apertura con la possibilità di considerare anche il livello locale. Chiaramente però si tratta di un ambito delicato, a causa degli interessi tutelati. La normativa europea non può mai applicarsi in contrasto con la sicurezza nazionale o con lo svolgimento di funzioni essenziali dello Stato. Di conseguenza, la direttiva non si applica a quelle pubbliche amministrazioni che siano portatrici di questi interessi o che si occupino di attività di indagine o di perseguimento dei reati.

In chiusura, viene poi lasciata al legislatore nazionale la libertà di collocare liberamente i soggetti individuati dagli allegati I e II nella categoria dei soggetti essenziali o in quella dei soggetti importanti. Questo dimostra la preannunciata mancanza di una corrispondenza fra gli allegati e le categorie di soggetti.

37 Per una definizione si confronti rispettivamente l'articolo 6 nn. 20, 21 e 26 della direttiva (UE) 2022/2555. Per i prestatori di servizi fiduciari qualificati viene fatto rimando all'articolo 3 n. 19 del regolamento (UE) 2014/910 (eIDas).
38 La precedente direttiva 2008/114/CE è stata abrogata e sostituita dalla direttiva (UE) 2022/2557, che è stata approvata in parallelo rispetto alla direttiva NIS2. Tra le principali novità della nuova direttiva si riscontra un ampliamento dell'ambito di applicazione, al quale consegue una maggiore chiarezza del processo di identificazione delle infrastrutture critiche europee. Inoltre, va sottolineata l'aggiunta del concetto di «soggetti critici di particolare rilevanza europea». Si confronti il capo IV della direttiva (UE) 2022/2557.
39 Si veda nota 14.

Queste possono essere concettualmente rappresentate come due insiemi concentrici, di cui al centro si pongono i soggetti essenziali. Alla libertà del legislatore di collocare i soggetti nell'una o nell'altra categoria, infatti, si accompagna la regola di identificazione in negativo dei soggetti importanti. Tutti quei soggetti identificati dagli allegati I o II ma non classificati come soggetti essenziali sono da considerarsi come soggetti importanti.

3.2. L'organizzazione a livello nazionale

Passando all'organizzazione a livello nazionale, fra gli obblighi principali vi è quello di adottare una strategia nazionale di cybersicurezza, aspetto che aveva caratterizzato la prima NIS. In tal caso però i contenuti della strategia vengono particolareggiati in maniera piuttosto minuziosa. Fra le aggiunte più rilevanti figurano le tematiche della supply chain e dell'information sharing, che vengono evidenziate complessivamente dalla nuova direttiva.

Tralasciando gli obblighi di nomina delle autorità competenti[40], che sono rimaste invariate, vengono anche introdotte le figure di autorità competenti per la gestione degli incidenti e delle crisi di cybersicurezza su vasta scala. Si parla in gergo di *cyber crisis management authorities*, (tradotto come autorità di gestione delle crisi informatiche) tra le quali una di queste deve ricoprire il ruolo di coordinatore. Questo comporta che alla strategia nazionale di cybersicurezza, si affianchi un piano per la gestione degli incidenti su larga scala e delle crisi cyber, che evidenzi chiaramente le capacità delle autorità, gli asset a loro disposizione e le procedure da seguire. Questa importante innovazione a livello nazionale corrisponde a livello europeo con l'istituzionalizzazione formale del *European cyber crisis liaison organisation network* (EU-CyCLONe), che rappresenta un tassello fondamentale all'interno del sistema europeo di risposta alle crisi[41].

La necessità sfruttare al meglio le sinergie fra i diversi attori e di rafforzare il coordinamento era già emersa più di un decennio addietro nelle conclusioni del Consiglio dell'Unione europea, che incoraggiava gli stati membri a partecipare allo sviluppo di un sistema Europeo di cooperazione contro gli incidenti[42]. I primi risultati concreti però sono relativamente recenti, perché erano seguiti all'idea della Commissione di

40 In particolare, il sistema NIS aveva introdotto la necessità di nominare una o più autorità competenti e fra queste di individuare un punto di contatto nazionale, al fine di semplificare i rapporti sia con le istituzioni europee, che con gli altri stati membri dell'Unione. A seguito della riforma attuata con l'introduzione della nuova agenzia cyber, il ruolo di punto di contatto è ricoperto per l'Italia dall'ACN.

41 L'EU-Cyclone è composto da rappresentanti delle autorità nazionali di prevenzione delle crisi cyber e dalla Commissione, che ricopre un ruolo di osservatore, a meno che si tratti di casi in cui un incidente su larga scala potrebbe avere un impatto significativo sui settori della direttiva. L'ENISA provvede per il segretariato. Il principale obiettivo è quello di un incremento della preparazione degli stati membri attraverso uno scambio informativo a beneficio della *situational awareness* collettiva.

42 European Commission, *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, *OJ L*, 13 settembre 2017, p. 9, consultabile qui.

consolidare un approccio di risposta alle crisi sfruttando gli elementi esistenti nell'ecosistema europeo. Benché il sistema NIS non prendesse in considerazione quest'aspetto, veniva suggerito l'innesto su di esso delle logiche necessarie, al fine di trarre il massimo dal sistema di cooperazione esistente[43]. Siccome «le conoscenze e le competenze in materia di sicurezza informatica [erano] disponibili a livello dell'UE, ma in modo dispersivo e non strutturato»[44], l'idea era di collocarle in un sistema strutturato.

Il risultato di questo sforzo era confluito in un blueprint, allegato ad una comunicazione della Commissione, che tentava di porre in un sistema organizzato tutti gli attori e le procedure esistenti in materia cyber, costruendo diversi livelli di risposta[45]. A distanza di pochi anni, tale sistema era stato ulteriormente integrato dalla creazione dell'EU-CyCLONe, il quale si sarebbe affermato come strumento di raccordo fra il livello politico[46] e il livello tecnico nella gestione delle crisi, gettando le basi per un network stabile di cooperazione fra le autorità degli stati membri[47]. Il suo primo test annuale è avvenuto nel 2020 in occasione della seconda edizione del Blue OLEx[48], una serie di test ed esercitazioni di cybersicurezza iniziati nel 2019[49].

Ma nuovo slancio per l'intero sistema è arrivato in particolare dall'ondata di COVID-19, durante la quale erano fiorite le discussioni per la creazione di una Joint Cyber Unit «per rispondere collettivamente e scambiare informazioni sulla base della «necessità di condividere [...]»[50]. Questo avrebbe permesso di

43 European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, 5 luglio 2016, p. 4, consultabile qui.

44 *Ibid.*, p. 4.

45 Rispondere agli incidenti di cybersecurity poteva assumere diverse forme, da decisioni operative in materia di misure di sicurezza, a decisioni politiche, che prevedevano una risposta diplomatica. Nel descrivere la sua architettura il *blueprint* stesso si articolava in tre livelli, a seconda degli attori coinvolti. Uno politico, uno operativo ed un altro tecnico. Per un approfondimento delle sue componenti si rimanda a European Commission, *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, p. 13.

46 L'organizzazione per la gestione delle crisi a livello politico si fonda sugli EU *Integrated Political Crisis Response* ('*IPCR*') *arrangements*, ad implementazione della clausola di solidarietà europea. L'adattamento dell'IPCR è avvenuto con una recente decisione di implementazione del Consiglio dell'Unione europea. Si veda Council of the European Union, Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements.

47 Per una breve descrizione dell'*EU CyCLONe*, si rimanda al sito di ENISA. Si confronti il considerando 71 della direttiva (UE) 2022/2555.

48 Per la precisione si tratta di un cosiddetto «*table-top exercise*», ossia un'esercitazione che si svolge esattamente come se si trattasse di un vero e proprio gioco da tavolo. Un'esercitazione di questo tipo è un'attività di formazione basata su uno scenario simulato, condotta in un ambiente da tavolo, che coinvolge in genere i principali soggetti interessati e i responsabili delle decisioni. Ha lo scopo di valutare e migliorare le capacità di preparazione, risposta e coordinamento nell'eventualità di un incidente o di una crisi reale. I partecipanti discutono e analizzano lo scenario, identificano le sfide potenziali e sviluppano collettivamente strategie e azioni per mitigarle e affrontarle. L'esercitazione di solito si svolge in un ambiente controllato senza dispiegamento attivo di risorse.

49 L'ultima edizione si è tenuta a Vilnius il 7 novembre 2022. Si veda *Blue OLEx 2020: The European Union Member States Launch the Cyber Crisis Liaison Organisation Network (CyCLONe)*, Press Release, ENISA, consultabile qui.

50 Traduzione libera. Si veda European Commission, *COMMISSION RECOMMENDATION on Building a Joint Cyber Unit*, 23 giugno 2021, consultabile qui.

supplire alla mancanza di una piattaforma europea per lo scambio delle informazioni e avrebbe migliorato le condizioni per la solidarietà e l'aiuto reciproco fra gli stati membri, senza necessariamente creare un nuovo organo a livello europeo.

In generale è possibile cogliere un ampliamento dell'attenzione ad altri aspetti connessi alla cybersecurity, segno di una maggiore consapevolezza. Sempre rimanendo a livello nazionale, un altro importante esempio, è la prescrizione dell'istituzione di un meccanismo a supporto della divulgazione coordinata delle vulnerabilità scoperte in prodotti o servizi ICT (da qui in avanti semplicemente disclosure). Si tratta della normazione di aspetti critici per una società digitale, ove la resilienza delle sue componenti essenziali è messa ogni giorno alla prova da nuovi attacchi. Ognuno di questi tende a sfruttare vulnerabilità note e non, per questo l'arricchimento costante della conoscenza in materia è fondamentale per poter prevenire il successo di degli attaccanti.

Allo stesso tempo, si tratta di una procedura delicata. Chi scopre una nuova vulnerabilità e sceglie di notificarla deve essere assistito affinché la divulgazione della scoperta porti a vantaggi per la società, ma non danneggi le entità potenzialmente affette, dando loro il tempo necessario per implementare opportune contromisure. Per questo viene solitamente negoziata una scadenza, oltre alla quale procedere con la pubblicazione della vulnerabilità. Tale pubblicazione avverrà in un database europeo predisposto e mantenuto da ENISA, che costituirà l'aspetto unificante del sistema di *disclosure* delle vulnerabilità a livello europeo[51].

L'ultima nota in merito all'organizzazione a livello nazionale riguarda la cooperazione fra le diverse autorità, che raggiunge un grande livello di maturazione. Si percepisce chiaramente lo sforzo verso la creazione di un sistema di raccordo allo scopo di garantire un allineamento della conoscenza in materia di cybersicurezza. Per questo non bisogna più inquadrare il sistema NIS come un sistema a parte, ma come una normativa di raccordo fra soggetti ed organi nati in contesti differenti e con competenze eterogenee. In particolare, quella sovrapposizione, dapprima implicita, con le procedure di *data breach* contenute nel GDPR viene esplicitata e regolamentata. Ogniqualvolta un incidente cyber implichi dati personali, le autorità NIS dovranno senza ritardo informare il Garante per la Protezione dei Dati Personali[52], in modo tale da evitare anche un'inutile duplicazione sanzionatoria.

51 Per lungo tempo la gestione delle vulnerabilità è stata trascurata nel vecchio continente, a differenza degli Stati Uniti dove sono gestiti tutti i più comuni database utilizzati dagli addetti ai lavori. Si noti come non tutti siano necessariamente mantenuti da entità pubbliche. Ad esempio, il più famoso e utilizzato è sicuramente il *Common Vulnerability Exposure* (CVE) database del MITRE, storica azienda americana attiva nel settore della cybersecurity. Un altro famoso database di vulnerabilità è quello del NIST americano. Indipendentemente dal database consultato, ogni vulnerabilità è ricercabile attraverso un codice univoco e progressivo CVE-YYYY-NNNN. Ciò è possibile perché ad ogni richiesta di *disclosure* viene richiesto il blocco di un codice da una cosiddetta *CVE Numbering Authority* (CNA), che può essere un veditore di prodotti o fornitore di servizi ICT, un CERT o una qualsiasi organizzazione specializzata nel *bug bounty*. Per approfondimento sul funzionamento si rimanda al sito del NIST.

52 Si confrontino gli articoli 13 e 35 della direttiva (UE) 2022/2555.

3.3. L'organizzazione a livello europeo

Anche sul piano europeo, si può percepire una netta maturazione della consapevolezza in ambito cyber. Se prima i report prodotti dall'ENISA erano alimentati principalmente dalle informazioni sugli incidenti, emerge un allargamento delle aree di interesse a comprendere anche altri aspetti inerenti, quali il livello delle capacità cyber, le buone pratiche di sicurezza e di formazione. Non è nemmeno secondario il fatto che tutti i report futuri dovranno essere resi disponibili in formato automatizzato, fattore che metterà a disposizione una base di dati pubblica per future analisi.

Non solo si fa leva su di un incremento dell'informazione disponibile, ma si vuole anche responsabilizzare attraverso l'introduzione di un meccanismo di peer review volontario, i cui aspetti dovranno essere definiti dal gruppo di cooperazione. Questo potrà diventare uno strumento per la crescita e l'uniformazione delle capacità cyber fra i diversi paesi, attraverso una valutazione oggettiva fra pari. L'idea alla base non è quella di rimarcare le mancanze di uno stato membro richiedente, ma di fornire ausilio tecnico per il miglioramento delle proprie pratiche di sicurezza[53].

La parte più interessante della normativa è però quella riferita alla governance. Vengono qui mantenuti i due obblighi fondamentali di adozione di misure di sicurezza adeguate e di notificazione degli incidenti.

Il primo aspetto da rilevare è come entrambi gli obblighi non trovino una diversa applicazione a seconda che si tratti di un soggetto essenziale o un soggetto importante, contrariamente a quanto avveniva fra operatori di servizi essenziali e fornitori di servizi digitali.

In generale, però permane un approccio basato sul rischio, da intendersi come rischio derivante da qualunque tipo di minaccia. La logica è quella di implementare quelle misure che, tenendo conto dello stato dell'arte, abbiano la maggiore efficacia nel migliorare l'esposizione al rischio, a parità di costi[54]. Per coadiuvare nell'identificazione, vengono elencate delle categorie di misure[55], tra le quali figurano quelle relative alla protezione della supply chain. Il tema delle relazioni con i fornitori viene tenuto in grande considerazione, al punto che il gruppo di cooperazione NIS, per coadiuvare i soggetti nella migliore selezione delle relative misure di protezione, dovrà svolgere un risk assessment coordinato di alcune

53 Si confronti l'articolo 19 della direttiva (UE) 2022/2555.

54 La logica si fonda su di una ormai consolidata standardizzazione internazionale, che viene menzionata dai considerando, che si rifanno alla serie ISO 27000. Per evitare che la sicurezza si traduca in un inutile peso burocratico, le misure dovrebbero sempre rimanere coerenti con la probabilità di accadimento degli incidenti e con la gravità dei loro effetti. Si vedano i considerando da 76 a 83. Ad ogni modo, l'applicazione di standard internazionali viene considerata come alternativa rispetto all'esistenza di schemi di certificazione ai sensi del cosiddetto *Cybersecurity Act*.

55 Le misure tecniche e metodologiche da adottare, con i loro appositi requisiti potranno essere raccolte in appositi atti di implementazione della Commissione. In particolare, per quei fornitori di servizi i quali, per via della natura della loro attività, sono distribuiti in diversi paesi nell'Unione, tale identificazione dovrà avvenire obbligatoriamente entro il 17 ottobre 2024.

supply chain critiche identificate dalla Commissione europea[56]. In tal caso il suggerimento è quello per i soggetti di implementare la sicurezza anche attraverso appositi accordi contrattuali[57], in modo da vincolare le proprie controparti al rispetto di un determinato standard.

Per quanto, almeno apparentemente, l'approccio sia simile, dal singolo articolo 21 non emerge il carattere unificante della direttiva NIS, che vuole diventare l'unico punto di riferimento sia per l'implementazione di misure di sicurezza, che per gli obblighi di notificazione. Di conseguenza, visto che i prestatori di servizi di fiducia, i fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico sono ormai ricompresi nell'ambito di applicazione della nuova NIS[58], le corrispondenti disposizioni previste dalle rispettive normative settoriali dovranno essere eliminate[59].

Il secondo obbligo rilevante è quello di notificazione degli incidenti significativi, i cui criteri di definizione risultano essere stati unificati e semplificati[60], e di quegli incidenti che potrebbero influire negativamente sulla fornitura dei servizi. Questa seconda categoria di incidenti rappresenta un'aggiunta ragionevole, al fine di non sottrarre dall'obbligo di notificazione informazioni utili, anche se non relative ad un evento di tale gravità da rientrare nella prima categoria. Inoltre, sono state anche specificate delle scadenze temporali precise per le diverse fasi della notificazione dell'incidente, che, riprendendo la prassi affermata con la prima direttiva, deve intendersi come uno scambio dinamico di informazioni in più fasi fra il soggetto interessato e lo CSIRT.

A grandi linee, i momenti fondamentali di questo scambio ricordano quelli della prima direttiva NIS, ai quali si aggiunge l'eventuale report intermedio, a seconda delle necessità del CSIRT. Altra differenza rilevante riguarda poi il report finale, il quale viene diviso in due momenti distinti.

Procedendo con ordine si cercherà ora di delineare il processo nella sua interezza, a partire dal momento zero, rappresentato dall'accadimento dell'incidente di sicurezza[61]. La reale base di partenza però è

56 Si confronti l'articolo 22 della direttiva (UE) 2022/2555. Al momento in cui si scrive, l'ENISA ha pubblicato un report di sintesi delle principali buone pratiche di cybersecurity adottate nella supply chain, per coadiuvare i futuri lavori del Gruppo di Cooperazione. Si rimanda a ENISA, *Good Practices for Supply Chain Cybersecurity*, giugno 2023, consultabile qui. Stando all'analisi che emerge dai considerando la futura analisi dovrà essere simile a quella già svolta per il settore delle telecomunicazioni di ultima generazione. Si veda European Commission, *Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G Networks*, 26 marzo 2019, consultabile qui.

57 Si confronti il considerando 85 della direttiva (UE) 2022/2555.

58 La loro previsione figura nel settore delle infrastrutture digitali. Si veda l'allegato I.

59 Tale abrogazione viene prevista dagli articoli 42 e 43 della direttiva in esame, la cui efficacia decorrerà dal 18 ottobre 2024. Ad ogni modo la direttiva si preoccupa di garantire il più possibile una continuità con il sistema precedente, da una parte tenendo in considerazione tutto il materiale predisposto a livello nazionale ed europeo per la corretta applicazione delle normative di settore. Dall'altra si invitano gli stati membri a nominare le autorità di settore come autorità NIS. Si confrontino i considerando 94 e 95.

60 All'articolo 23 par. 3 della direttiva in esame si fa riferimento ad una grave interruzione dell'operatività dei servizi o a una grave perdita finanziaria. In alternativa si tiene conto della possibilità di influenzare altri soggetti, causando considerevoli danni materiali e non materiali.

61 Per incidente si intende «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi». Si

costituita dalla scoperta dell'incidente. Quando un soggetto NIS viene a conoscenza di tale evento, deve immediatamente provvedere ad informare lo CSIRT nazionale. Si parla in gergo di *early warning*, ossia di una comunicazione iniziale che ha solo lo scopo di informare l'autorità dell'esistenza dell'incidente, senza fornire dettagli approfonditi su di esso. La logica è quella di non rallentare la procedura di notificazione, prescrivendo fin da subito dettagli che normalmente richiedono un maggior tempo di indagine. Mentre l'early warning si colloca entro ventiquattr'ore dalla conoscenza dell'incidente, la prima notificazione vera e propria, corredata di un'iniziale valutazione d'impatto e degli eventuali indicatori di compromissione disponibili, giunge solo successivamente, ossia entro settantadue ore.

Si noti come fino a questo momento non si sia ancora formato un vero e proprio report, ma sia stata solo confezionata una conoscenza iniziale. Per un vero e proprio report c'è tempo fino ad un mese dalla data della notificazione, a meno che lo CSIRT non prescriva, per ragioni di opportunità, un report intermedio. Ad ogni modo la normativa acconsente ad un tempo ragionevole per lo svolgimento delle operazioni di analisi forense dei sistemi interessati, operazioni necessarie per poter giungere ad una presentazione strutturata dell'informazione. Non solo il report deve contenere una descrizione dettagliata dell'incidente, ma deve anche esplicare le misure di mitigazione adottate per affrontarlo.

Non si tratta però di un report necessariamente definitivo. Qualora l'incidente duri più di un mese rispetto alla notificazione, deve essere predisposto anche un report successivo alle operazioni di ripristino. Come anticipato, la scelta del legislatore europeo di spezzare in due momenti il report finale si spiega alla luce della volontà di evitare il decorrere di un tempo eccessivo senza il coinvolgimento dello CSIRT.

Sicuramente maggiori informazioni verranno specificate dalla Commissione che dovrà adottare entro il 17 ottobre 2024 un proprio atto di implementazione per precisare il concetto di incidente significativo per alcune categorie di entità particolarmente distribuite nell'Unione. Viene però anche lasciata la possibilità di precisare ulteriormente il tipo di informazione, il formato e la procedura di notificazione.

Infine, un'ultima particolarità riguardante la notificazione degli incidenti può essere colta nelle disposizioni riguardanti la notificazione volontaria[62], nelle quali viene introdotto il concetto di «quasi incidente» (dall'inglese «*near miss event*»)[63]. La notificazione volontaria, infatti, non riguarda solo i soggetti non ricompresi nell'ambito di applicazione della normativa, ma anche i soggetti essenziali e i soggetti importanti, che hanno la possibilità di notificare anche quegli eventi che in potenza avrebbero potuto

confronti l'articolo 6 n. 6 della direttiva (UE) 2022/2555. Tale compromissione però deve essere anche rilevante ai fini della notificazione, ossia deve avere un impatto significativo sui servizi o, in alternativa, influire negativamente sulla fornitura del servizio. A seguire si parlerà genericamente di incidente di sicurezza, dando per scontato che tale incidente deve essere anche un incidente rilevante.

62 Si confronti l'articolo 30 della direttiva (UE) 2022/2555.

63 Si riporta di seguito la definizione di cui all'articolo 6 numero 5: «un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato».

impattare sui dati o sui servizi offerti. L'efficacia di questa possibilità opera in sinergia con gli eventuali accordi volontari per lo scambio di informazioni rilevanti sulla cybersecurity. Tali accordi possono coinvolgere sia soggetti esterni, che soggetti interni alla normativa[64].

Senza alcuna pretesa di completezza, vi sono poi alcuni ed ulteriori aspetti meritevoli di menzione.

Uno di questi può essere ricercato nei molti problemi ingenerati dalla poca chiarezza circa alla giurisdizione da applicarsi ai diversi soggetti. In merito a questo, la nuova direttiva dedica molto più spazio alla definizione del loro corretto collocamento. Il criterio principale è quello dello stabilimento, secondo il quale semplicemente un soggetto è sottoposto alla giurisdizione del paese nel quale è stabilito. A questo però seguono alcune eccezioni, che riguardano quei soggetti caratterizzati da una prestazione per lo più transfrontaliera delle proprie attività[65]. In particolare, per quei soggetti ai quali si applica il criterio dello stabilimento principale viene predisposta una serie alternativa di parametri oggettivi per la sua corretta individuazione[66].

Indubbiamente però la più importante novità sta nella predisposizione di un registro di entità presso l'ENISA, nel quale raccogliere le informazioni riguardanti proprio quelle entità sottoposte al criterio dello stabilimento principale, in modo da evitare ogni possibile dubbio in merito all'applicazione della giurisdizione. Il popolamento del registro richiederà una prima fase di raccolta di informazioni da parte delle autorità competenti degli stati membri entro il 17 gennaio 2025, per poi inoltrare i risultati all'ENISA attraverso il proprio punto di contatto[67].

In generale, può dirsi che uno dei più grandi cambiamenti apportati con la NIS2 stia nell'attenzione dedicata alla corretta tenuta dei registri, anche quelli già esistenti. Un altro esempio è costituito dai registri contenenti i dati di registrazione dei nomi a dominio, i cosiddetti WHOIS data. La correttezza e la pubblicità di tali dati è essenziale per la prevenzione di abusi del DNS, per questo devono essere

64 Si confronti l'articolo 29 della direttiva (UE) 2022/2555.

65 Brevemente, ai fini dell'identificazione della corretta giurisdizione per soggetti transfrontalieri ci sono tre criteri differenti. Il primo è quello della fornitura del servizio, applicato ai fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico. Questi sono considerati sottoposti alla giurisdizione di quello stato membro nel quale forniscono i loro servizi. Il secondo è quello dello stabilimento principale, il quale trova applicazione per una serie di soggetti comunemente caratterizzati dalla fornitura di servizi potenzialmente in tutta l'Unione. Si pensi, ad esempio, ai fornitori di servizi DNS, ai motori di ricerca o ai registri di nomi a dominio di primo livello per citarne alcuni. Il terzo e ultimo criterio è quello dello stabilimento per istituzione, il quale trova applicazione per la pubblica amministrazione, la quale deve essere soggetta alla giurisdizione dello stato che la ha istituita.

66 Il primo criterio è quello del luogo ove vengano prese in maniera prioritaria le decisioni in materia di gestione del rischio di cybersicurezza. In alternativa, si guarda al luogo ove le operazioni cyber vengano svolte. Infine, in mancanza di altro, si guarda allo stabilimento con il maggior numero di dipendenti. Si confronti l'articolo 26 par. 2 e 3 della direttiva in esame.

67 Si confronti l'articolo 27 della direttiva (UE) 2022/2555.

implementati specifici controlli ex ante ed ex post rispetto alla registrazione e almeno i dati relativi alle persone giuridiche dovrebbero essere resi pubblici[68].

Un'ultima tematica al quale il legislatore europeo ha dedicato spazio, è quella delle misure di vigilanza e controllo da parte delle autorità competenti degli stati membri. Mentre la prima direttiva si limitava a richiedere la generica attribuzione di poteri e risorse adeguate, nel nuovo testo non ci si limita semplicemente a richiedere misure effettive, proporzionate e dissuasive, ma viene prevista un'elencazione sia di poteri minimi di vigilanza, che di poteri minimi di controllo[69]. Per quanto l'esemplificazione non sia tassativa ha certamente il pregio di favorire un'armonizzazione dei poteri a livello di Unione, cercando anche di bilanciare l'imposizione di sanzioni con l'esercizio del diritto di difesa nelle opportune sedi, tenendo in considerazione la serietà della violazione e la sua durata, come anche gli eventuali danni prodotti. Le misure devono certamente essere proporzionate al rischio intrinseco alla violazione, ma deve essere sempre tutelata la possibilità di un contraddittorio. In proposito viene anche abbozzata una procedura che idealmente dovrebbe precedere la somministrazione di sanzioni. L'autorità competente dovrebbe sempre notificare le proprie conclusioni preliminari alle entità coinvolte, per lasciare loro un tempo ragionevole per produrre osservazioni.

Nonostante questa notevole maturazione, che porta a rendere esplicito il richiamo ai diritti fondamentali nell'ambito della parte operativa del testo normativo, rimane invece l'idea di un doppio binario fra soggetti essenziali e soggetti importanti. Per quest'ultimi, sull'impronta di quanto avviene fra operatori di servizi essenziali e fornitori di servizi digitali, le misure di intervento devono essere unicamente ex post[70].

Infine, per quanto riguarda le sanzioni, da una parte vengono introdotte delle soglie minime e massime per le sanzioni amministrative, in modo da superare lo stato di estrema frammentazione causato dalla completa mancanza d'indicazioni. Dall'altra, vengono nominate espressamente le sanzioni penali, la cui introduzione sarà pertanto obbligatoria per tutti gli stati membri, che dovranno notificare alla Commissione le disposizioni introdotte per l'implementazione[71].

68 Si confrontino i considerando dal 109 al 112 della direttiva (UE) 2022/2555.

69 Si confronti l'articolo 32 par. 2 e 3 della direttiva (UE) 2022/2555.

70 La logica della prima direttiva NIS già prevedeva un trattamento di favore per i fornitori di servizi digitali, identificati dall'allora allegato III. La ragione può essere emblematicamente ricercata nei considerando 48 e 49 della direttiva (UE) 2016/1148. «La sicurezza, la continuità e l'affidabilità del tipo di servizi digitali di cui alla presente direttiva sono essenziali per il buon funzionamento di molte imprese. […] Tali servizi digitali potrebbero pertanto rivestire un'importanza fondamentale per il buon funzionamento delle imprese che dipendono da essi nonché per la partecipazione di tali imprese al mercato interno e agli scambi commerciali transfrontalieri nell'Unione». Tuttavia, dovendo gli stessi operatori di servizi essenziali spesso fare affidamento sui servizi dei fornitori di servizi digitali, «per gli operatori di servizi essenziali che spesso sono essenziali per il mantenimento delle attività sociali ed economiche critiche, il grado di rischio è più elevato che per i fornitori di servizi digitali. Pertanto, gli obblighi di sicurezza per i fornitori di servizi digitali dovrebbero essere meno rigidi. I fornitori di servizi digitali dovrebbero rimanere liberi di adottare le misure che ritengono adeguate alla gestione dei rischi che corre la sicurezza delle loro reti e dei loro sistemi informativi.»

71 Si confronti l'articolo 36 della direttiva (UE) 2022/2555.

In mancanza, di ulteriori interventi da parte delle istituzioni europee, si deve attendere l'opera di trasposizione a livello nazionale, che dovrà avvenire entro il 17 ottobre 2024, data oltre alla quale la precedente direttiva verrà abrogata[72]. La data di prima revisione degli effetti della NIS2 è fissata entro il 17 ottobre 2027, a tre anni dalla prima applicazione degli effetti. Nonostante sia ancora presto per dare un giudizio definitivo, gli interventi sembrano tenere conto delle mancanze del precedente sistema, lasciando ben sperare per la sua futura efficacia.

72 L'allegato III della direttiva contiene una tabella di trasposizione per consentire di traslare gli eventuali richiami alla vecchia direttiva alle disposizioni aggiornate.