CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

LA SICUREZZA INFORMATICA NELL´ORDINAMENTO ITALIANO: CRITICITÀ E OPPORTUNITÀ A SEGUITO DELL'ENTRATA IN VIGORE DELLA DIRETTIVA EUROPEA NIS2

Nel 2016, l'Unione europea adotta la Direttiva NIS, primo strumento legislativo sulla sicurezza informatica a livello europeo. L'Italia, dopo averla recepita, ha potenziato il suo ordinamento con interventi ulteriori: perimetro di sicurezza nazionale cibernetica; Agenzia per la cybersicurezza nazionale. La Direttiva NIS sta già tramontando: presso le istituzioni europee è in fase di approvazione la sua revisione. Il contributo analizza la normativa in materia presentando criticità ed opportunità, rispetto all'entrata in vigore della nuova Direttiva NIS2.

di **Marco Ripiego**
IUS/14 - DIRITTO DELL'UNIONE EUROPEA
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Mercoledì 9 Febbraio 2022

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

In 2016, European Union passed the NIS Directive, first cyber security legislation at European level. After having adopted that, Italy reinforced its legal system by further legislation: cybernetic national security perimeter; National cybersecurity agency. NIS Directive is already about to revoke – European institutions are going to introduce its revision. The paper hereby analyses Italian cyber security legislation disclosing criticality and opportunity due to the new NIS2 Directive coming into force.

Sommario: 1. Introduzione; 2. Uno sguardo alla Direttiva NIS; 3. L'esigenza di revisione: la proposta di Direttiva NIS2; 4. La normativa italiana in materia, alla prova dell'entrata in vigore della Direttiva NIS2; 5. Conclusioni.

1. Introduzione

L'ordinamento giuridico italiano della sicurezza informatica, ossia l'insieme delle norme giuridiche in materia di sicurezza informatica, seppur giovane, si compone di una pluralità di atti, nazionali e di matrice sovranazionale-europea, alcuni dei quali si sovrappongono, almeno parzialmente, tra loro, risultando così un coacervo normativo. Tale ordinamento verrà a breve condizionato, dalla verosimile entrata in vigore della Direttiva europea cosiddetta NIS2.

La proposta di Direttiva NIS2 – che segue la procedura legislativa ordinaria ex art. 294 del Trattato sul funzionamento dell'Unione europea1 –, reca nell'intitolazione «Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148». La Direttiva europea 2016/11482, recante «misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione», viene adottata dal Parlamento europeo e dal Consiglio dell'Unione europea, il 6 luglio 2016; è più comunemente conosciuta come Direttiva NIS (da network and information security, ossia «sicurezza delle reti e delle informazioni»). La Direttiva NIS2, qualora approvata, abrogherà, sostituendola, la vigente Direttiva NIS.

Una delle particolarità della materia – la sicurezza informatica – sta nella mancanza di una definizione ampiamente riconosciuta dalla comunità scientifica3; ciò si ripercuote, di conseguenza, anche sul piano giuridico. Le stesse normative in materia, infatti, impiegano espressioni linguistiche e formule, differenti, per riferirsi alla sicurezza informatica.

CamminoDiritto.it
ISSN 2421-7123

Andando per ordine, la Direttiva NIS definisce «sicurezza della rete e dei sistemi informativi», «la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi»4. Il Regolamento sulla cibersicurezza5, definisce «cybersicurezza»: «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»6. La normativa sulla «architettura di cybersicurezza nazionale»7 italiana, definisce «cybersicurezza»: «l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza»8.

Il presente contributo, anzitutto, dedicherà un paragrafo ad una sommaria disamina della Direttiva NIS. Successivamente, verrà introdotta la nuova Direttiva NIS2, segnalando ed analizzando quelle che per l'Autore saranno le principali novità, rispetto alla Direttiva NIS. Verrà poi svolta una ricognizione del quadro normativo italiano attualmente vigente in materia di sicurezza informatica, al fine di individuare quelle che saranno, verosimilmente, le criticità derivanti dall'entrata in vigore della Direttiva NIS2 ed in particolare, dal suo recepimento nell'ordinamento italiano. Infine, con spirito propositivo, si argomenterà quanto alla possibilità di trasformare le criticità di cui alla Direttiva NIS2, in opportunità per l'ordinamento italiano, al fine di incrementare la qualità della normativa italiana in materia di sicurezza informatica nazionale.

2. Uno sguardo alla Direttiva NIS

La Direttiva NIS nasce dall'idea del legislatore europeo, di disporre di uno strumento giuridico comune a tutti gli Stati membri, finalizzato ad introdurre un corpo di regole aventi la funzione di costruire un sistema per la gestione degli e la risposta agli incidenti informatici, che possono subire gli operatori economici del mercato unico, piccoli o grandi che siano, piccoli o grandi che siano9. Gli incidenti informatici10, infatti, possono compromettere l'operatività e le attività di tali soggetti e quindi, di conseguenza, possono ripercuotersi sul funzionamento del mercato interno dell'Unione nel suo complesso11.

Gli operatori economici – ma non solo – nello svolgimento della loro attività tipica, impiegano al giorno d'oggi mezzi e strumenti informatici, utili per svolgere in maniera più efficace ed efficiente le proprie attività. È essenziale che tali mezzi e strumenti siano sicuri ed affidabili: una compromissione degli stessi, infatti, comporterebbe l'arrecare un danno alle attività dell'operatore. Il legislatore europeo comprende dunque come la sicurezza delle reti e dei sistemi informativi (più in generale la sicurezza dei sistemi

CamminoDiritto.it
ISSN 2421-7123

informatici, quindi la sicurezza informatica) degli operatori del mercato unico, sia essenziale per il suo armonioso funzionamento12.

Il legislatore europeo, con la Direttiva NIS, introduce così per la prima volta, una legislazione in materia di sicurezza informatica. E ciò, attraverso lo strumento giuridico della Direttiva ex art. 288, par. 3 del Trattato sul funzionamento dell'Unione europea: al fine di predisporre una normativa flessibile, senza imporre rigidamente agli Stati membri specifiche misure da adottare. Con essa, si è cercato di uniformare le normative nazionali in materia di sicurezza informatica, che si trovavano a diversi livelli di preparazione.

La Direttiva NIS si articola su due pilastri: da un lato un'architettura multilivello per la gestione degli incidenti informatici (governance); dall'altro, un regime di conformità per la sicurezza informatica di determinati soggetti.

Costituiscono l'architettura del sistema NIS, il «Gruppo di cooperazione»13 e la «Rete di CSIRT»14 che, quali organi di livello unionale, si interfacciano con gli organi di livello nazionale individuati dagli Stati membri. In particolare, i Paesi dell'Unione europea sono tenuti ad individuare una o più «autorità nazionali competenti in materia di sicurezza della rete e dei sistemi informativi»15, un «punto di contatto unico»16 ed almeno un «CSIRT»17 (computer security incident responce team, ossia una «squadra di intervento per la sicurezza informatica in caso di incidente»). Sommariamente, compito di questi organi è interfacciarsi e comunicare tra di loro ed i rispettivi omonimi instaurati negli altri Stati membri, al fine di scambiarsi quelle informazioni necessarie per prevenire incidenti informatici e contrastare i loro effetti negativi. I CSIRT, nello specifico, si occupano della prevenzione e della gestione degli incidenti informatici, in concreto.

Quanto al secondo pilastro, sono soggetti a rischio informatico18, coloro che operano in determinati settori socioeconomici o erogano specifici servizi digitali, espressamente individuati dalla Direttiva NIS (allegati II e III). Essa distingue due categorie di soggetti: «operatori di servizi essenziali» e «fornitori di servizi digitali».

Un «operatore di servizi essenziali» è un soggetto pubblico o privato che svolge un'attività rientrante in uno dei seguenti sette settori: «energia»; «trasporti»; «banca»; «infrastrutture dei mercati finanziari»; «sanità»; «fornitura e distribuzione di acqua potabile»; «infrastrutture digitali»19. Inoltre, è identificato «operatore di servizi essenziali» quel soggetto che fornisce un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali, la cui fornitura dipende dalla rete e dai sistemi informativi, per cui un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio20.

CamminoDiritto.it
ISSN 2421-7123

Un «fornitore di servizi digitali» è una «qualsiasi persona giuridica che fornisce un servizio digitale»21, ossia un qualsiasi servizio della società dell'informazione prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi22 e che rientri nei tipi di servizi individuati nell'allegato III della Direttiva NIS, ossia: servizi di mercato online23; servizi di motore di ricerca online24; servizi cosiddetti della nuvola25 («cloud computing»). Inoltre, mentre i «fornitori di servizi digitali» sono individuati come tali ex lege, gli «operatori di servizi essenziali» necessitano di essere individuati direttamente dagli Stati membri26, a séguito di un processo di identificazione che l'Italia ha attribuito in capo all'«autorità nazionale competente NIS» e alle «autorità di settore»27.

La Direttiva NIS prevede, nei confronti di «operatori di servizi essenziali» e «fornitori di servizi digitali», specifici obblighi in materia di sicurezza informatica, sostanzialmente riconducibili: da un lato, in misure di sicurezza in senso stretto; dall'altro, nella notifica di incidenti. Mediante le misure di sicurezza, i soggetti si dotano di regole interne idonee a prevenire e gestire gli incidenti; mediante l'esercizio della notifica, essi rendono noto alle autorità competenti dell'incidente subìto. Prevede anche un regime di vigilanza ed esecuzione (disciplinato poi in concreto dagli Stati membri) nei confronti di quegli «operatori di servizi essenziali» e «fornitori di servizi digitali», che omettono di conformarsi ai doveri di sicurezza.

La Direttiva NIS è stata recepita dall'Italia con il Decreto legislativo 18 maggio 2018, n. 6528, in attuazione della delega contenuta nella Legge 25 ottobre 2017, n. 16329.

Il legislatore delegato italiano aveva inizialmente individuato una pluralità di «autorità nazionali competenti», ognuna responsabile per i vari settori e servizi individuati dalla Direttiva NIS. A séguito dell'entrata in vigore del Decreto-Legge n. 82/2021 (v. infra, par. 4), si decide di costituire una sola «autorità nazionale competente», definita dalla normativa italiana «autorità nazionale competente NIS», mentre gli enti precedentemente individuati quali «autorità nazionali competenti», vengono ora designati quali «autorità di settore»30. La creazione delle «autorità di settore» da parte del legislatore italiano pare essere quella di realizzare uno stretto raccordo funzionale tra la nuova Agenzia per la cybersicurezza nazionale, quale «autorità nazionale competente NIS», e tali autorità, non vanificando il lavoro svolto dalle stesse, fino alla modifica normativa.

Le «autorità di settore» sono: il Ministero dello sviluppo economico, per il settore «infrastrutture digitali» e per i «servizi digitali»; il Ministero delle infrastrutture e della mobilità sostenibili, per il settore «trasporti»; il Ministero dell'economia e delle finanze, in collaborazione con la Banca d'Italia e la CONSOB, per i settori «banca» ed «infrastrutture dei mercati finanziari»; il Ministero della salute, per il settore «sanità»,

CamminoDiritto.it
ISSN 2421-7123

direttamente o per il tramite delle autorità sanitarie territorialmente competenti; il Ministero della transizione ecologica, per il settore «energia» e, insieme alle Regioni e le Province autonome di Trento e Bolzano, direttamente o per il tramite delle autorità territorialmente competenti, per il settore «fornitura e distribuzione di acqua potabile».

Per quanto invece riguarda il «punto di contatto unico», il Decreto legislativo n. 65/2018 (di seguito, anche "Decreto legislativo NIS") lo aveva originariamente individuato nella figura del Dipartimento delle informazioni per la sicurezza31, organo del «Sistema di informazione per la sicurezza della Repubblica». Il Decreto-Legge n. 82 trasferisce le funzioni di «punto di contatto unico», dal Dipartimento delle informazioni per la sicurezza all'Agenzia per la cybersicurezza nazionale32.

In maniera simile, il CSIRT Italiano, originariamente istituito presso il DIS dal Decreto legislativo NIS, è stato trasferito, con il Decreto-Legge n. 82, presso l'Agenzia per la cybersicurezza nazionale33; ora è denominato «CSIRT Italia»34.

3. L'esigenza di revisione: la proposta di Direttiva NIS2

Il 16 dicembre 2020, la Commissione europea ha adottato un atto interno di proposta di Direttiva del Parlamento europeo e del Consiglio dell'Unione, idoneo ad abrogare e sostituire la vigente Direttiva NIS. La revisione della stessa è espressamente contemplata dal suo considerando n. 71, affermando come la Commissione europea debba necessariamente riesaminarla, a scadenze regolari, in funzione delle evoluzioni della società, della politica, delle tecnologie o delle condizioni del mercato.

Come si legge nella relazione alla proposta di revisione35, essa «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 cybersicurezza e della protezione delle infrastrutture critiche. Essa è in linea con le priorità della Commissione [europea] di preparare l'Europa per l'era digitale e costruire un'economia pronta per le sfide del futuro e al servizio dei cittadini».

Nonostante i risultati raggiunti dalla Direttiva NIS, in termini di miglioramento del livello di capacità di ripresa dell'Unione europea in materia di sicurezza informatica e nel completamento dei quadri nazionali di strategia di sicurezza informatica nazionale, essa ha rivelato carenze che le impediscono di affrontare efficacemente il rischio informatico nella società attuale.

La proposta di revisione si prefigge di modernizzare il quadro giuridico esistente, tenendo

CamminoDiritto.it
ISSN 2421-7123

conto, della crescente informatizzazione del mercato interno dell'Unione avvenuta negli ultimi anni, nonché dell'evoluzione delle minacce di tipo informatico; la crisi pandemica da SARS-CoV-2, ha ulteriormente amplificato tali fenomeni – come segnala la relazione.

La proposta di revisione tiene anche conto del fatto che alcuni soggetti non sono rientrati nell'ambito di applicazione della Direttiva NIS, pur svolgendo quelle attività tipizzate dalla Direttiva; perciò, tali soggetti non sono stati tenuti ad attuare le dovute misure di sicurezza. In particolare, la relazione fa riferimento ad alcuni ospedali nel territorio dell'Unione che, per via della discrezionalità e della normativa interna nazionale, non sono rientrati nell'ambito di applicazione della Direttiva NIS.

La proposta di revisione mira a ridurre gli oneri sia a carico delle autorità competenti, sia a carico dei soggetti destinatari dei doveri di sicurezza. Viene proposto di raggiungere tale obiettivo, abolendo – per gli Stati membri – l'obbligo di individuare gli operatori di servizi essenziali, ed aumentando il livello di armonizzazione dei requisiti di sicurezza e segnalazione tra i diversi soggetti, allo scopo di facilitare la conformità normativa per coloro i quali offrono servizi transfrontalieri.

La revisione della Direttiva NIS verrà compiuta adottando una nuova Direttiva europea, che abrogherà e sostituirà la Direttiva NIS. La scelta dello strumento della Direttiva è funzionale al fine di dotare gli Stati membri della flessibilità necessaria per tenere conto, in sede di recepimento, delle varie specificità nazionali – secondo quanto riportato nella relazione. Le Direttive europee, ai sensi dell'art. 288, par. 3, del Trattato sul funzionamento dell'Unione europea, vincolano gli Stati membri quanto agli scopi da realizzare, enunciati nelle stesse Direttive36.

Le modifiche degne di segnalazione, rispetto alla vigente Direttiva NIS, riguardano principalmente la formula dell'intitolazione della nuova Direttiva e la disciplina dei nuovi soggetti destinatari dei doveri di sicurezza.

La proposta di Direttiva NIS2 reca l'intitolazione: «Direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148». Viene sostanzialmente ripreso il titolo dato alla Direttiva NIS, ma ciò che salta all'occhio è la sostituzione della formula «sicurezza delle reti e dei sistemi informativi nell'Unione» di cui alla NIS, con il vocabolo «cibersicurezza»37 nella NIS2. Da ciò discendono due problemi.

Se con la nuova Direttiva non si farà più riferimento alla mera network and information security ma, come da intitolazione, alla cybersicurezza, in che rapporto starà questo nuovo atto, disciplinante la «cybersicurezza» a livello europeo, rispetto al Regolamento – (UE)

CamminoDiritto.it
ISSN 2421-7123

2019/881 – sulla cybersicurezza? Tale Regolamento disciplina un ambito differente rispetto a quello della Direttiva NIS (e poi NIS2): disciplina, infatti, l'istituzione ed il funzionamento della "nuova" Agenzia dell'Unione europea per la cibersicurezza38, nonché il quadro europeo di certificazione della cybersicurezza per prodotti, servizi e processi informatici. Tale Regolamento sulla cybersicurezza (così denominato nella sua intitolazione) disciplina elementi che certamente contribuiscono alla sicurezza informatica dell'Unione europea, ma non si occupa dell'architettura, della governance, della sicurezza informatica europea. La sua intitolazione sarebbe da rivedere.

Ulteriore problema – che non può essere univocamente ed esclusivamente risolto nell'ambito del diritto – è quello di comprendere cosa si debba realmente intendere per cybersicurezza, e quindi individuare una definizione, almeno normativa, che sia armonica in tutto il territorio dell'Unione europea.

Per quanto riguarda la disciplina dei soggetti a rischio informatico, quelli destinatari dei doveri di sicurezza, la Direttiva NIS2, come aveva fatto la NIS, individua due categorie di soggetti.

La bipartizione operata dalla Direttiva NIS – secondo la relazione alla proposta di revisione – si è rivelata obsoleta, in quanto non più riflettente l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno. L'ambito di applicazione dei settori della Direttiva NIS2 dovrebbe essere esteso a una parte più ampia dell'economia e della società. I settori contemplati dalla Direttiva NIS dovrebbero pertanto essere ampliati, per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche, nel mercato interno dell'Unione.

La proposta di Direttiva NIS2 individua: da un lato, «soggetti essenziali»; dall'altro, «soggetti importanti».

Diversamente dalla Direttiva NIS, nella NIS2 – al fine di eliminare le divergenze tra gli Stati membri quanto all'individuazione dei soggetti destinatari dei doveri di sicurezza e garantire la certezza del diritto per quanto riguarda tali doveri per tutti i soggetti pertinenti – si stabilisce un criterio uniforme che determina quali soggetti debbano rientrare nell'ambito di applicazione della nuova Direttiva. Dunque, gli Stati membri non dovranno più individuare i soggetti destinatari dei doveri di sicurezza: in particolare, gli «operatori di servizi essenziali» di cui alla Direttiva NIS.

La Direttiva NIS2 individua, quale criterio per l'individuazione dei soggetti destinatari dei doveri di sicurezza, la dimensione del soggetto: rientrerebbero nell'ambito di applicazione

CamminoDiritto.it
ISSN 2421-7123

della Direttiva NIS2, tutte le medie e le grandi imprese39, che operano nei settori o forniscono il tipo di servizi contemplati dalla stessa Direttiva – con delle eccezioni.

Ai sette settori individuati dalla Direttiva NIS, la NIS2 ne aggiunge tre nuovi: «acque reflue», «pubblica amministrazione» e «spazio». Vengono inoltre aggiunti dei nuovi sottosettori, ai settori già previsti dalla Direttiva NIS.

È interessante notare come la categoria «fornitori di servizi digitali» di cui alla Direttiva NIS, nella NIS2 venga trasformata – e quindi regredita, per così dire – ad un mero settore economico all'interno della categoria dei «soggetti importanti»40.

Significativa è la novità di prevedere una disciplina unitaria quanto ai doveri di sicurezza, quindi applicabile sia ai «soggetti essenziali» che ai «soggetti importanti». La NIS2 supera così la precedente impostazione, che prevedeva un differente regime quanto agli obblighi di sicurezza, per «operatori di servizi essenziali» e «fornitori di servizi digitali»41.

Entrambe le categorie di soggetti saranno poi tenute ad individuare, internamente alla loro organizzazione, un organo di gestione dei rischi di cybersicurezza, competente: ad approvare le misure di sicurezza adottate dall'ente, al fine di conformarsi alle prescrizioni normative; a vigilare sulle stesse. I membri di tale organo di gestione dovranno seguire periodicamente attività di formazione, al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi di cybersicurezza e le relative pratiche di gestione42.

Inoltre, all'istituto della notifica di incidente disciplinato dalla Direttiva NIS, la NIS2 vi sostituisce l'istituto della segnalazione: consistente nell'invio di una notifica iniziale, entro 24 ore dalla scoperta dell'incidente informatico, seguita, se richiesta, da una relazione di aggiornamento della situazione e poi da una relazione finale, da inviare entro un mese dalla prima notifica43.

Quanto alle novità in ambito sanzionatorio, la NIS2 individua un regime di vigilanza ed esecuzione differenziato per «soggetti essenziali» e «soggetti importanti», con la peculiarità che, mentre per i «soggetti essenziali» l'attività di vigilanza – per il mancato rispetto degli obblighi di cui alla Direttiva NIS2 – è sia preventiva che successiva, per i «soggetti importanti» essa è prevista solo ex post. E ciò, al fine di ridurre gli oneri rispetto alla conformità dei «soggetti importanti», in quanto non svolgenti funzioni ritenute essenziali44.

CamminoDiritto.it
ISSN 2421-7123

4. La normativa italiana in materia, alla prova dell'entrata in vigore della Direttiva NIS2

Nelle more del recepimento della Direttiva NIS – entrata in vigore nel 2016 –, il Governo italiano, nel 2017, con Decreto del Presidente del Consiglio dei ministri, ha adottato la «Direttiva sugli indirizzi di protezione cibernetica e sicurezza informatica nazionali»45, cui è seguito l'anno successivo il Decreto legislativo NIS.

A quest'ultimo atto, nel 2019, si aggiunge il Decreto-Legge n. 10546 (convertito, con modificazioni, con la Legge n. 133/201947), che introduce la disciplina del «perimetro di sicurezza nazionale cibernetica».

Il Governo prima ed il legislatore della conversione poi, accanto al sistema imposto dall'ordinamento sovranazionale-europeo di cui alla Direttiva NIS, decidono di affiancarvi uno strumento giuridico ulteriore in materia di sicurezza informatica. Il «perimetro», infatti, non rientra tra i doveri che la Direttiva NIS impone agli Stati membri. Esso rappresenta una scelta politica tutta italiana, nata dal lavoro del comparto intelligence48, che ne ha promosso l'iniziativa.

Il sistema del «perimetro di sicurezza nazionale cibernetica»49 come si ricava dalla formula impiegata per denominarlo, si occupa di disciplinare un settore specifico della sicurezza nazionale50 – un sottosettore, quello della sicurezza informatica nazionale – che attiene alla tutela della sicurezza nazionale da azioni o eventi a danno di sistemi informatici generalmente intesi, nella disponibilità di attori nazionali, tanto pubblici quanto privati, che esercitano una funzione essenziale dello Stato oppure hanno carattere strategico per gli interessi del Paese. Più semplicemente, azioni o eventi, tali da arrecare un pregiudizio proprio alla sicurezza nazionale51 e quindi all'ordinamento giuridico nel suo complesso.

Il «perimetro» si fonda su due pilastri, ricalcando sostanzialmente il sistema della Direttiva NIS. Da un lato (primo pilastro), individua criteri per l'identificazione di soggetti da includere nel «perimetro» (cosiddetti "soggetti perimetrati") e, dall'altro lato (secondo pilastro), introduce un regime di conformità dei doveri in materia di sicurezza informatica per tali soggetti, prevedendo anche un regime di vigilanza ed esecuzione per la mancata conformità.

Lo spirito del sistema «perimetro» è quello di costruire una cornice normativa – un perimetro, appunto – per tutti quei soggetti pubblici e privati, dai quali discenderebbe un pregiudizio – non solo per loro ma anche, nello specifico, – per la sicurezza nazionale, in caso di incidente informatico subìto, indipendentemente dal fatto che tali soggetti siano

CamminoDiritto.it
ISSN 2421-7123

già stati individuati come destinatari della Direttiva NIS.

L'approccio italiano pare dunque essere quello del "non lasciare nessuno fuori": individuare, sia grazie alla Direttiva NIS, sia tramite il «perimetro», tutti quei soggetti pubblici e privati per cui un incidente informatico avrebbe effetti negativi, a vario titolo, sull'ordinamento in generale – oltreché, ovviamente, sullo stesso soggetto-vittima dell'incidente.

Il Governo italiano della XVIII legislatura – l'attuale, presieduto da Mario Draghi –, nel 2021, adotta il Decreto-Legge n. 82, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»52 (convertito, con modificazioni, con la Legge n. 109/202153). Il nuovo atto d'urgenza riforma il quadro normativo in materia di sicurezza informatica (nazionale).

Tale Decreto-Legge (di séguito, anche "Decreto-Legge cybersicurezza"54) definisce una nuova architettura nazionale in materia di sicurezza informatica, accentrando gran parte delle competenze in materia nella nuova Agenzia per la cybersicurezza nazionale, trasferendole dal comparto intelligence, cui originariamente appartenevano.

Il quadro normativo italiano in materia di sicurezza informatica, risulta quindi essere composto da una pluralità di atti, legislativi (delegati, d'urgenza e di conversione) ed amministrativi, uno connesso all'altro, nella misura in cui uno rinnova l'altro, che disegnano un sistema di governo deputato a prevenire incidenti informatici, rispondendo ad essi, subiti da determinati soggetti ritenuti strategici per le attività che svolgono, tutelando sia essi che, di conseguenza, l'ordinamento in generale. Una pluralità di atti che sicuramente non aiuta gli operatori e l'interprete, sia dal lato della governance che dal lato dei soggetti tenuti a conformarsi – con anche il rischio di creare maggiori oneri nei confronti di tali soggetti.

Con la verosimile approvazione della Direttiva NIS2 e la sua entrata in vigore, gli Stati membri saranno tenuti a recepirla all'interno dei propri ordinamenti nazionali. L'Italia vi provvederà mediante l'emanazione di un Decreto legislativo, sulla base della delega del Parlamento al Governo, che verrà disposta nella Legge di delegazione europea55.

L'ordinamento italiano dovrà quindi, non solo rinnovare il testo del Decreto legislativo NIS, ma creare anche un necessario raccordo tra la nuova disciplina di matrice europea e gli altri atti normativi nazionali in materia: sistema «perimetro» ed «architettura nazionale di cybersicurezza» (definita nel Decreto-Legge cybersicurezza).

CamminoDiritto.it
ISSN 2421-7123

Con l'entrata in vigore della Direttiva NIS2, il punto maggiormente critico starà nel recepimento della disciplina avente ad oggetto i nuovi «soggetti essenziali» ed «importanti», che andranno a sostituire le attuali categorie degli «operatori di servizi essenziali» e «fornitori di servizi digitali» di cui alla Direttiva NIS. La criticità starà, in particolare, nel costruire un efficace raccordo tra la disciplina di tali nuovi soggetti e quella di cui al sistema «perimetro». È infatti molto probabile che diversi soggetti rientrati nell'ambito di applicazione della Direttiva NIS56, siano anche stati perimetrati57. Infatti, gli «operatori di servizi essenziali» ed i «fornitori di servizi digitali», se esercitanti funzioni essenziali per lo Stato o se prestatori di servizi essenziali per lo Stato58, possono essere individuati quali soggetti da includere nel «perimetro»; in tal caso, essi vengono qualificati anche come soggetti perimetrati e quindi saranno tenuti ad osservare anche le disposizioni previste dal sistema «perimetro».

Nello specifico, tali soggetti devono osservare i doveri di sicurezza previsti dal Decreto legislativo NIS, se di livello almeno equivalente a quelle prescritte dal sistema «perimetro»59; eventuali divergenze dovranno essere colmate da misure aggiuntive definite dall'Agenzia per la cybersicurezza nazionale, necessarie al fine di assicurare i livelli di sicurezza previsti dal sistema «perimetro»60.

A ciò si aggiunge che, tra i nuovi settori di attività dei «soggetti essenziali», la Direttiva NIS2 introdurrà quello delle «pubbliche amministrazioni». Ciò risulterà un poco problematico, in quanto il sistema «perimetro» definisce i soggetti perimetrati – proprio – le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati, aventi una sede nel territorio nazionale61. Il legislatore delegato italiano dovrà quindi trovare il modo per rispettare la Direttiva NIS2, assoggettando le pubbliche amministrazioni (ora definite soggetti perimetrati) alla nuova disciplina europea, cercando, al tempo stesso, di non stravolgere l'impianto del sistema «perimetro».

La criticità quanto alla disciplina dei soggetti a rischio informatico, non sta solo nella loro individuazione, ma pure nella previsione del regime di conformità quanto ai loro doveri di sicurezza. La Direttiva NIS prevede un differente regime di conformità per «operatori di servizi essenziali» e «fornitori di servizi digitali»; e ciò in quanto, secondo la Direttiva NIS62, i «fornitori di servizi digitali» sono esposti ad un rischio meno elevato rispetto agli «operatori di servizi essenziali», poiché i servizi erogati da questi ultimi sono spesso essenziali per il mantenimento delle attività sociali ed economiche critiche63.

Pertanto, gli obblighi di sicurezza per i «fornitori di servizi digitali» sono meno rigidi rispetto a quelli prescritti per gli «operatori di servizi essenziali». Il sistema «perimetro» prevede un differente – seppur in linea di principio simile –, regime per i propri soggetti perimetrati. La Direttiva NIS2 introdurrà invece un regime unico quanto ai «soggetti

CamminoDiritto.it
ISSN 2421-7123

essenziali» ed «importanti», sostituendo quello di cui alla Direttiva NIS. Anche qui, il punto starà nello sviluppare il giusto raccordo tra le due discipline – NIS2 e «perimetro» –, anche e soprattutto in funzione di quei soggetti che, verosimilmente, rientreranno nel campo di applicazione della NIS2 e al tempo stesso saranno, o verranno, perimetrati.

A conferma di quanto detto, va aggiunto che alcune delle attività tipiche svolte dai soggetti destinatari della Direttiva NIS («operatori di servizi essenziali» e «fornitori di servizi digitali»), sono così essenziali per lo Stato, al punto che una loro compromissione non può non essere considerata come pregiudizio per l'ordinamento nel suo complesso e di conseguenza, pregiudizio per la sicurezza nazionale. Si pensi alla compromissione delle capacità energetiche di un Paese: il settore «energia», non a caso, è il primo settore di attività contemplato nell'allegato II della Direttiva NIS64. Oppure, quanto ai servizi di «cloud computing»: si pensi alla violazione dei dati di pubbliche amministrazioni e di istituzioni repubblicane. O ancora, quanto al settore «sanità», per ciò che riguarda la violazione dei dati65, il funzionamento dei sistemi informatici per attività sanitarie, finanche il funzionamento di dispositivi biomedici – che si basano anch'essi su sistemi informatici.

Tutto ciò determina una palese sovrapposizione tra la normativa europea NIS e quella italiana di cui al sistema «perimetro», specificatamente posta a tutela della sicurezza nazionale – che rimane materia di competenza dei singoli Stati membri66.

5. Conclusioni

Il sistema «perimetro» risulta essere perfettamente in sintonia con lo spirito della normativa NIS, di prevedere misure giuridiche volte ad incrementare il livello complessivo di sicurezza informatica nell'Unione e, quanto al «perimetro», in Italia. Entrambi gli strumenti giuridici hanno uno scopo tendenzialmente comune, nella misura in cui il «perimetro» introduce una disciplina con l'intento esplicitamente dichiarato, di tutelare la sicurezza nazionale.

Non solo. Tutti e tre gli strumenti – NIS (e NIS2), «perimetro di sicurezza nazionale cibernetica», «architettura nazionale di cybersicurezza» – sono palesemente tra di loro collegati, in quanto disciplinano la medesima materia: la sicurezza informatica nazionale. Le normative NIS e «perimetro» si occupano del regime di sicurezza informatica per determinati soggetti a rischio informatico; NIS prima e Decreto-Legge cybersicurezza poi, disciplinano, insieme, l'architettura istituzionale in materia di sicurezza informatica (la governance).

La normativa NIS è stata introdotta, come si è detto, mediante lo strumento della Direttiva

CamminoDiritto.it
ISSN 2421-7123

europea. Le Direttive – come già detto – vincolano gli Stati membri quanto agli scopi, non quanto ai mezzi per realizzarli. Il legislatore italiano del 2019, avrebbe dunque potuto modificare il Decreto legislativo NIS, introducendo nell'ordinamento italiano il sistema «perimetro», venendo alla luce come una modifica dello stesso Decreto legislativo: ciò non avrebbe pregiudicato gli scopi della Direttiva NIS; semplicemente, si sarebbe potenziata la normativa italiana di sicurezza informatica, senza l'aggiunta di un nuovo, ulteriore e separato, atto in materia (quale è stato il Decreto-Legge disciplinante il «perimetro»).

Si sarebbero così potute evitare inutili duplicazioni – che, in generale, determinano poi sul piano pratico-applicativo, un incremento farraginoso di lavoro degli uffici nonché difficoltà nel recepimento delle misure da parte dei soggetti destinatari.

La complessità, dovuta anche alle criticità che deriveranno dal recepimento della Direttiva NIS2, potrebbe così trasformarsi in una opportunità per il legislatore italiano: quella di riformare la normativa in materia, dando alla luce un testo di legge a carattere organico in tema di sicurezza informatica nazionale – a beneficio di istituzioni, operatori ed interprete – che raggiunga gli obiettivi previsti dalla NIS2 e al tempo stesso tenga conto delle specificità nazionali in materia. Un unico testo legislativo che disciplini, una volta per tutte, quanto ai soggetti a rischio informatico e quindi quanto alla loro identificazione ed al loro regime di conformità per la sicurezza informatica, evitando sovrapposizioni tra normative diverse.

La relazione alla proposta di Direttiva NIS2, afferma chiaramente che la scelta di rivedere la Direttiva NIS attraverso il medesimo strumento della Direttiva europea, è funzionale a dotare gli Stati membri della flessibilità necessaria per tenere conto delle loro specificità nazionali, e ciò, anche al fine di individuare – come si legge – ulteriori soggetti destinatari dei doveri di sicurezza.

Perciò, accanto ai «soggetti essenziali» ed «importanti» di cui alla NIS2, il legislatore italiano potrebbe, per esempio, affiancarvi una nuova categoria di soggetti, corrispondenti agli attuali soggetti perimetrati di cui al «perimetro»; verrebbe quindi a delinearsi non una bipartizione, bensì una tripartizione di soggetti a rischio informatico, destinatari dei doveri di sicurezza. Oppure, potrebbe creare una nuova tipologia di «soggetti essenziali», portatori di interessi nazionali, e quindi corrispondenti agli attuali soggetti perimetrati, specificando poi il differente regime di conformità applicabile ad essi.

Più in generale, il legislatore italiano, in sede di recepimento della NIS2, potrebbe traslare la disciplina del «perimetro», integrandola in quello che sarà l'atto interno di recepimento della Direttiva NIS2, in quanto il recepimento di una Direttiva non richiede una esatta

CamminoDiritto.it
ISSN 2421-7123

riproduzione delle sue disposizioni nell'atto interno. Come già detto, la Direttiva NIS2 verrà recepita mediante un Decreto legislativo, a séguito di specifica delega del Parlamento al Governo. Perciò spetterà al legislatore, l'onere di formulare una delega che, oltre a disporre il mero recepimento della NIS2, contempli anche un efficace coordinamento della normativa in materia, nelle more del recepimento stesso67.

Così facendo, si andrebbe a formare una normativa unitaria che abbraccerebbe le normative NIS e «perimetro», avente ad oggetto il regime di sicurezza informatica per i cosiddetti soggetti a rischio, necessariamente coordinata con la disciplina dell'«architettura nazionale di cybersicurezza».

Nelle more della redazione e pubblicazione di questo articolo, la proposta di Direttiva NIS2 è in attesa della posizione del Parlamento europeo in prima lettura, ex art. 294, paragrafi 3-6, del Trattato sul funzionamento dell'Unione europea.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

1 Si sviluppa attraverso tre letture eventuali. La Commissione europea presenta una proposta di Regolamento, Direttiva o Decisione al Parlamento europeo e al Consiglio dell'Unione: il Parlamento adotta la sua posizione e la trasmette al Consiglio. Se il Consiglio la approva, l'atto è adottato e la procedura si chiude; se, invece, non la approva, adotta la sua posizione e la trasmette al Parlamento. Si apre la seconda lettura. Il Parlamento può approvare la posizione del Consiglio e in tal caso l'atto viene adottato e la procedura si chiude; oppure, può respingere la posizione del Consiglio, cosicché l'atto non viene adottato con chiusura della procedura; altrimenti, può emendare l'atto rinviandolo al Consiglio. Il Consiglio, a sua volta, in seconda lettura: può approvare l'atto emendato trasmessogli dal Parlamento e in tal caso l'atto viene adottato e la procedura si chiude; oppure, può non approvare l'atto trasmessogli, con conseguente convocazione del comitato di conciliazione, avente il compito di trovare un accordo su di un progetto comune. In caso di mancato accordo, l'atto non entra in vigore e la procedura si chiude; se invece viene concordato un progetto comune, questo viene trasmesso al Parlamento e al Consiglio per la terza lettura. In terza lettura, se entrambe le istituzioni approvano il progetto comune, l'atto viene adottato e la procedura si chiude; se anche una sola delle due istituzioni respinge il progetto comune o non si pronuncia, l'atto non viene adottato con conseguente chiusura della procedura.

2 Gazzetta Ufficiale dell'Unione europea (serie L) del 19 luglio 2016, n. 194.

3 D. CRAIGEN, N. DIANKUN-THIBAULT, R. Purse, Defining Cybersecurity, in Technology Innovation Management Review, 2014, 4, 13-21.

4 Art. 2, punto 2, Direttiva NIS.

5 Regolamento (UE) 2019/881 (Gazzetta Ufficiale dell'Unione europea (serie L) del 7 giugno 2019, n. 151).

6 Art. 2, punto 1, Regolamento (UE) 2019/881.

7 Di cui al Decreto-Legge n. 82/2021 (v. infra, par. 4).

8 Art. 1, lett. a), Decreto-Legge n. 82/2021.

9 Quanto la gestione pratica della sicurezza informatica in ambito aziendale, si veda a proposito G. ZICCARDI, Sicurezza informatica, protezione dei dati e nuove strategie digitali per la piccola e media impresa 4.0, in Quaderni di ricerca sull'artigianato, 2017, 2 (DOI: {https/URL}); G. ZICCARDI, La protezione dei dati nel contesto della piccola e media impresa tra GDPR e cybersecurity, in Quaderni di ricerca sull'artigianato, 2020, 1 (DOI: {https/URL}).

10 L'art. 4, punto 7, Direttiva NIS, definisce incidente informatico «ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi». Il successivo art. 4, punto 8, definisce invece trattamento dell'incidente, «tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente». L'art. 4, punto 5, della proposta di Direttiva NIS2, definirà, verosimilmente, l'incidente come «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei relativi servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi». Un incidente informatico, per la normativa in materia, consiste in un evento derivante, o da una condotta umana, oppure da un mero evento naturale e cioè non direttamente derivante da una condotta umana, idoneo ad arrecare un danno ad un sistema informatico, che si trova nella disponibilità del soggetto-vittima dell'incidente, in termini di violazione dei dati e/o compromissione del fisiologico funzionamento del sistema stesso.

11 Cfr. considerando n. 31, Direttiva NIS.

12 Si riporta, per intero, il testo del considerando n. 3, Direttiva NIS: «Le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno».

CamminoDiritto.it
ISSN 2421-7123

13 Art. 11, Direttiva NIS.

14 Art. 12, Direttiva NIS.

15 Art. 8, Direttiva NIS.

16 Art. 8, par. 3, Direttiva NIS.

17 Art. 9, Direttiva NIS.

18 Coloro i quali sono destinatari dei doveri di sicurezza di cui alle varie normative in materia. Segnalo che, non sono a rischio informatico solo i soggetti individuati dalle normative sulla sicurezza informatica, ma, in generale, qualsivoglia soggetto, individuale e collettivo. L'uso di questa terminologia è una convezione adottata dal sottoscritto Autore, per riferirsi ai soggetti destinatari dei doveri di sicurezza, ai fini di questo articolo.

19 Art. 4, punto 4 ed allegato II, Direttiva NIS.

20 Art. 5, par. 2, Direttiva NIS.

21 Art. 4, punto 6, Direttiva NIS.

22 Art. 4, punto 5, Direttiva NIS.

23 È definito come «un servizio digitale che consente ai consumatori e/o ai professionisti [...] di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online» (art. 4, punto 17, Direttiva NIS).

24 È definito come «un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto» (art. 4, punto 18, Direttiva NIS).

25 È definito come «un servizio digitale che consente l'accesso a un insieme scalabile e elastico di risorse informatiche condivisibili» (art. 4, punto 19, Direttiva NIS).

26 Art. 5, par. 1, Direttiva NIS.

27 Artt. 4 e 5, Decreto legislativo n. 65/2018.

28 Gazzetta Ufficiale del 9 giugno 2018, n. 132.

29 Gazzetta Ufficiale del 6 novembre 2017, n. 259.

30 Art. 7, comma 1, Decreto legislativo n. 65/2018, come modificato dall'art. 15, comma 1, lett. f), Decreto-Legge n. 82/2021.

31 Istituito dall'art. 4, Legge n. 124/2007 (Gazzetta Ufficiale del 13 agosto 2007, n. 187), recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto».

32 Art. 7, comma 3, Decreto legislativo n. 65/2018, come modificato dall'art. 15, comma 1, lett. f), Decreto-Legge n. 82/2021.

33 Art. 8, comma 1, Decreto legislativo n. 65/2018, come modificato dall'art. 15, comma 1, lett. h), Decreto-Legge n. 82/2021.

34 Art. 7, comma 3, Decreto-Legge n. 82/2021.

35 Consultabile, insieme al testo della proposta di Direttiva NIS2, su EUR-LEX (URL consultato il 31 gennaio 2022).

36 «La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi.» (art. 288, par. 3, Trattato sul funzionamento

CamminoDiritto.it
ISSN 2421-7123

dell'Unione europea). Cfr. R. ADAM, A. TIZZANO, Lineamenti di Diritto dell'Unione europea, Giappichelli, 2014, 159 ss.

37 Nella versione in lingua inglese è «cybersecurity».

38 In verità, l'Agenzia era già stata istituita con il Regolamento (CE) 2004/460, poi abrogato dal Regolamento (UE) 2013/526, che ha re-istituito l'Agenzia. Quest'ultimo Regolamento è poi stato abrogato dal Regolamento (UE) 2019/881 e l'Agenzia, per la seconda volta, re-istituita.

39 Come definite dalla Raccomandazione 2003/361/CE della Commissione europea, del 6 maggio 2003.

40 Il nuovo settore «fornitori di servizi digitali», contempla i sottosettori: «fornitori di mercati online»; «fornitori di motori di ricerca online»; «fornitori di piattaforme di servizi di social network». Il sottosettore cloud computing della Direttiva NIS, nella NIS2 viene trasformato in un tipo di soggetto rientrante nel settore «infrastrutture digitali», di cui ai nuovi «soggetti essenziali». Ciò pare riflettere la funzione – appunto essenziale – svolta da tale tipologia di servizio: quella di conservare, e consentire l'accesso a, dati di persone ed organizzazioni che, nell'attuale società, sono di grande se non di vitale importanza per gli stessi.

41 La proposta di Direttiva NIS2 fa riferimento ad «obblighi di gestione e segnalazione dei rischi di cibersicurezza», laddove invece la Direttiva NIS fa riferimento ad «obblighi in materia di sicurezza e notifica degli incidenti».

42 Ogni persona fisica operante all'interno di tali soggetti – e non solo –, dovrebbe disporre di un'adeguata educazione al rischio informatico; cfr. M. CARLTON, Y. LEVY, M. RAMIM, Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills, in Information & Computer Security, 2019, 27, 1, 101-121 (DOI: {https/URL}).

43 Art. 20, par. 4, proposta di Direttiva NIS2.

44 Considerando n. 70, proposta di Direttiva NIS2.

45 DPCM 17 febbraio 2017 (Gazzetta Ufficiale del 13 aprile 2017, n. 87). Si segnala che già il DPCM 24 gennaio 2013 (Gazzetta Ufficiale del 19 marzo 2013, n. 66), aveva introdotto un'architettura nazionale in materia di sicurezza informatica; quest'ultimo è stato poi sostituito dal DPCM 17 febbraio 2017.

46 Gazzetta Ufficiale del 21 settembre 2019, n. 222.

47 Gazzetta Ufficiale del 20 novembre 2019, n. 272.

48 «Sistema di informazione per la sicurezza della Repubblica» (Legge n. 124/2007).

49 Il riferimento all'aggettivo «cibernetica» in questo ambito, genera, a mio parere, confusione; cfr. N. WIENER, Cybernetics or Control and Communication in the Animal and the Machine, Quid Pro Books, 2015 (ristampa della 2a ed. di N. WIENER, Cybernetics or Control and Communication in the Animal and the Machine, The M.I.T. Press, 1948).

50 Cfr. E. CAMILLI, Sicurezza nazionale: tra concetto e strategia, in sicurezzanazionale.gov.it (URL consultato il 31 gennaio 2022).

51 Il DPCM 30 luglio 2020, n. 131 (Gazzetta Ufficiale del 21 ottobre 2020, n. 261), recante «Regolamento in materia di perimetro di sicurezza nazionale cibernetica [...]», all'art. 1, lett. f), definisce pregiudizio per la sicurezza nazionale, il «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero gli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale di cui all'articolo 2» dello stesso Decreto.

52 Gazzetta Ufficiale del 14 giugno 2021, n. 140.

53 Gazzetta Ufficiale del 4 agosto 2021, n. 185.

54 La forma linguistica «cybersicurezza», secondo quanto segnalato dall'Accademia della Crusca, non è da ritenersi corretta: è preferibile la forma «cibersicurezza»; cfr. Accademia della Crusca, Gruppo Incipit, Comunicato n. 16: La

CamminoDiritto.it
ISSN 2421-7123

cibersicurezza è importante. L'italiano pure, in accademiadellacrusca.it (URL consultato il 31 gennaio 2022).

55 Legge 24 dicembre 2012, n. 234 (Gazzetta Ufficiale del 4 gennaio 2013, n. 3), recante «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea».

56 A dicembre 2018, sono stati individuati 465 «operatori di servizi essenziali», come riporta una comunicazione sul sito internet del Ministero dello sviluppo economico (URL consultato il 31 gennaio 2022).

57 Ai sensi dell'art. 1, comma 2-bis, Decreto-Legge n. 105/2019, l'elencazione dei soggetti perimetrati è contenuta in un atto amministrativo, non soggetto a pubblicazione, per il quale è escluso il diritto di accesso.

58 Art. 2, comma 1, DPCM 30 luglio 2020, n. 131.

59 Art. 1, comma 8, lett. a), Decreto-Legge n. 105/2019.

60 Ibidem.

61 Art. 1, comma 1, Decreto-Legge n. 105/2019.

62 Considerando n. 49, Direttiva NIS.

63 Cfr. D. MARKOPOULOUA, V. PAPAKONSTANTINOUA, P. DE HERT, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, in Computer Law & Security Review, 2019, 35, 6, 5 ss.

64 Allegato I della proposta di Direttiva NIS2.

65 Cfr. A. MANTELERO, G. VACIAGO, M. S. ESPOSITO, N. MONTE, The common EU approach to personal data and cybersecurity regulation, in International Journal of Law and Information Technology, 2020, 28, 4, 297-328.

66 Si veda a proposito l'art. 1, par. 6, Direttiva NIS.

67 L'art. 32, comma 1, lett. b), Legge n. 234/2012, prevede che «ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione normativi con l'indicazione esplicita delle norme abrogate [...]».

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=8058