La nuova normativa italiana in materia di *cybersecurity* a valle della Direttiva NIS I

31/03/2021 PROTEZIONE DEI DATI E CYBERSECURITY, IT&TMT, PROSPETTIVE

Roberto A. Jacchia
Marco Stillo

In data 5 novembre 2020 è entrato in vigore il Decreto del Presidente del Consiglio dei Ministri n.131/2020[1], con il quale il c.d. "Perimetro di Sicurezza Nazionale Cibernetica" istituito dal Decreto-legge n. 105/2019[2] inizia a prendere forma.

Le minacce cibernetiche che, negli ultimi tempi, si sono sempre più di frequente imposte all'attenzione hanno reso necessario sviluppare in tempi brevi meccanismi difensivi idonei e sempre più stringenti. Se, a livello europeo, questa esigenza è stata affrontata attraverso la c.d. "Direttiva NIS"[3], introdotta nel 2016 per assicurare un elevato livello di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti gli Stati

[1] Decreto del Presidente del Consiglio dei Ministri n.131 del 30.07.2020, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, GU n. 261 del 21.10.2020.
[2] Decreto-legge n. 105 del 21.09.2019, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, GU Serie Generale n. 222 del 21.09.2019, convertito con modificazioni dalla L. n. 133 del 18.11.2019, GU 133 del 20.11.2019.
[3] Direttiva 2016/1148/UE del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GUUE L 194 del 19.07.2016.

Membri[4], a livello nazionale è il decreto legislativo n. 65/2018[5] a dettare la cornice legislativa delle misure di sicurezza delle reti e dei sistemi informativi e ad individuare i relativi soggetti responsabili.

Successivamente, il Decreto-legge n. 105/2019 aveva definito le modalità e le procedure per l'istituzione del Perimetro di sicurezza nazionale cibernetica, volto ad assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale e che esercitano le c.d. "funzioni e servizi essenziali" dello Stato, e dal cui malfunzionamento, interruzione o utilizzo improprio potrebbe derivare un pregiudizio alla sicurezza nazionale[6]. La determinazione delle modalità e dei criteri procedurali per individuare i soggetti inclusi nel Perimetro, tuttavia, era stata rinviata ad un successivo intervento regolatorio. Il DPCM 131/2020 stabilisce tali modalità e criteri, individuando i settori di attività in cui operano i soggetti inseriti nel Perimetro e definendo i parametri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici.

Più particolarmente, ai sensi del DPCM 131/2020 un soggetto esercita funzioni essenziali qualora abbia il compito di assicurare, tra le altre cose, la continuità dell'azione di Governo e degli organi costituzionali, la sicurezza all'interno e all'esterno dei confini nazionali, la difesa dello Stato e l'amministrazione della giustizia. Un soggetto presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, invece, laddove ponga in essere attività necessarie per l'esercizio e il godimento dei diritti fondamentali, o necessarie alla continuità degli approvvigionamenti e all'efficienza delle infrastrutture della logistica e della ricerca[7]. Si tratta, dunque, di categorie di riferimento molto

[4] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[5] Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GU n.132 del 09.06.2018.
[6] L'articolo 1 del Decreto-legge n. 105/2019, intitolato "Perimetro di sicurezza nazionale cibernetica", al comma 1 dispone: "*... Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica...*".
[7] L'articolo 2 del DPCM 131/2020, intitolato "Soggetti che esercitano funzioni essenziali e servizi essenziali", ai commi 1-2 dispone: "*... Ai fini di quanto previsto dall'articolo 1, comma 2, lettera a), del decreto-legge:*
a) un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti;
b) un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, di seguito servizio essenziale, laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.
Gli Organi costituzionali, ove intendano adottare, per le proprie reti e i propri sistemi informativi e servizi informatici, misure di sicurezza analoghe a quelle previste da decreto-legge, possono concludere per tali finalità appositi accordi con il Presidente del Consiglio dei ministri…".

ampie che conseguentemente consentono un'ampia perimetrazione.

Tali soggetti (150 circa) saranno sottoposti alle disposizioni del Perimetro qualora facenti parte di settori rilevanti per la sicurezza nazionale cibernetica. Nello specifico, in base al criterio di gradualità[8] si tratterà dei soggetti che operano nel settore governativo (che riguarda, nell'ambito delle attività di amministrazione dello Stato, quelle svolte dalle amministrazioni che compongono il Comitato Interministeriale per la Sicurezza della Repubblica, CISR[9]) nonché degli altri soggetti pubblici e privati che operano nei settori dell'interno, della difesa, dello spazio e aerospazio, dell'energia, delle telecomunicazioni, dell'economia e finanza, dei trasporti, dei servizi digitali, delle tecnologie critiche, degli enti previdenziali e del lavoro[10]. Anche in questo caso, non sfuggirà l'ampiezza dell'elencazione, che investe concretamente tutti i gangli essenziali del funzionamento dello Stato, della difesa e dell'economia.

L'individuazione e l'elencazione effettiva dei soggetti che rientrano nel Perimetro verrà svolta dall'amministrazione competente per il singolo settore[11], che dovrà identificare le funzioni e i servizi

[8] L'articolo 1 del Decreto-legge n. 105/2019 al comma 2-bis dispone: "… *L'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti*…".

[9] Il CISR è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza.

[10] L'articolo 3 del DPCM 131/2020, intitolato "Settori di attività", al comma 1 dispone: "… *Ai fini dell'inclusione nel perimetro, sono oggetto di individuazione, in applicazione del criterio di gradualità di cui all'articolo 1, comma 2, del decreto-legge, in via prioritaria, fatta salva l'estensione ad altri settori in sede di aggiornamento, i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo:*
a) interno;
b) difesa;
c) spazio e aerospazio;
d) energia;
e) telecomunicazioni;
f) economia e finanza;
g) trasporti;
h) servizi digitali;
i) tecnologie critiche, di cui all'articolo 4, paragrafo 1, lettera b), del Regolamento (UE) 2019/452 del Parlamento Europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo;
l) enti previdenziali/lavoro…".

[11] L'articolo 3 del DPCM 131/2020 al comma 2 dispone "*... All'espletamento delle attività di cui agli articoli 4 e 5 provvedono, per il settore governativo, le amministrazioni CISR, ciascuna nell'ambito di rispettiva competenza, e, per i settori di cui al comma 1, lettere da a) a l), le seguenti amministrazioni:*
a) per il settore interno, il Ministero dell'interno, nell'ambito delle attribuzioni di cui all'articolo 14 del decreto legislativo 30 luglio 1999, n. 300;
b) per il settore difesa, il Ministero della difesa;
c) per il settore spazio e aerospazio, la Presidenza del Consiglio dei ministri, ai sensi della legge 11 gennaio 2018, n. 7;
d) per il settore energia, il Ministero dello sviluppo economico;
e) per il settore telecomunicazioni, il Ministero dello sviluppo economico;
f) per il settore economia e finanza, il Ministero dell'economia e delle finanze;
g) per il settore trasporti, il Ministero delle infrastrutture e dei trasporti;
h) per il settore servizi digitali, il Ministero dello sviluppo economico, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione:

essenziali svolti da ciascun soggetto che dipendano da reti, sistemi informativi o servizi informatici e la cui interruzione o compromissione potrebbe arrecare un pregiudizio alla sicurezza nazionale, da valutare in termini di perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni, nonché le tempistiche necessarie per ristabilire l'erogazione della funzione o del servizio in condizioni di sicurezza.
L'amministrazione competente, inoltre, dovrà identificare e graduare in una scala crescente le funzioni e i servizi essenziali per i quali, in caso di interruzione o compromissione, il rischio di pregiudizio alla sicurezza nazionale sia ritenuto massimo e le possibilità di mitigazione minime[12]. I soggetti così individuati dovranno essere inclusi in una lista da sottoporre alla valutazione del CISR. Dopodiché, la loro elencazione sarà contenuta in un atto amministrativo adottato e periodicamente aggiornato dalla Presidenza del Consiglio dei Ministri su proposta del CISR. Spetterà, tuttavia, al Dipartimento delle Informazioni per la Sicurezza (DIS)[13] il compito di comunicare l'inclusione nella lista (che rimane comunque secretata) all'ente interessato entro trenta giorni dall'avvenuta inclusione nell'atto, con indicazione delle funzioni in relazione alle

i) per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca;
l) per il settore enti previdenziali/lavoro, il Ministero del lavoro e delle politiche sociali...".

[12] L'articolo 4 del DPCM 131/2020, intitolato "Modalità e criteri procedurali di individuazione dei soggetti inclusi nel perimetro", dispone: "… *Fermo restando quanto previsto per gli organismi di informazione per la sicurezza dall'articolo 1, comma 2, lettera a), del decreto-legge, ai fini dell'individuazione dei soggetti inclusi nel perimetro, le amministrazioni di cui all'articolo 3, comma 2, in relazione ai settori di attività di competenza di cui al medesimo articolo:*
a) identificano le funzioni essenziali e i servizi essenziali di diretta pertinenza ovvero esercitati o prestati da soggetti vigilati o da operatori anche privati, che dipendono da reti, sistemi informativi o servizi informatici, la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale;
b) valutano a tali fini, tenendo conto della rilevanza di ciascun criterio in relazione agli specifici settori di attività:
1) quanto agli effetti di una interruzione della funzione essenziale o del servizio essenziale, la estensione territoriale della funzione essenziale o del servizio essenziale, il numero e la tipologia di utenti potenzialmente interessati, i livelli di servizio garantiti, ove previsti, le possibili ricadute economiche, ove applicabili, e ogni altro elemento rilevante;
2) quanto agli effetti della compromissione dello svolgimento della funzione essenziale o del servizio essenziale, le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati per il loro svolgimento, avuto riguardo alla tipologia ed alla quantità degli stessi, alla loro sensibilità ed allo scopo cui sono destinati;
3) la possibile mitigazione, rispetto all'interruzione o alla compromissione dello svolgimento della funzione essenziale o del servizio essenziale, in relazione al tempo necessario per ripristinarne lo svolgimento in condizioni di sicurezza e alla possibilità che lo svolgimento della funzione essenziale o del servizio essenziale possano o meno essere assicurati, anche temporaneamente, con modalità prive di supporto informatizzato ovvero anche parzialmente da altri soggetti;
c) individuano le funzioni essenziali e i servizi essenziali di cui alla lettera a) per i quali, sulla base dei criteri di cui alla lettera b), in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime, e li graduano in una scala crescente;
d) individuano i soggetti che svolgono le funzioni essenziali o i servizi essenziali di cui alla lettera c). In fase di prima applicazione e fino all'aggiornamento del presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, sono individuati i soggetti titolari delle funzioni essenziali o dei servizi essenziali di cui alla lettera c), un'interruzione delle cui attività comporterebbe il mancato svolgimento della funzione o del servizio…".

[13] Il DIS è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni e per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI).

quali il soggetto in questione rientra nel Perimetro[14].

Sui soggetti ricompresi nel Perimetro gravano tre diversi obblighi.

In primo luogo, un obbligo di notifica entro sei ore al *team* di risposta agli incidenti di sicurezza informatica (*Computer Security Incident Response Team*, CSIRT)[15] qualora si rimanga vittime di un attacco cyber-informatico, con il successivo coinvolgimento del Nucleo di Sicurezza Cibernetica (NSC)[16] in caso di particolare gravità della violazione.

In secondo luogo, l'obbligo di aggiornare, con cadenza almeno annuale, l'elenco dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione (*information and communication technology*, ICT) di rispettiva pertinenza con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono. Più particolarmente, i soggetti che rientrano nel Perimetro dovranno effettuare un'analisi del rischio al fine di identificare i fattori di pericolo di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità, sulla sicurezza o sulla efficacia della funzione o del servizio essenziale, individuando successivamente, per ognuno di essi, **i** beni ICT necessari a svolgerli, valutando altresì l'impatto potenziale di un eventuale incidente sul bene in questione, tanto in termini di limitazione dell'operatività del bene stesso, quanto di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, nonché le inter-dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti[17].

---

[14] L'articolo 5 del DPCM 131/2020, intitolato "Elencazione dei soggetti inclusi nel perimetro" dispone: *"… Le amministrazioni di cui all'articolo 3, comma 2, in relazione ai settori di attività di competenza, predispongono, per la sottoposizione al CISR ai fini della formulazione della proposta di cui al comma 2, una lista di soggetti individuabili ai sensi dell'articolo 4, e la trasmettono al CISR tecnico.*
L'elencazione dei soggetti è contenuta in un atto amministrativo, adottato e periodicamente aggiornato dal Presidente del Consiglio dei ministri, su proposta del CISR, ai sensi dell'articolo 1, comma 2-bis, del decreto-legge.
La comunicazione di cui all'articolo 1, comma 2-bis, secondo periodo, del decreto-legge, è effettuata dal DIS entro trenta giorni dall'avvenuta iscrizione di ciascun destinatario nell'elenco di cui al comma 2. Nella comunicazione vengono indicati la funzione essenziale o il servizio essenziale in relazione al cui espletamento il soggetto è stato incluso nell'elenco, informandone le amministrazioni di cui all'articolo 3, comma 2. Dell'avvenuta iscrizione è data altresì comunicazione da parte del DIS alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice dell'amministrazione digitale, e al Ministero dello sviluppo economico, per quelli privati. L'elencazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica è altresì comunicata dal DIS all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155...".

[15] Il CSRT è la struttura, istituita in ogni Stato Membro, che ha la responsabilità di monitorare, intercettare, analizzare e rispondere alle minacce relative alla cibersicurezza.

[16] Il NSC promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte dei soggetti pubblici e degli operatori privati interessati, elaborando le relative procedure di coordinamento interministeriale.

[17] L'articolo 7 del DPCM 131/2020, intitolato "Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici", ai commi 1-2 dispone: "… *Ai sensi dell'articolo 1, comma 2, del decreto-legge, i soggetti inclusi nel perimetro predispongono e aggiornano, con cadenza almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono, osservando i criteri individuati nel successivo comma.*
Ricevuta la comunicazione prevista dall'articolo 1, comma 2-bis), secondo periodo, del decreto-legge, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale di cui all'articolo 4, comma 1, lettera c), provvedono:
a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati: 1) l'impatto di un incidente sul bene ICT, in termini sia di limitazione della

Infine, l'obbligo di predisporre un secondo elenco contenente la descrizione dell'architettura e della componentistica relative ai propri beni ICT, ossia l'insieme delle architetture realizzate e delle componenti utilizzate a livello di rete, dati e *software*[18]. Entrambi gli elenchi dovranno essere trasmessi, entro sei mesi dalla comunicazione dell'inclusione nel Perimetro, alla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione (per i soggetti pubblici) o al Ministero dello Sviluppo Economico (per i soggetti privati)[19].

Il DPCM 131/2000 rappresenta solamente il primo dei quattro DPCM attuativi del Perimetro di sicurezza nazionale cibernetica previsti dal Decreto legge n. 105/2019. Nuovi sviluppi e chiarimenti, pertanto, sono da attendersi nel corso dei prossimi mesi.

Più particolarmente, oltre a chiarire le procedure in materia di affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati dai soggetti rientranti nel Perimetro, che dovranno essere sottoposti al controllo preventivo del Centro di valutazione e certificazione nazionale (CVCN)[20] istituito presso il Ministero dello Sviluppo Economico, rimane ancora incerto il rapporto tra il Perimetro e la normativa europea, soprattutto alla luce della recente proposta della Commissione di rivedere le norme contenute nella Direttiva NIS al fine di adeguare l'attuale quadro giuridico europeo alla crescente digitalizzazione del mercato interno[21]. Mentre, infatti, il Decreto-legge n. 105/2019 prevede che un soggetto ricompreso nel del Perimetro

operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali; 2) le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione;
b) a predisporre l'elenco dei beni ICT di cui all'articolo 1, comma 2, lettera b), del decreto-legge. In fase di prima applicazione e fino all'aggiornamento del presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, sono individuati, all'esito dell'analisi del rischio, in ossequio al principio di gradualità, i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni...".

[18] L'articolo 8 del DPCM 131/2020, intitolato "Descrizione dell'architettura e della componentistica", dispone: *"... L'architettura e la componentistica relative ai beni ICT individuati negli elenchi di cui all'articolo 7, sono descritte conformemente al modello predisposto, sentito il CISR tecnico, dal DIS, che ne cura la comunicazione ai soggetti interessati unitamente alla comunicazione di cui all'articolo 5, comma 3. Il modello contiene l'indicazione degli elementi utili alla descrizione dei beni ICT e delle relative dipendenze ed è periodicamente aggiornato con le medesime modalità di cui al presente comma.*
Il modello di cui al comma 1 individua altresì le informazioni necessarie ai fini della trasmissione prevista dall'articolo 9...".

[19] L'articolo 9 del DPCM 131/2020, intitolato "Modalità di trasmissione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici", al comma 1 dispone: "... *Entro sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco di cui all'articolo 1, comma 2-bis), del decreto-legge, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, nonché quelli privati ivi inclusi, trasmettono, rispettivamente, alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico, gli elenchi di beni ICT di cui all'articolo 1, comma 2, lettera b), del decreto-legge, comprensivi della descrizione dell'architettura e della componentistica predisposta secondo il modello di cui all'articolo 8, nonché dell'analisi del rischio. La trasmissione degli elenchi di beni ICT avviene per il tramite di una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al NSC, nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente. Le disposizioni di cui al presente comma si applicano anche per l'aggiornamento degli elenchi di beni ICT e del modello di cui all'articolo 8, comma 1…*".

[20] Il CVCN ha il compito di effettuare la valutazione di beni, sistemi e servizi ICT destinati ad essere impiegati su infrastrutture ICT che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato.

[21] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.

che sia contemporaneamente un operatore di servizi essenziali (OSE) o un fornitore di servizi digitali (FSD) secondo la Direttiva NIS sia tenuto all'osservanza delle regole ivi contenute solo se di livello almeno equivalente a quelle contenute nel Perimetro[22], la futura Direttiva NIS II abolirà la distinzione tra OSE e FSD, introducendo invece quella tra entità essenziali[23] ed entità importanti[24]. Va da sé che queste evoluzioni del quadro europeo di riferimento dovranno a tempo debito venire trasposte anche al livello domestico.

[22] L'articolo 1 del Decreto-legge n. 105/2019, intitolato "Perimetro di sicurezza nazionale cibernetica", al comma 8 lettera a) dispone: "*... I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-ter, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:*
a) osservano le misure di sicurezza previste, rispettivamente, dai predetti decreti legislativi, ove di livello almeno equivalente a quelle adottate ai sensi del comma 3, lettera b), del presente articolo; le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto sono definite dalla Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera a), del presente articolo, e dal Ministero dello sviluppo economico per i soggetti privati di cui alla medesima lettera, avvalendosi anche del CVCN; il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri si raccordano, ove necessario, con le autorità competenti di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65...".

[23] Quali, tra gli altri, i settori dell'energia, dei trasporti, delle banche, delle infrastrutture del mercato finanziario, della salute e della pubblica amministrazione. Per ulteriori informazioni si veda l'Allegato I della proposta.

[24] Quali, tra gli altri, i servizi postali, la gestione dei rifiuti, l'industria chimica nonché quella alimentare. Per ulteriori informazioni si veda l'Allegato II della proposta.

Roberto A. Jacchia

PARTNER

r.jacchia@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano

Marco Stillo

ASSOCIATE

m.stillo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com