di Roberto Setola e Giacomo Assenza

PERIMETRO NAZIONALE DI SICUREZZA CIBERNETICA

Roberto SETOLA è professore ordinario (settore ING-INF/04 Automatica) presso l'Università Campus BioMedico di Roma dove ricopre anche il ruolo di Direttore del Laboratori Sistemi Complessi e Sicurezza. È il Direttore Scientifico del Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management". È il Direttore del Consorzio inter-universitario NITEL sulla Logistica e i Trasporti.

Giacomo ASSENZA, dopo aver conseguito un Master in Intelligence and International Security presso il King's College of London e il Master In Homeland Security presso l'Università Campus Bio-Medico di Roma, collabora dal 2018 con il Laboratorio Sistemi Complessi e Sicurezza del Prof. Setola, svolgendo ricerca nell'ambito della cyber-war e cyber-security.

Il **18 novembre 2019** è stata emanata la **Legge n. 133 sul perimetro cibernetico,** che vuole contribuire ad innalzare la sicurezza del sistema Paese verso le minacce ***cyber***, individuando, da un lato, alcuni obblighi in capo a coloro che gestiscono infrastrutture essenziali per il Paese e, dall'altro, definendo un'architettura in grado di valutare ***ex-ante*** l'adeguatezza dei diversi componenti informatici che andranno ad essere utilizzati da tali gestori.

L'obbiettivo della legge n. 133 del 18 novembre 2019, che ha convertito il decreto legge *"recante disposizioni urgenti in materia di perimetro di sicurezza cibernetica"*, è quello di tracciare il perimetro di sicurezza cibernetica nazionale per garantire un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici per tutti quei soggetti, pubblici o privati, esecutivi nel campo dei servizi essenziali. La nuova normativa rappresenta il frutto delle riflessioni riguardo la rilevanza e l'urgenza della minaccia cibernetica che, risultando sempre più significativa, impone il passaggio da strategie meramente di contrasto a un approccio proattivo. Tale approccio, riconoscendo il legame ormai imprescindibile tra *cybersecurity*, benessere della popolazione e sicurezza nazionale, si muove in una cornice di partecipazione pubblico-privata per depotenziare la minaccia *cyber* attraverso l'adozione di *policy* e verifiche *ex-ante* in grado di ridurre l'esposizione e la vulnerabilità del sistema Paese.
Il titolo della norma è stato leggermente modificato nel corso del dibattito parlamentare con l' aggiunta, dopo la parola "cibernetica", della seguente frase *"e di disciplina dei poteri speciali nei settori di rilevanza strategica"*. Tale inserimento mette ulteriormente in luce il focus della norma che, come evidenziato già dai considerata presenti nel testo del decreto legge, risulta suddiviso in due ambiti: il perimetro cibernetico (artt. 1, 2 e 5) e gli aspetti legati alla disciplina dei poteri speciali, leggasi 5G, a cui sono dedicati gli artt. 3 e 4. Nel prosieguo di questo articolo ci soffermeremo sugli aspetti connessi con il solo perimetro cibernetico.

1. Definizione del perimetro cibernetico

La necessità della norma è chiarita nelle premesse che evidenziano l'urgenza di *"disporre per le finalità di sicurezza nazionale, di un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti"* informatici utilizzati da tutti quei soggetti, pubblici o 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"* (art. 1, comma 1).
Tale locuzione, che richiama in parte la definizione di Operatore di Servizi Essenziali (OSE), introdotta nell'ordinamento nazionale con la Disciplina NIS (*Network and Information Security*), mira ad evidenziare la rilevanza di tali soggetti, in quanto da un loro *"malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio"* può derivare un pregiudizio per la sicurezza nazionale.
La Legge non definisce in modo puntuale quali sono gli attori che, ricadendo all'interno del perimetro, saranno tenuti al rispetto delle prescrizioni contenute nella legge, ma si limita a conferire questo mandato al CISR (Comitato Interministeriale per la Sicurezza della Repubblica) affinchè individui tali soggetti entro la fine di marzo 2020.
Il lavoro del CISR appare non semplice, in quanto l'individuazione dei confini del perimetro cibernetico, ovvero di quelli che saranno i discrimini per l'inclusione o meno di un soggetto all'interno di esso, dovrà bilanciare due necessità contrapposte. Da un lato vi è l'esigenza di limitare il perimetro ad un nucleo di soggetti "significativamente" strategici per la sicurezza nazionale, questo per contenere gli oneri a carico delle società e della collettività. Dall'altro, appare necessario includere tutte le componenti che "costruttivamente" rappresentano l'ossatura informatica del Paese. Fra i tecnici circola con insistenza il quesito se il

perimetro, al netto delle pubbliche amministarzioni da inserire, investirà gli stessi soggetti già individuati come OSE ai sensi della direttiva NIS, ovvero ne comprenderà un sottoinsieme ristretto (solo alcuni degli OSE), più ampio (tutti gli OSE più altri) oppure ancora se l'insieme dei soggetti individuati come OSE e quelli inclusi nel perimetro cibernetico saranno solo parzialmente sovrapposti.

Occorre precisare che, a differenza della direttiva NIS, il legislatore non ha ritenuto opportuno indivduare a priori i settori all'interno dei quali devono operare gli afferenti al perimetro, ma si è limitato a specificare criteri di appartenza estremamente ampi (art.1, comma 2, lettera a):

1. *"il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato";*
2. *"l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici".*

In sede di conversione del decreto, il legislatore ha ritenuto utile aggiungere a questi due criteri di perimetrazione "orizzontali" un ulteriore criterio di perimetrazione "verticale" mediante l'inserimento:

2-*bis*. *"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".*

Tale criterio consente di identificare, all'interno degli *asset* dei vari attori, quella porzione dell'infrastruttura IT/OT da assoggettare agli obblighi della legge. In tal modo sarà possibile assoggettare agli obblighi della norma anche solo una porzione dei sistemi informativi di un determinato operatore.

2. Inventario, notifica e linee guida

Sempre al CISR, e sempre entro 4 mesi dall'emanazione della legge[1], compete la determinazione dei criteri *"sulla base di un'analisi del rischio e di un criterio di gradualità"*, secondo i quali, i soggetti afferenti al perimetro sono tenuti a predisporre un inventario dei propri sistemi informativi. Tale inventario, da finalizzare e trasmettare entro sei mesi dall'emanazione dei suddetti criteri, dovrà includere *"l'elenco delle reti, dei sistemi informativi e dei servizi informatici […] comprensivo della relativa architettura e componentistica"*. Questa disposizione rigurda anche i soggetti che emettono certificati digitali e accreditati ai sensi dell'art.29 del codice dell'amministrazione digitale[2].

Onere questo che, specialmente per i soggetti Pubblici, potrebbe risultare complesso, soprattutto in sede di prima attuazione.

Occorre inoltre osservare che, mentre vi è un obbligo da parte dei soggetti inseriti all'interno del perimetro di aggiornare su base annuale gli inventari, la legge non prevede una specifica cadenza per la ri-determinazione dei criteri, sulla base dei quali tali inventari devono essere strutturati.

Inoltre, entro la fine di settembre 2020, il CISR dovrà elaborare le procedure per la notifica degli *"incidenti aventi impatto su reti, sistemi informativi e servizi informatici"* afferenti al perimetro, ed elaborare le *"misure volte a garantire elevati livelli di sicurezza"* per tali sistemi. Quest'ultime dovranno fornire, sulla falsa riga di quanto fatto con le Linee Guida che hanno corredato la direttiva NIS, indicazioni su:

- la struttura organizzativa preposta alla gestione della sicurezza nonché le politiche di sicurezza e di gestione del rischio;
- la gestione degli incidenti, della loro mitigazione e prevenzione;
- la protezione fisica e logica e dei dati, delle reti e dei sistemi informativi;
- la gestione operativa, ivi compresa la continuità del servizio;
- le modalità per il monitoraggio, il *test* ed il controllo dei sistemi informativi e dei suoi componenti;
- la formazione e consapevolezza del personale;
- le modalità di acquisizione di beni e servizi di ICT (aspetto dettagliato nel comma 6 - si veda oltre).

Per i soggetti privati sarà il Ministero dello Sviluppo Economico, *"nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica"*, a svolgere attività di ispezione e verifica della corretta ed adeguata adozione delle misure predisposte dal CISR *"impartendo, se necessario, specifiche prescrizioni"*.

La rilevanza delle prescrizioni contenute nella norma si evince dal comma 9 che prevede, in caso di mancata attuazione anche solo parziale degli obblighi derivanti dalla normativa, sanzioni pecuniarie fino a € 1.800.000[3].

Inoltre, qualora si utilizzino prodotti o componenti che non abbiano superato le prescritte verifiche, si può incorrere nella *"sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni"* (comma 10).

Infine, qualora si ravveda il dolo, è prevista dal comma 11 anche la reclusione da uno a tre anni per *"chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti […] fornisce informazioni, dati o elementi di fatto non rispondenti al vero […] od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto"*. Quest'ultima fattispecie di reati è anche inclusa, ai sensi del comma 11-*bis*, fra quelli per i quali sussiste la responsabilità penale del soggetto giuridico ai sensi della Legge 231/2001.

3. Determinazioni del Presidente del Consiglio dei Ministri

L'art.5 attribuisce al Presidente del Consiglio dei Ministri *"in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici"* di *"disporre, ove indispensabile e per il tempo strettamente*

1 La tempistica specificata nella norma per quel che riguarda gli atti e i decreti attuativi necessari per la piena operatività della norma appare molto stringente. Se si analizza quanto occorso con l'entrata in vigore della Direttiva NIS si evidenzia che non tutte le amministrazioni pubbliche sono state in grado di produrre nei tempi prescritti gli atti attuativi inducendo una adozione della direttiva a macchia di leopardo.

2 Il testo normativo non fornisce una indicazione specifica circa gli eventuali obblighi dei certificatori accreditati presso altri Stati Membri ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE ed equiparati a quelli nazionali ai sensi del comma 8 dell'art. 29 del *Codice dell'Amministrazione Digitale*.

3 Gli importi massimi sono diversificati in funzione della fattispecie omissiva.

necessario […] la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti o nei sistemi o per l'espletamento dei servizi interessati". Tale previsione dunque, conferisce un significativo potere di *switch-off* su qualunque elemento o apparato informatico del Paese (in sede di conversione in legge, il legislatore ha ritenuto, infatti, di espungere ogni riferimento al perimetro nazionale di sicurezza cibernetica).
Occorre però rilevare che tale articolo appare nella formulazione promulgata più un'indicazione di principio tesa a rafforzare l'importanza e la supremazia dell'interesse nazionale – e nello specifico della sua sicurezza cibernetica - rispetto alle scelte (economiche) dei singoli. Tale lettura deriva dalla costatazione che il legislatore non fa menzione né delle modalità di notifica di tale atto[4] né delle sanzioni irrorabili in caso di omessa o ritardata attuazione, senza considerare che dal punto di vista tecnico lo *switch-off* non programmato di un qualunque apparato all'interno di una rete complessa, quali sono quelle utilizzate dagli operatori dei servizi essenziali, può avere impatti non facilmente prevedibili sulla stabilità e capacità di erogazione dei servizi stessi.

4. Centro di Valutazione e Certificazione Nazionale (CVCN)

Sicuramente l'aspetto maggiormente oggetto di riflessione, durante l'intero *iter* di approvazione della norma, rigurda il comma 6 dell'art.1 che stabilisce, con un regolamento da adottare entro fine settembre 2020, le modalità di svolgimento delle attività di *procurement* da parte dei soggetti inclusi nel perimetro cibernetico nazionale per quel che concerne l'acquisizione di beni e servizi informatici. Con tale articolo, il legislatore vuole favorire quell'azione proattiva menzionata precedentemente e quindi anticipare le valutazioni di criticità già in fase di acquisizione del bene o servizio, prevenendo in questo modo l'introduzione di vulnerabilità all'interno delle infrastrutture degli operatori del perimentro cibernetico.
La norma prevede, in estrema sintesi, che i soggetti afferenti al perimetro cibernetico nazionale che intendano acquisire beni, sistemi e servizi ICT, devono darne comunicazione al CVCN (Centro di Valutazione e Certificazione Nazionale) istituito presso il MISE[5]. La comunicazione deve includere anche la valutazione da parte dell'operatore *"del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego"* (art.1, comma 6, lettera a).
Il CVCN nel termine di 45 giorni, prorogabile una sola volta di ulteriori 15 gg. in caso di particolari complessità *"può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software"*.
In caso di imposizione di specifiche condizioni e *test* di *hardware* e *software*, i relativi bandi di gara e contratti devono essere integrati con clausole che vincolano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei *test* disposti dal CVCN. I *test* da parte del CVCN (ovvero dei centri da questi autorizzati ed accreditati) devono essere conclusi nel termine di sessanta giorni[6].

Il successivo comma b) specifica che i *"soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti […] assicurano al CVCN la propria collaborazione per l'effettuazione delle attività di test*[7]*"* sostenendone gli oneri.
Dal combinato disposto dei due commi si evince che l'azione del CVCN si estrinseca nell'ambito dell'*iter* del processo di acquisizione, a valle della valutazione tecnico-economica da parte dell'operatore e prima dell'aggiudicazione formale da parte di questi al soggetto individuato per l'affidamento. Secondo alcuni tale impostazione potrebbe essere oggetto di impugnativa, in quanto la natura dei *test* sarebbe definita solo dopo che la stazione appaltante ha preso contezza delle caratteristiche proposte dai diversi concorrenti. Per altro, in presenza di erogazione di servizi o qualora l'oggetto della fornitura non si trattasse di un prodotto a scaffale, bensì di un bene (sia esso *hardware* o *software*) da realizzare, assemblare e/o costruire, la possibilità di effettuare *test* di verifica appare di difficile attuazione, non potendo essere disponibile il sistema nel termine dei 60 giorni.

Problematica inversa emerge in relazione alle attività di *patching*[8] che non è chiaro se siano o meno soggette all'obbligo da parte dell'operatore di preventiva comunicazione al CVCN. Infatti, se da un lato tale attività non si configura come una nuova "acquisizione" (e quindi non direttamente assoggettabile a quanto previsto dal comma 6, punto a), la relativa istallazione altera l'oggetto della verifica originale e quindi, in linea di principio, espone l'operatore alle sanzioni previste dal comma 9. D'altro canto, soprattutto in presenza di attività di *patching* relativa a falle di sicurezza, l'obbligo di dover attendere le determinazioni del CVCN potrebbe introdurre ritardi nell'adozioni di tali contromisure, con potenziale maggiore esposizione al rischio da parte degli operatori. Ancora più complessa appare l'applicazione delle attività di verifica allorquando l'oggetto della fornitura rigurda la gestione, manutenzione e aggiornamento di sistemi o apparati già in uso da parte degli operatori del perimetro.
Aspetti questi che potranno trovare puntuale illustrazione all'interno del regolamento da emanare.

5. Conclusioni

Il quadro normativo delineato dagli artt.1, 2 e 5 va, come detto, nella direzione di migliorare la capacità di pro-attività del sistema Paese nei confronti della sempre più diffusa e subdola minaccia *cyber*. Questo è un aspetto importante e condivisibile, è però auspicabile che nel corpo dei decreti e regolamenti che dovranno essere emanati, oltre alla puntuale illustrazione delle procedure e degli obblighi in capo ai soggetti che ricadono nel perimetro cibernetico nazionale, si individuino anche meccanismi e strumenti per migliorare ulteriormente la cooperazione pubblico-privata, soprattutto nella direzione di fornire servizi e supporto agli operatori del perimetro (siano essi pubblici o privati), per meglio valutare le potenziali vulnerabilità, l'insorgenza di nuove minacce e quale sprone per una costante rivisitazione e ri-allineamento dei loro assetti, organizzativi e tecnologici, al mutevole panorama di riferimento.©

4 L'unica indicazione è quella contenuta nel comma 1-*bis* che prevede la notifica di tale atto al COPASIR, entro 30 giorni dalla sua emanazione.

5 Ovvero ai CVNC istituendi presso il Ministero degli Interni ed il Ministero della Difesa.

6 La norma non specifica il termine da cui decorrono i 60 giorni.

7 La omessa collaborazione può essere sanzionata con un'ammenda da € 250.000 a € 1.500.000.

8 Tale aspetto abbraccia anche le attività di manutenzione correttiva, *predittiva* e di *upgrading*.