*Direzione Nazionale Antimafia e Antiterrorismo*

# COMMISSIONE AFFARI COSTITUZIONALI
CAMERA DEI DEPUTATI

AUDIZIONE DEL
Procuratore nazionale antimafia e antiterrorismo
Federico Cafiero de Raho

7 ottobre 2019

DECRETO LEGGE 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

DECRETO LEGGE 21 settembre 2019, n. 105 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica)

Lo schema di Decreto Legge in materia di **perimetro di sicurezza cibernetica,** datato 17 settembre 2019 e che segue di qualche mese il Decreto Legge del 25 marzo 2019, n. 22[1], nasce con il preciso scopo di rispondere all'esigenza di aggiornare l'assetto istituzionale complessivo (inteso come "sistema di organi, procedure e misure") per migliorare la strategia nazionale per la protezione delle infrastrutture tecnologiche (reti, sistemi informativi e servizi informatici) definite "strategiche" e, come tali, "critiche" in relazione all'esercizio di **funzioni essenziali dello Stato** e alla **prestazione di servizi essenziali** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

L'imprescindibilità e l'improrogabilità della tematica sono strettamente correlate non già alla valutazione del rischio connesso, bensì dell'impatto, ovvero del pregiudizio per la sicurezza nazionale derivante da eventuali malfunzionamenti ed interruzioni, anche parziali, perpetrati a mezzo di attacchi "cyber", ovvero da utilizzi impropri delle medesime infrastrutture.

Riallacciandosi al d.lgs. 18 maggio 2018, n.65 con cui è stata recepita dall'Italia la direttiva[2] europea 2016/1148, la policy di risposta alla minaccia informatica indirizzata alle amministrazioni pubbliche, gli enti e gli operatori nazionali (pubblici e privati) inclusi nel cosiddetto "perimetro di sicurezza nazionale cibernetica" si declina, nelle intenzioni del legislatore, su due differenti piani:

- Di "*continuità operativa*", intesa come la capacità (resilienza tecnica) delle organizzazioni interessate di continuare ad erogare prodotti e/o servizi a livelli predefiniti accettabili a seguito di un incidente e/o attacco, attraverso l'adozione (preventiva e successiva all'evento) di specifiche ed adeguate misure tecnologiche e logistico/organizzative di "ripristino in caso di disastro o di emergenza";
- di "cultura condivisa di gestione del rischio", già perentoriamente affermata dalla citata direttiva UE 2016/1148 e realizzata ora anche attraverso una tempestiva e "circolare" segnalazione degli incidenti/attacchi in ambito cyber a specifici centri coordinatori, così da implementare una ciclica revisione degli standard di sicurezza ("certificazione cibernetica") idonei a superare eventuali *bugs* di sistema (emersi *ex post*), criticità infrastrutturali, omogeneizzare i protocolli di comunicazione tra diverse architetture (ad esempio di enti differenti che devono aggiornare, ciascuno per la propria parte di competenza, una banca dati comune), nonché testare l'effettiva rispondenza di beni, sistemi e servizi ICT forniti da soggetti ammessi[3] a partecipare ai relativi bandi di gara.

---

[1] Decreto-legge 25 marzo 2019, n. 22 convertito, con modificazioni, in legge 20 maggio 2019, n. 41, recante misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea.», che recita al Capo I "Disposizioni in materia di poteri speciali inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G".

[2] Cosiddetta direttiva "NIS", acronimo di "Network and Information Security".

[3] Intendendo sia agli **operatori di servizi essenziali** ("OSE", a cui fanno capo, ad esempio, le infrastrutture digitali) che i **fornitori di servizi digitali** ("FSD" a cui fanno capo, ad esempio, i motori di ricerca e il *cloud computing*).

L'art. 1, co. 6, rimette ad un regolamento da emanarsi, con decreto del Presidente del Consiglio dei ministri, entro 10 mesi dalla data di entrata in vigore del presente decreto-legge, la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi tutti i soggetti riconosciuti come facenti parte del perimetro di sicurezza nazionale cibernetica, e che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'apposito elenco trasmesso alla Presidenza del Consiglio dei ministri ed al Ministero dello sviluppo economico.

A fronte della previsione di un sistema di analisi e valutazione dei rischio in capo al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, e dell'inserimento nei bandi di gara e nei relativi contratti di clausole sospensivamente o risolutivamente condizionate all'esito positivo di apposite verifiche tecniche, per quanto concerne lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati il decreto si limita a ribadire la necessità che le reti ed i sistemi utilizzati siano conformi ai livelli di sicurezza di cui all'art.1 co.3, lett. b), qualora non incompatibili con gli specifici impieghi cui essi sono destinati.

All'elaborazione delle misure volte a garantire tali livelli di sicurezza sono chiamati a partecipare, secondo i rispettivi ambiti di competenza, il Ministero dello Sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della Difesa, il Ministero dell'Interno, il Ministero dell'Economia e delle Finanze e il Dipartimento delle Informazioni per la Sicurezza (DIS)[4].

E qui si impone una prima riflessione, che investe tanto il merito della questione quanto l'approccio metodologico scelto per la sua risoluzione.

Si potrebbe ritenere una carenza, da colmare eventualmente in sede di conversione del decreto legge in argomento, l'esclusione da tali procedure del Ministero della giustizia e dei competenti dipartimenti.

La necessità di "*assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche...da cui dipende una funzione essenziale dello Stato*", esplicitamente formalizzata nell'art.1 co.1 del citato decreto, dovrebbe coinvolgere anche le tematiche di interesse strategico per l'amministrazione della Giustizia ed il contrasto dei più gravi fenomeni criminali, con conseguenze strettamente ma non esclusivamente legate alla tutela dell'ordine e della sicurezza pubblica.

La rivoluzione che ha investito nell'ultimo decennio il settore dell'ICT (Information and Communication Technology) ha consentito di innovare sensibilmente i canoni di conduzione delle attività di indagine, a partire ad esempio dal *modus operandi* delle banche dati, ora non più suscettibili di una mera interrogazione semantica ma divenute nel tempo sofisticati strumenti di supporto decisionale attraverso l'estrapolazione di dati eterogenei e la loro successiva agglomerazione in prodotti informativi complessi.

L'avvento del 5G e dell'intelligenza artificiale non potrà che rafforzare in modo vertiginoso le attuali capacità di trasmissione e conservazione (*storage*) dati, segnando

---

[4] Quest'ultimo già designato nel d.lgs. n.65/2018 (in linea con la disciplina precedente data dalle leggi n.124/2007 e 133/2012, nonché dal DPCM del 17 febbraio 2017) quale **punto di contatto unico** all'interno di un modello settoriale, diffuso e decentrato nel quale sono stati previsti, come autorità "NIS" cinque ministeri, ognuno responsabile per il settore di propria competenza, tra cui compare il Ministero dello sviluppo economico per i settori energetico e delle infrastrutture e servizi digitali mentre non è fatto cenno alcuno al Ministero di giustizia.

un passaggio decisivo per l'implementazione, a fini investigativi, di strumenti afferenti all'area della "*intelligenza non convenzionale*" ("unconventional IP intelligence"), quali ad esempio biometrica vocale (*voice biometrics*) e riconoscimento del volto (*face recognition*, quale l'analisi integrata di sistemi di videosorveglianza), *target geo-location, cell positioning, geofencing*[5], *IP decoding, social networks analysis, metadata extraction&analysis*[6].

Ciò sta portando e porterà sempre di più ad un nuovo modo di rappresentare le dinamiche investigative attraverso la confluenza organica, all'interno di annotazioni multimediali, di dati altamente tecnologici elaborati e riscontrati con le risultanze di attività consolidate come i servizi di osservazione e pedinamento.

Tali considerazioni comportano due ordini di necessità:

- elaborare le informazioni (con annessa certificazione forense dell'intero processo, dalla primigenia acquisizione dei dati fino alla tracciabilità di ogni operazione successiva) mediante l'interoperabilità di piattaforme informatiche distinte (banche dati, fonti aperte, database delle procure e delle FF.PP.);
- archiviare (in sicurezza) flussi imponenti[7] di "big data" e garantire una efficace difesa da attacchi informatici esterni.

In merito, mi preme rappresentare che la DNA ha saputo anticipare i tempi.
Ci si riferisce, innanzitutto, ai sistemi informativi a disposizione del circuito DNA/DDA, che contengono gli atti giudiziari (quali le informative di PG, Intercettazioni telefoniche, ambientali e telematiche, le richieste di misure cautelari, le ordinanze di misure cautelari e tutti gli altri atti del procedimento penale) ed i dati di tutti i procedimenti penali in materia di reati di mafia e di terrorismo, ivi compresi i procedimenti di prevenzione patrimoniale e personale (per i quali la Direzione

---

[5] Il geofencing è una sorta di "recinto virtuale" utilizzato dalla tecnologia GPS sui dispositivi di telefonia portatili per definire i confini geografici virtuali di un'entità in movimento (oggetto o persone), poiché viene rilevato il segnale di un insieme di telefoni mobili identificati su un perimetro geografico definito.

[6] Un metadato (letteralmente "dato per mezzo di un altro dato"), rappresenta un'informazione che descrive un insieme di dati. I metadati possono essere distinti in vari modi; uno dei più diffusi li raggruppa in tre macro-categorie:

- *descrittivi*: servono per l'identificazione ed il recupero di oggetti digitali e sono costituiti da descrizioni dei documenti "fonte";
- *amministrativi e gestionali*: evidenziano le modalità di archiviazione e manutenzione degli oggetti digitali nel sistema di gestione del relativo archivio in cui vengono depositati, e sono necessari per una corretta esecuzione delle relative attività. Data la labilità dell'informazione elettronica, questi tipi di metadati assumono un'importanza *preponderante* ai fini della conservazione permanente degli oggetti digitali: essi possono inoltre fornire informazioni sulle condizioni e i diritti di accesso ad essi, certificare l'autenticità e l'integrità del contenuto, documentare la catena di custodia degli oggetti, identificarli in maniera univoca;
- *strutturali*: usati per descrivere la struttura interna dei documenti e gestire le relazioni fra le varie parti componenti degli *oggetti* digitali". Inoltre forniscono dati di identificazione e localizzazione del documento, come l'indirizzo del file sul server, l'archivio digitale di appartenenza ed il suo indirizzo Internet.

[7] L'Internet of Things richiederà una progettazione della rete mobile differente rispetto al passato, quando le comunicazioni erano solo di tipo "HTC" (Human Type Communication) cioè tese a mettere in relazione solo interlocutori umani. Oggi il numero di utenti mobili è piccolo se paragonato al bacino generato dai nuovi dispositivi predisposti per l'IoT, mentre la quantità di dati scambiati è superiore rispetto alle trasmissioni sporadiche tra le macchine. Cambiando il paradigma da pochi utenti (umani) con molto traffico ciascuno a molti utenti (umani e macchine) con poco traffico ciascuno, è facile prevedere che la quantità complessiva di dati scambiati sarà enormemente superiore ma, soprattutto, distribuita molto più capillarmente.

Nazionale può essere parte proponente), la cui analisi consente al Procuratore Nazionale Antimafia e Antiterrorismo di promuovere gli "atti d'impulso" nei confronti delle Procure Distrettuali, oppure consente il coordinamento delle indagini relative a procedimenti penali di propria competenza, la cui delicatezza è chiara a tutti[8].
Inoltre, in DNA, fin dal dicembre 2012 è operativo uno specifico servizio "risorse tecnologiche, gestione flussi e sicurezza", costituito allo scopo di ridefinire i moduli organizzativi e i protocolli di sicurezza nei settori dell'informatica, delle risorse tecniche, delle procedure e dei flussi di lavoro funzionali a garantirne non solo l'efficace esercizio delle funzioni giudiziarie ma anche l'integrità funzionale dell'Ufficio rispetto a possibili aggressioni esterne e/o interne che potrebbero minare l'esercizio delle proprie funzioni e la tutela del patrimonio informativo.
Con specifico riferimento all'avvento delle più evolute tecnologie, è necessario, inoltre, evidenziare quanto devastante potrebbe essere l'impatto delle nuove reti 5G con riferimento alla tematica delle prestazioni obbligatorie, ex art. 96 del d.lgs. 1 agosto 2003, n. 259 (Codice delle comunicazioni elettroniche).

Se è vero che le disposizioni di raccordo tra il decreto in commento e la normativa in materia di esercizio dei poteri speciali governativi sulla tecnologia 5G, di cui all'art.3 co.3, subordinano l'esercizio di tali poteri alla valutazione degli elementi indicanti **la presenza di fattori di vulnerabilità** che potrebbero compromettere genericamente **l'integrità** e la **sicurezza** delle reti e dei dati che vi transitano, non viene fatto esplicito riferimento alla necessità di assicurare anche la "**funzionalità**" della rete stessa per ottemperare alle prestazioni obbligatorie di giustizia.

Appare pleonastico sottolineare l'importanza a dir poco nevralgica che la captazione dei flussi comunicativi riveste nelle indagini in materia di criminalità organizzata e terrorismo; la crittografia del numero IMSI ed i rigorosi processi di autenticazione sugli smartphones di ultima generazione rendono particolarmente difficoltoso, se non quasi impossibile, per l'autorità giudiziaria e per le forze dell'ordine identificare i dispositivi mobili, con notevoli ripercussioni anche in termini di acquisizione di alcuni metadati normalmente acquisibili tramite intercettazione (localizzazione, data, ora, durata della chiamata, numero contattato).

In tale contesto, dunque, appare fondamentale, oggi più di ieri, che l'esigenza legittima da parte di ogni cittadino-utente riguardo l'integrità e l'inviolabilità da attacchi cyber tanto dei propri dispositivi digitali, quanto delle relative comunicazioni, si accompagni alle garanzie funzionali a preservare l'efficacia dell'azione inquirente della magistratura, garantendo senza ambiguità alcuna le prestazioni obbligatorie previste per legge.

Mi si consenta, inoltre, un'ultima considerazione circa l'art. 1, comma 6, lett. c) del decreto; in esso si individua nella Presidenza del Consiglio dei ministri e nel Ministero dello sviluppo economico le autorità competenti per le attività di ispezione e verifica, rispettivamente sui soggetti pubblici e privati.

Per le reti, i sistemi informativi ed i servizi informatici connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, invece, le attività di ispezione e verifica

8 Il sistema SIDNA/SIDDA accede, facendoli propri, anche ai dati delle segnalazioni di operazioni sospette dell'UIF della Banca d'Italia ed ai dati dell'Autorità nazionale Anticorruzione. Si connette, inoltre: alle banche dati dell'Agenzia delle Entrate quali puntofisco, Rapporti Finanziari e fatturazione elettronica in materia di commercio di carburanti; alle banche dati dell'Agenzia delle Dogane, ivi compresa la parte riguardante i giochi e le scommesse.

vengono assegnate alle strutture specializzate in tema di protezione di reti e sistemi, che non appare agevole individuare compiutamente.

Ora, non posso che evidenziare come la mancata previsione di un coinvolgimento del Ministero della Giustizia nella definizione dell'architettura di condivisione delle procedure e delle misure relative alle politiche di sicurezza e della gestione del rischio delle reti, dei sistemi informativi e dei sistemi informatici connessi alla funzione di prevenzione e repressione dei reati contribuisca a rendere poroso e friabile il muro di protezione che si vorrebbe erigere.

Non possiamo ignorare che la partita sulla sicurezza cibernetica delle infrastrutture tecnologiche a supporto dell'organizzazione giudiziaria abbia riflessi diretti sulla più ampia categoria della "sicurezza nazionale"[9].

Un approccio metodologico più profondo sulla delimitazione del perimetro della cyber sicurezza nazionale dovrebbe indurci a rovesciare la prospettiva, non già partendo dalla definizione dell'oggetto da proteggere bensì dei soggetti da coinvolgere.

Appare fondamentale partire dall'individuazione di tutte quelle "organizzazioni" (di cui all'art.1) la cui sicurezza cibernetica vada necessariamente promossa e garantita; e solo a seguito di questa prima fase, proiettarsi, come logica deduzione, in una definizione reale ed oggettiva dei concreti ambiti da difendere a titolo comune (e di cui ciascuno dei soggetti chiamati in causa rappresenterà il naturale *stakeholder*).

Occorrerebbe che nel contesto in esame rientrassero prioritariamente le amministrazioni pubbliche e gli enti governativi anche laddove gestiscano dati ed attività in ambito non classificato[10].

Già in quest'alveo si muoveva, peraltro, il decreto del ministro dell'interno del 9 gennaio 2008, denominato *Individuazione delle infrastrutture critiche informatiche di interesse nazionale* e pubblicato sulla G.U. 101 del 30 aprile 2008, che stabilisce che "*sono da considerare infrastrutture critiche di interesse nazionale i sistemi e i servizi informatici di supporto alle funzioni istituzionali di ministeri, agenzie ed enti da essi vigilati [...] la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale*".

---

[9] In tal senso già la Corte costituzionale aveva compiuto un passo decisivo con la storica sentenza n.86 del 1977, associando a tale categoria "*la necessità di protezione.....dei supremi interessi che valgono per qualsiasi collettività organizzata a Stato e che possono coinvolgere l'esistenza stessa dello Stato*", facendo riferimento pertanto non solo allo "Stato-ordinamento" inteso come l'insieme delle sue regole e dei suoi principi costitutivi, ma anche allo "Stato-comunità", vale a dire lo spazio comune nel quale si muovono soggetti pubblici e privati, portatori di interessi costituzionalmente sanciti di cui lo Stato è di volta in volta arbitro, garante, controllore con poteri sanzionatori.

[10] Come pure le società che, pur trattando dati classificati, non siano riconducibili al ristretto ambito degli assetti strategici, oppure le società assoggettabili al regime del *golden power*, ma che, tuttavia, non siano annoverabili nella categoria delle infrastrutture critiche. E, sulla stessa lunghezza d'onda, vi sarebbe posto per gli Ose (Operatori di servizi essenziali) che non costituiscono infrastrutture critiche. Così come, a livello di principio, per una casistica particolarmente complessa, quella delle società di telecomunicazioni, che non sono al momento qualificabili come Ose, ma per le quali si pone in maniera peculiare il problema del *procurement* di tutti gli apparati e le infrastrutture di rete, anche di quelli che non sono necessariamente finalizzati agli aspetti di sicurezza, ma che, per la loro natura tecnologica e telematica, possono in ogni caso nascondere insidie per la sicurezza delle strutture nazionali.

L'identificazione dell'interesse nazionale è certamente uno dei momenti più qualificanti del processo di definizione dell'indirizzo politico complessivo da parte dell'Autorità di governo, e come tale rappresenta un peculiare terreno di confronto in Parlamento.

Riconoscere flessibilità al perimetro della sicurezza nazionale si rivela come una strada obbligata per rimanere sempre al passo con la realtà e tenere il Paese al riparo da quelle insidie suscettibili di arrecare danni sistemici al funzionamento della sua architettura democratica. Nell'ottica di voler adottare in concreto ogni forma di cautela e misura necessaria a garantire non solo l'integrità e la sicurezza dei sistemi, ma anche la loro più completa e continuativa "funzionalità" agli scopi di giustizia, auspico quindi che in sede di conversione possano essere inserite le rimodulazioni necessarie a garantire la partecipazione di interlocutori specifici a garanzia dell'integrità, sicurezza e funzionalità di ogni rete e sistema informatico impiegato per le esigenze di giustizia.

In concreto:

- prevedere, al comma 4 dell'art. 1 del decreto, il Ministero della Giustizia tra coloro che elaborano le misure di cui al comma 3 lett. b;
- prevedere anche per i sistemi informatici strategici in uso all'Autorità giudiziaria strumenti per la effettuazione di attività di valutazione preventiva di cui al comma 6 lett. a) dell'art.1 del decreto de quo, nonché di attività di ispezione e verifica di cui al comma 6 lett. c) dell'art.1, eventualmente a cura di apposite strutture tecniche del Ministero della Giustizia, che comunque si coordinino con il CVCN e con la Presidenza del Consiglio dei Ministri;
- prevedere espressamente che attributo della sicurezza di reti, sistemi informativi e servizi informatici sia anche la loro funzionalità, intesa anche quale funzionamento in conformità delle previsioni legislative.

*Il Procuratore nazionale antimafia e antiterrorismo*

*Federico Cafiero de Raho*

Nota predisposta con la collaborazione del Procuratore Nazionale Aggiunto Giovanni Russo, Responsabile del Servizio Risorse Tecnologiche e Sicurezza della Direzione Nazionale Antimafia e Antiterrorismo