Il nuovo Decreto Legge in materia di Sicurezza Nazionale Cibernetica

1. Premessa

In data 21 settembre 2019 è stato pubblicato in Gazzetta Ufficiale (Serie Generale n. 222 del 21-09-2019) il decreto legge n. 105/2019 (cd. il "**Decreto Legge sulla Sicurezza Cibernetica**")[1] che **istituisce il perimetro di Sicurezza Nazionale Cibernetica** e introduce **misure idonee a garantire standard di sicurezza** delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, che svolgono funzioni essenziali dello Stato o prestano servizi essenziali in campo civile, sociale, economico e dal cui malfunzionamento possa derivare un pregiudizio per la sicurezza nazionale.

Al fine di apprestare misure idonee di tutela alle reti, ai sistemi informativi, e ai servizi di comunicazione a banda larga basati sulla tecnologia 5G, nonché di coordinare l'attuazione del Regolamento UE 2019/452, il Decreto Legge sulla Sicurezza Cibernetica **adegua** altresì il **quadro normativo per l'esercizio dei poteri speciali** da parte del Governo di cui al d.l. 15 marzo 2012, n. 21 ("**d.l. *Golden Power***").

2. Principali novità del Decreto Legge sulla Sicurezza Cibernetica

i. Ambito di applicazione del perimetro di sicurezza nazionale

Ai fini della delimitazione del perimetro di Sicurezza Cibernetica Nazionale, all'articolo 1, è previsto che la disciplina attuativa sia definita attraverso alcuni decreti del Presidente del Consiglio dei ministri (DPCM) – da aggiornarsi con cadenza biennale in relazione all'evoluzione tecnologica – adottati su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), e un decreto del presidente della Repubblica (DPR). In particolare è previsto che l'implementazione avvenga attraverso:

- un DPCM, da adottarsi entro quattro mesi dalla data di entrata in vigore della legge di conversione, che individui i **soggetti** pubblici e privati rientranti nel perimetro della sicurezza nazionale nonché i **criteri per la formazione degli elenchi delle rispettive reti, sistemi e servizi rilevanti** da tenere aggiornati annualmente. I criteri dovranno essere elaborati da un organismo tecnico di supporto al CISR e gli elenchi, predisposti dai soggetti pubblici e privati, dovranno essere trasmessi rispettivamente alla Presidenza del Consiglio dei Ministri e al Ministero dello Sviluppo Economico che svolgeranno un ruolo di supervisione e attività di ispezione e verifica, e che a loro volta dovranno inoltrare tali dati al Dipartimento delle informazioni per la sicurezza (DIS) e all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione;
- un DPCM, da adottarsi entro dieci mesi dalla data di entrata in vigore della legge di conversione, che provvederà a definire le **procedure per la notifica degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici (da inoltrare al Gruppo di intervento per la Sicurezza informatica in caso di incidente), nonché le **misure** volte a favorire un elevato livello di

[1] Il suddetto Decreto Legge sulla Sicurezza Cibernetica è in vigore dal giorno della sua pubblicazione in GU ma dovrà essere convertito in legge nei 60 giorni successivi alla data di pubblicazione, a pena di decadenza automatica retroattiva (i.e. con effetti *ex tunc*).

sicurezza, relative, *inter alia*, alla gestione e mitigazione degli incidenti e alla loro prevenzione, alla gestione operativa, al monitoraggio, test e controlli;

- un DPR, da adottarsi entro dieci mesi dalla data di entrata in vigore della legge di conversione, che dovrà prevedere un meccanismo più sicuro che i soggetti inclusi nel perimetro dovranno seguire per l'**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 – diversi da quelli inerenti lo svolgimento delle attività connesse ai profili di rilevanza penale – e che dovrà prevedere appositi compiti di verifica dei rischi in capo al Centro di valutazione e certificazione nazionale (CVCN). In particolare è previsto che il CVCN, sulla base di una valutazione del rischio, possa imporre condizioni e test di *hardware* e *software* che andranno ad integrare i bandi o i contratti in questione attraverso clausole che condizionano sospensivamente o risolutivamente l'affidamento dei beni o servizi al rispetto delle condizioni. I soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici sono tenuti ad assicurare al CVCN la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri.

L'articolo 1, inoltre, definisce il sistema sanzionatorio in caso di mancato adempimento agli obblighi di cui allo stesso Decreto Legge sulla Sicurezza Cibernetica, salvo che il fatto costituisca reato e aggiunge anche un'ulteriore fattispecie penale, sanzionata con la reclusione da uno a cinque anni, per chiunque fornisce (o non presta) informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti, tra l'altro, per la predisposizione o l'aggiornamento degli elenchi sopracitati e, in capo all'ente, responsabile ai sensi del d.lgs. 231/2001, prevede la sanzione pecuniaria fino a quattrocento quote.

Infine, sempre all'articolo 1, sono individuate le specifiche competenze attribuite al CVCN e, all'articolo 2, è disciplinata la dotazione di personale qualificato per le esigenze di funzionamento del CVCN, del ministero dello Sviluppo Economico e della Presidenza del Consiglio dei Ministri.

ii. Disposizioni relative ai poteri speciali in materia di comunicazione a banda larga con tecnologia 5G e infrastrutture e tecnologie critiche

L'articolo 3 del Decreto Legge sulla Sicurezza Cibernetica prevede che i **poteri speciali** *ex* art. 1*bis* del d.l. *Golden Power*, in materia di comunicazione elettronica a banda larga con tecnologia 5G, **siano esercitati previa valutazione** del CVCN – secondo la disciplina di cui all'emanando DPR sopra citato, ai sensi dell'articolo 1 del Decreto Legge sulla Sicurezza Cibernetica – sulla presenza di **fattori di vulnerabilità**, capaci di compromettere l'integrità e la sicurezza delle reti e dei dati.

L'articolo 4 invece integra la disciplina dei poteri speciali in materia di infrastrutture e tecnologie critiche di cui all'art. 2, comma 1*ter*, del d.l. *Golden Power*, specificando che la verifica in ordine alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico ricomprende anche il pregiudizio sulla sicurezza delle reti e degli impianti e sulla continuità degli approvvigionamenti, e coordina tale disciplina con l'attuazione del Regolamento UE 2019/452 sul controllo degli investimenti esteri, estendendola a **ulteriori specifiche infrastrutture e tecnologie critiche**, come trasporti, acqua, salute, comunicazione, media.

Inoltre, l'articolo 4 dispone che, sino all'entrata in vigore del regolamento da adottarsi ai sensi dell'art. 2, comma 1*ter*, d.l. *Golden Power*, è soggetto **all'obbligo di notifica alla Presidenza del Consiglio dei Ministri**, di cui al comma 5, dell'art. 2, del d.l. *Golden Power*, l'acquisto a qualsiasi titolo, da parte di un soggetto esterno all'UE, di partecipazioni in società che detengono beni e rapporti nei settori di infrastrutture e tecnologie critiche di cui al Regolamento UE 2019/452 di rilevanza tale da

determinare l'insediamento stabile dell'acquirente, in ragione dell'assunzione del controllo, ai sensi dell'articolo 2359 del codice civile, della società la cui partecipazione è oggetto dell'acquisto.

Infine, all'articolo 5, il Decreto Legge sulla Sicurezza Cibernetica attribuisce al Presidente del Consiglio dei ministri la possibilità di disporre la disattivazione di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei relativi servizi, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi e comunque nei casi di crisi cibernetica di cui al DPCM del 17 febbraio 2017, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, laddove sia indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità.

GIANNI·ORIGONI
GRIPPO·CAPPELLI
PARTNERS

Il presente documento viene consegnato esclusivamente per fini divulgativi.

Esso non costituisce riferimento alcuno per contratti e/o impegni di qualsiasi natura.

Per ogni ulteriore chiarimento o approfondimento Vi preghiamo di contattare:

Francesco Gianni
Founding Partner

Roma
+39 06 478751
fgianni@gop.it

Valentina Canalini
Counsel

Roma
+39 06 478751
vcanalini@gop.it

Sofia Gentiloni Silveri
Associate

Roma
+39 06 478751
sgentilonisilveri@gop.it

gop.it