CONFINDUSTRIA

Nota di Aggiornamento

Decreto-legge n. 105/2019 cd. Decreto Cyber Security

27 novembre 2019

Nota di Aggiornamento

Premessa

Lo scorso 20 novembre, è stata pubblicata in Gazzetta Ufficiale la legge di conversione del DL n. 105/2019 (cd. DL Cyber Security).

Il Decreto detta una serie di misure volte, nel complesso, a: *i)* garantire, per le finalità di sicurezza nazionale, l'integrità e la sicurezza delle reti; *ii)* configurare un sistema di organi, procedure e misure, al fine di consentire un'efficace valutazione tecnica della sicurezza degli apparati e dei prodotti, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

In particolare, il provvedimento, oltre a rafforzare i poteri della Presidenza del Consiglio e dei Ministeri in ambito informatico, istituisce il perimetro di sicurezza nazionale e detta una serie di disposizioni specifiche in materia di affidamenti di forniture di beni, sistemi e servizi ICT (cd. *procurement ICT*) destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale.

Inoltre, nel corso della prima lettura parlamentare del disegno di legge di conversione del DL, la Camera dei Deputati ha approvato un emendamento governativo che ha integrato il provvedimento con alcune disposizioni in tema di esercizio dei poteri speciali del Governo nei settori di rilevanza strategica (cd. *golden power*).

Di seguito, le misure di maggiore interesse per il mondo produttivo.

A) Perimetro di sicurezza nazionale cibernetica

Il provvedimento prevede l'istituzione del **"perimetro di sicurezza nazionale cibernetica"**, al fine di rafforzare i livelli di sicurezza di reti, sistemi informativi e servizi informatici di una serie di soggetti preposti allo svolgimento di attività di rilevanza nazionale.

I **soggetti** da includere in tale perimetro sono le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati aventi una sede nel territorio nazionale, che saranno individuati con DPCM, entro quattro mesi dalla data di entrata in vigore della legge di conversione del DL, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR).

Tale selezione dovrà avvenire sulla base dei seguenti criteri: *i)* i soggetti *devono* esercitare una **funzione essenziale** dello Stato o assicurare un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; *ii)* l'esercizio di tali funzioni e servizi dipende da reti, sistemi informativi e servizi informatici; *iii)* dovrà essere garantito un approccio **graduale**, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che può derivare dal malfunzionamento, dall'interruzione, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e servizi informatici.

Con il medesimo DPCM, saranno individuati anche i criteri per la predisposizione e l'aggiornamento da parte dei soggetti individuati di un **elenco di reti, di sistemi informativi e servizi informatici**, rilevanti ai fini della nuova disciplina. Tale individuazione avverrà sulla base di un'analisi del rischio e di un criterio di gradualità, analogamente alla selezione dei soggetti. L'aggiornamento degli elenchi dovrà avvenire con cadenza almeno annuale.

Procedure per la notifica degli incidenti e livelli di sicurezza

Il Decreto prevede che, con un ulteriore DPCM (su proposta del CISR), da emanare entro 10 mesi dalla entrata in vigore della legge di conversione del DL, saranno disciplinate sia le **procedure per la notifica degli incidenti** che hanno un impatto su reti, sistemi e servizi inclusi nel perimetro di sicurezza nazionale cibernetica, sia le **misure volte a garantirne elevati livelli di sicurezza**, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

In particolare, i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica dovranno notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente, che procede poi a inoltrare tempestivamente tali notifiche al Dipartimento delle informazioni della sicurezza (DIS).

***Procurement* ICT**

Il DL prevede l'adozione di un regolamento governativo, entro dieci mesi dalla data di entrata in vigore della legge di conversione, per la definizione di procedure, modalità e termini del cd. ***procurement ICT***, nonché delle relative misure di vigilanza.

In particolare, prevede che i soggetti inclusi nel perimetro di sicurezza nazionale, ovvero le centrali di committenza alle quali essi fanno ricorso, 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 nei citati elenchi, ne debbano dare comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il MiSE, allegando anche la **valutazione del rischio associato** all'oggetto della fornitura.

Sugli affidamenti che vengono notificati, il CVCN può effettuare **verifiche preliminari e imporre condizioni e test di *hardware* e *software*,** da compiere anche in collaborazione con i soggetti interessati.

Al riguardo, in base a un correttivo apportato durante l'iter parlamentare nella direzione auspicata dalle imprese dei settori interessati, la procedura di verifica e imposizione di tali test dovrà avvenire secondo un **approccio gradualmente crescente** e dovrà concludersi entro quarantacinque giorni, prorogabili una sola volta in caso di particolare complessità. Una volta decorso il termine senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione potranno comunque proseguire nella procedura di affidamento.

In caso di imposizione di condizioni e *test*, i bandi di gara e i contratti dovranno essere integrati con clausole che ne condizionino (sospensivamente o

risolutivamente) l'operatività al rispetto delle condizioni o all'esito favorevole dei test disposti.

Per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici **del Ministero della difesa** o **del Ministero dell'interno**, gli stessi Ministeri possono procedere attraverso la comunicazione ai propri centri di valutazione, accreditati presso il CVCN.

Sono **esclusi dall'obbligo di comunicazione** gli affidamenti delle forniture di beni, sistemi e servizi ICT destinati a reti, sistemi e servizi informatici per lo svolgimento delle attività di **prevenzione, accertamento e repressione dei reati** e i casi di deroga stabiliti con riguardo alle forniture per le quali sia indispensabile procedere in **sede estera**.

Regime sanzionatorio

Il provvedimento prevede anche un articolato regime sanzionatorio per il mancato assolvimento degli obblighi introdotti. In particolare, sono previste **sanzioni amministrative pecuniarie** che, nel complesso, partono dai 200.000 euro e arrivano fino a 1.800.000 euro.

L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in assenza della comunicazione o del superamento dei *test* o in violazione delle condizioni imposte comporta, oltre alle relative sanzioni amministrative pecuniarie (da 300.000 a 1.800.000 euro), la **sanzione amministrativa accessoria** dell'incapacità di assumere incarichi di direzione, amministrazione e controllo per un periodo di tre anni decorrente dalla data di accertamento della violazione.

Inoltre, è prevista la pena della **reclusione da uno a tre anni** per coloro che, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici e quelli relativi all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti e sui sistemi informativi o delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Mise forniscono informazioni, dati o fatti non rispondenti al vero o che omettono di comunicare i predetti dati, informazioni o elementi di fatto.

Questa nuova fattispecie di reato è, inoltre, inserita nel catalogo dei reati presupposto della **responsabilità amministrativa degli enti** di D.lgs. n. 231/2001 e, quindi, potranno essere chiamate e risponderne anche le società, nei confronti delle quali la sanzione pecuniaria applicabile è fino a 400 quote.

B) Golden power e misure in tema di reti di telecomunicazione elettronica a banda larga con tecnologia 5G

Il provvedimento prevede una serie di modifiche al DL n. 21/2012, recante disposizioni in tema di poteri speciali del Governo (cd. Golden power), per la cui

analisi si rinvia alla nota CoPre del 6 novembre, non essendo stati apportati ulteriori correttivi in sede di approvazione definitiva (v. Allegato).

Rimanendo in tema di Golden power, il DL contiene disposizioni di raccordo tra la nuova disciplina introdotta e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla **tecnologia 5G**.

In particolare, il DL stabilisce che le nuove disposizioni si applicano ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica anche con riferimento ai contratti o agli accordi (se conclusi con soggetto extra Ue) relativi ai **servizi di comunicazione elettronica a banda larga basato sulla tecnologia a 5G.**

Tuttavia, posto che tali soggetti sono già obbligati a effettuare la notifica alla Presidenza del Consiglio per l'esercizio dei poteri speciali di cui al DL n. 21/2012 (DL sul golden power), agli stessi non si applica la nuova disciplina del DL in tema di comunicazione al CVCN relativa al *procurement ICT*, già descritta.

Come già rilevato nella nota allegata, quanto ai poteri speciali, il DL prevede che, dopo l'entrata in vigore del regolamento sulle procedure relative al *procurement* ICT, essi saranno esercitati previa valutazione, secondo i rispettivi ambiti di competenza, da parte del CVCN, del Centro di valutazione del Ministero della difesa e del Ministero dell'interno, degli **elementi indicanti la presenza di fattori di vulnerabilità** che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano.

Infine, il DL stabilisce, in via **transitoria**, la possibilità di ridefinire, ove risulti necessario e nel termine di sessanta giorni dalla data di entrata in vigore del regolamento, le condizioni o le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati, al fine di garantire livelli di sicurezza equivalenti a quelli previsti dal DL, anche prescrivendo la sostituzione di apparati o prodotti.

C) Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica

Infine, il DL stabilisce che il Presidente del Consiglio, su deliberazione del CISR, possa disporre la **disattivazione, totale o parziale, di uno o più apparati o prodotti** impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati, nel caso in cui si verifichi un **rischio grave e imminente per la sicurezza nazionale** connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici.

Tale intervento deve risultare indispensabile e realizzarsi per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di **proporzionalità**.

ALLEGATO

DL n. 105/2019 (cd. DL Cyber Security)

Nota CoPre del 6 novembre 2019

Il Decreto interviene sul quadro normativo in materia di esercizio dei poteri speciali da parte del Governo - cd. *Golden power* - in considerazione dell'evoluzione tecnologica intercorsa e dei rischi per la sicurezza nazionale connessi a un uso improprio dei dati. In particolare, il DL n. 21/2012 viene modificato e integrato in modo da comprendere l'attuazione del Regolamento (UE) 2019/452 sul controllo degli investimenti esteri e prevedere misure di tutela di infrastrutture o tecnologie critiche non ricadenti nel campo di applicazione di tale quadro normativo.

Di seguito, un dettaglio delle principali modifiche.

Poteri speciali nel settore della difesa e della sicurezza nazionale

- Per l'esercizio dei poteri speciali - *i.e*. di imporre condizioni, di veto, di opporsi all'acquisito - da parte del Governo viene previsto un ampliamento dei termini (da 15 a 45 giorni) e viene arricchita l'informativa da rendere al Governo medesimo, che può anche formulare richieste istruttorie a terzi;

- con riferimento al potere di veto, quest'ultimo viene esteso anche ad atti o operazioni da parte delle imprese che detengono *asset* strategici; con riferimento agli altri poteri speciali, vengono individuate ulteriori e particolari circostanze che il Governo può tenere in considerazione qualora l'acquisto sia effettuato da un soggetto extra UE;

- viene previsto un obbligo di notifica, qualora l'acquirente venga a detenere una partecipazione qualificata anche nell'ipotesi di acquisto di partecipazioni di una società non ammessa alla negoziazione nei mercati regolamentati.

Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G

- In sede di prima applicazione dell'obbligo di notifica della stipula di contratti o accordi riguardanti tecnologie 5G, posti in essere con soggetti extra UE, viene richiesta un'informativa completa sui contratti o accordi conclusi prima del 26 marzo 2019 e che non siano in corso di esecuzione**;**

- viene disciplinata un'apposita procedura di notifica, in modo da renderla simmetrica a quella per l'esercizio dei poteri speciali nei settori della difesa e

della sicurezza nazionale, con previsione della sanzione connessa alla violazione (pena pecuniaria fino al 50% per cento del valore dell'operazione e comunque non inferiore al 25% del medesimo valore);

•viene previsto che l'esercizio dei poteri speciali venga effettuato previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità da parte dei centri di valutazione individuati dalla nuova normativa e, con riferimento alle autorizzazioni già rilasciate, viene riconosciuta la possibilità di integrare o modificare le misure prescrittive già previste alla luce dei nuovi standard.

Poteri speciali inerenti agli attivi strategici nei settori dell'energia, dei trasporti e delle comunicazioni

• Viene semplificato e velocizzato l'*iter* procedurale per l'adozione dei decreti per individuare gli *asset* di rilevanza strategica (decreti del Presidente del Consiglio dei Ministri e non della repubblica, anche in deroga alle procedure all'uopo richieste dalla legge n. 400/1988);

• nel delimitare l'ambito oggettivo di applicazione, viene espunta l'elencazione dei settori ad alta intensità tecnologica, che comunque sono ricompresi nel Regolamento sullo *screening* degli investimenti esteri diretti;

• viene introdotta una specifica disciplina per la notifica di delibere, atti o operazioni relativi agli ulteriori *asset* strategici, quando siano idonei ad avere effetti a favore di un soggetto extra UE o altri effetti consistenti sugli *asset* medesimi;

• viene delineata una procedura sostanzialmente analoga a quanto previsto per l'esercizio dei poteri speciali del Governo negli altri settori (i.e. ampliamento dei termini, informativa rafforzata);

• viene sostituita la definizione di soggetto esterno all'Unione europea, in modo da renderla univoca ai fini dell'esercizio dei poteri speciali nei vari settori;

• viene modificato e integrato il criterio per determinare se un investimento estero diretto possa incidere sulla sicurezza e sull'ordine pubblico.

Infine, viene introdotta una nuova forma di collaborazione tra autorità amministrative di settore che impone a Banca d'Italia, CONSOB, COVIP, IVASS, ART, AGCM, AGCOM, ARERA e il Gruppo di coordinamento all'uopo costituito di collaborare tra loro, anche mediante scambio di informazioni e senza poter opporre il segreto d'ufficio, al fine di agevolare l'esercizio delle funzioni di cui al decreto.