PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA: OPERATORI PRIVATI STRATEGICI IN PRIMA LINEA.

Con la recente conversione in legge[1] del d.l. 21 settembre 2019, n. 105 , recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (il "**Decreto**"), si consolidano le regole e gli obblighi a carico dei **soggetti privati che prestano servizi di rilevanza strategica a livello nazionale**. Tali soggetti saranno tenuti ad assicurare **elevanti livelli di sicurezza dei sistemi informatici e delle reti**. Per le violazioni sono previste **sanzioni fino ad 1,8 milioni di Euro**. Nel contesto della tutela della sicurezza nazionale e dei settori strategici, si introducono **significative novità in ambito "Golden Power"**.

Key issues

- Privati in settori strategici inclusi nel perimetro di sicurezza nazionale cibernetica
- Previsti nuovi obblighi di trasmissione degli elenchi delle reti
- Previste misure organizzative per garantire livelli elevati di cyber sicurezza
- Violazioni dei nuovi obblighi punite con sanzioni da un minimo di Euro 200.00 ad un massimo di Euro 1.800.000
- Introdotte disposizioni di coordinamento con la normativa NIS
- Golden Power: estesi i poteri del Governo anche a settori "ad alta densità tecnologica"

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Il Decreto istituisce il perimetro di sicurezza nazionale cibernetica (il "**Perimetro**") al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici (i) dal cui malfunzionamento, interruzione od uso improprio può derivare un pregiudizio per la sicurezza nazionale e (ii) e che siano gestiti dai soggetti che prestano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per l'interesse dello state.

Entro quattro mesi dalla data di entrata in vigore della legge di conversione (quindi in data 21 marzo 2020), un decreto del Presidente del Consiglio dei Ministri individuerà i **gli enti e gli operatori nazionali pubblici e privati con sede nel territorio nazionale da includere nel Perimetro**, che saranno tenuti ad osservare gli obblighi e le disposizioni di cui al Decreto.

Criteri di individuazione dei soggetti inclusi nel Perimetro:

- il soggetto assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
- l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;
- nell'individuazione si tiene conto, secondo un criterio di gradualità, del pregiudizio per la sicurezza nazionale, **in relazione alla specificità dei diversi settori di attività**, che può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici.

[1] Legge 18 novembre 2019, n. 133.

GLI OBBLIGHI A CARICO DEI SOGGETTI RIENTRANTI NEL PERIMETRO

Comunicazione degli elenchi

Entro sei mesi dall'entrata in vigore del decreto di individuazione dei soggetti inclusi nel Perimetro, gli stessi saranno tenuti ad inviare alla Presidenza del Consiglio dei Ministri e al Ministero dello Sviluppo Economico un elenco, **da aggiornare almeno una volta all'anno**, delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza.

Obbligo di notifica dei *cyber incidents*

Ulteriore novità di notevole impatto per i soggetti inclusi nel Perimetro consiste nell'obbligo di notifica dei *cyber incidents*: verranno infatti definite con apposito decreto del Presidente del Consiglio di Ministri, da emanarsi **entro dieci mesi dall'entrata in vigore della legge di conversione (quindi entro il 21 settembre 2020)**, le specifiche procedure secondo le quali i soggetti inclusi nel Perimetro saranno tenute a **notificare al Computer Security Incident Response Team (CSIRT) italiano ogni incidente che abbia avuto un impatto sulle reti, sui sistemi informativi o sui servizi informatici** di rispettiva pertinenza. Il CSIRT, a sua volta, avrà il compito di inoltrare tempestivamente tali notifiche al Dipartimento delle informazioni per la sicurezza, anche per le attività demandate al Nucleo per la sicurezza cibernetica.

Misure per garantire elevati livelli di sicurezza informatica

Con il medesimo decreto attuativo da adottarsi entro il 21 settembre 2019, la Presidenza del Consiglio dei Ministri elaborerà inoltre le **misure volte a garantire elevati livelli di sicurezza** delle reti, dei sistemi informativi e dei servizi informatici di pertinenza dei soggetti inclusi nel Perimetro.

Tali misure terranno conto degli **standard definiti a livello internazionale e dell'Unione Europea**, e riguarderanno i seguenti ambiti:

- struttura organizzativa preposta alla gestione della sicurezza;
- politiche di sicurezza e gestione del rischio;
- mitigazione e gestione degli incidenti e prevenzione, anche con interventi su apparati o prodotti gravemente inadeguati sul piano della sicurezza;
- protezione logica e fisica dei dati;
- integrità delle reti e dei sistemi informativi;
- gestione operativa, con specifico riguardo alla continuità del servizio;
- monitoraggio, test e controllo;
- formazione e consapevolezza;
- affidamento di forniture di beni, sistemi e servizi di *information and communication technology* ICT, anche mediante la definizione di caratteristiche e requisiti di carattere generale.

Contratti con efficacia condizionata al superamento di test *hardware/software*

I soggetti inclusi nel Perimetro e appartenenti a categorie individuate da un decreto del Presidente del Consiglio dei Ministri[2], 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, dovranno fornire **apposita comunicazione, completa di valutazione del rischio associato all'oggetto della fornitura, al Centro di valutazione e certificazione nazionale** (CVCN) da istituirsi presso il Ministero dello sviluppo economico.

Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili una sola volta di ulteriori quindici giorni, Il CVCN può effettuare **verifiche**, imporre **condizioni** e imporre l'esecuzione di **test *hardware* e *software***.

In tal caso, il Decreto impone **l'integrazione dei contratti di fornitura** (o dei bandi di gara, nel caso di amministrazioni) **con clausole che subordinano, sospensivamente o risolutivamente, l'efficacia degli stessi al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.**

SANZIONI

Salvo che le medesime violazioni costituiscano reato, l'art. 1, comma 9, del Decreto **introduce consistenti sanzioni amministrative** per le violazioni dei nuovi obblighi. In particolare, ai soggetti privati il Ministero dello Sviluppo Economico può applicare le seguenti sanzioni:

- **da Euro 300.000 a Euro 1.800.000** per la mancata comunicazione al CVCN o l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN;
- **da Euro 250.000 a Euro 1.500.000** per il mancato tempestivo adempimento dell'obbligo di notifica, l'inosservanza delle misure di sicurezza di cui sopra e la mancata collaborazione per l'effettuazione dei testi imposta dal CVCN, il mancato adempimento delle prescrizioni del Ministero dello Sviluppo Economico o della Presidenza del Consiglio dei Ministro all'esito di attività ispettive, il mancato rispetto delle prescrizioni del CVCN;
- **da Euro 200.000 a 1.200.000**, per la violazione degli obblighi di predisposizione e aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici.

E' introdotta la pena della **reclusione da uno a tre anni** per chiunque, allo scopo di ostacolare o condizionare l'espletamento dei menzionati procedimenti di verifica della sicurezza informatica dei soggetti compresi nel Perimetro o lo svolgimento delle attività ispettive e di vigilanza, fornisca informazioni, dati o elementi di fatto non rispondenti al vero od ometta di comunicarli entro i termini prescritti. **Il reato è inserito nel novero degli illeciti presupposto di responsabilità degli enti ai sensi del d.lgs. 8 giugno 2001, n. 231.**

COORDINAMENTO CON LA DISCIPLINA "NIS"

Gli **operatori di servizi essenziali** (OSE), i **fornitori di servizi digitali** individuati ai sensi del d.lgs. 18 maggio 2018, n. 65, emanato in attuazione della

[2] Pure da adottarsi entro dieci mesi dall'entrata in vigore della legge di conversione.

direttiva NIS[3], e le **imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico**, di cui al codice delle comunicazioni elettroniche (d.lgs. 259/2003), **inclusi nel perimetro di sicurezza nazionale cibernetica**, dovranno inoltre:

- Osservare le misure di sicurezza informatica previste dai rispettivi decreti legislativi di riferimento sopra indicati, **se di livello almeno equivalente a quelle adottate ai sensi del Decreto**. Il Ministero dello Sviluppo Economico ha il compito di individuare, **per i privati, le ulteriori misure aggiuntive eventualmente necessarie** per assicurare il raggiungimento dei livelli di sicurezza previsti dal Decreto.
- La notifica dei *cyber incidents* effettuata ai sensi del Decreto **vale ad assolvere l'obbligo di notifica degli incidenti con impatto rilevante sul servizio fornito**, di cui agli artt. 12-14 del d.lgs. 65/2018 (notifica NIS) e di cui all'art. 16-*ter* del Codice delle Comunicazioni Elettroniche. A tal fine, il CSIRT italiano ha il compito di inoltrare al Ministero competente le notifiche.

NOVITA' IN TEMA "GOLDEN POWER"

Il Decreto estende anche i poteri del Governo in materia di c.d. Golden Power di cui al d.l. 21/2012, con la quale si intendono i poteri speciali del Governo rispetto ad acquisizioni di società nazionali in ambiti di rilevanza strategica nei settori dell'energia, dei trasporti, delle comunicazioni. Secondo il Decreto:

- con appositi provvedimenti attuativi, da adottarsi entro centoventi giorni dall'entrata in vigore del Decreto, saranno individuati i c.d. "**settori ad alta intensità tecnologica**" a cui si applica la normativa Golden Power, tenuto conto delle tecnologie, dei fattori produttivi critici e delle informazioni sensibili indicate all'art. 4, par. 1 regolamento (UE) 2019/452.
- Il Governo ha ora **fino a 45 giorni dalla notifica dell'operazione rientrante in ambito "Golden Power" per esercitare i propri poteri**. Se richiede ulteriori informazioni ai notificanti, il termine di 45 giorni è sospeso, fino a ricevimento delle informazioni, **da comunicarsi entro 10 giorni dalla richiesta**. Tale ultimo termine è **aumentato a 20 giorni** se il destinatario della richiesta di informazioni è una soggetto terzo rispetto all'operazione.
- Viene introdotta l'ulteriore **soglia del 50% delle partecipazioni in società che svolgono attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale**, che consente al Governo di esercitare i propri poteri speciali.
- Con anticipo sull'entrata in vigore del Regolamento (UE) 2019/452[4], vengono introdotte disposizioni di adeguamento che comportano, fra l'altro, **un possibile aumento del termine di 45 giorni entro cui il governo può esercitare i propri poteri speciali**, ove uno Stato Membro, o la Commissione Europea, comunichino l'intenzione di formulare osservazioni o di emettere un parere in relazione ad un operazione.

[3] Direttiva (Ue) 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("**Direttiva NIS**"). Con riguardo alla disciplina NIS, si rinvia al nostro precedente *briefing* disponibile qui.

[4] Regolamento (UE) 2019/452 del 19 marzo 2019 che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione.

CLIFFORD
CHANCE

AUTORI

Carlo Felice Giampaolino
Partner, Roma

T +39 064223 1356
E carlofelice.giampaolino @cliffordchance.com

Alessandro Sciarra
Associate, Roma

T +39 064229 1384
E alessandro.sciarra @cliffordchance.com

NETWORK

Jonathan Kewley
Partner, Londra

T +44 207006 3629
E jonathan.kewley @cliffordchance.com

Dessislava Savova
Partner, Parigi

T +33 14405 5483
E dessislava.savova @cliffordchance.com

Richard Jones
Director of Data Privacy, Londra

T +44 207006 8238
E Richard.jones @cliffordchance.com

Megan Gordon
Partner, Washington DC

T +1 202 912 5021
E megan.gordon @cliffordchance.com

Grégory Sroussi
Counsel, Parigi

T +33 14405 5248
E gregory.sroussi @cliffordchance.com

Maxime D'Angelo Petrucci
Avocat, Parigi

T +33 14405 5167
Emaxime.dangelopetrucci @cliffordchance.com

www.cliffordchance.com

Clifford Chance, Via di Villa Sacchetti, 11, 00197 Rome, Italy

Clifford Chance Studio Legale Associato

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.