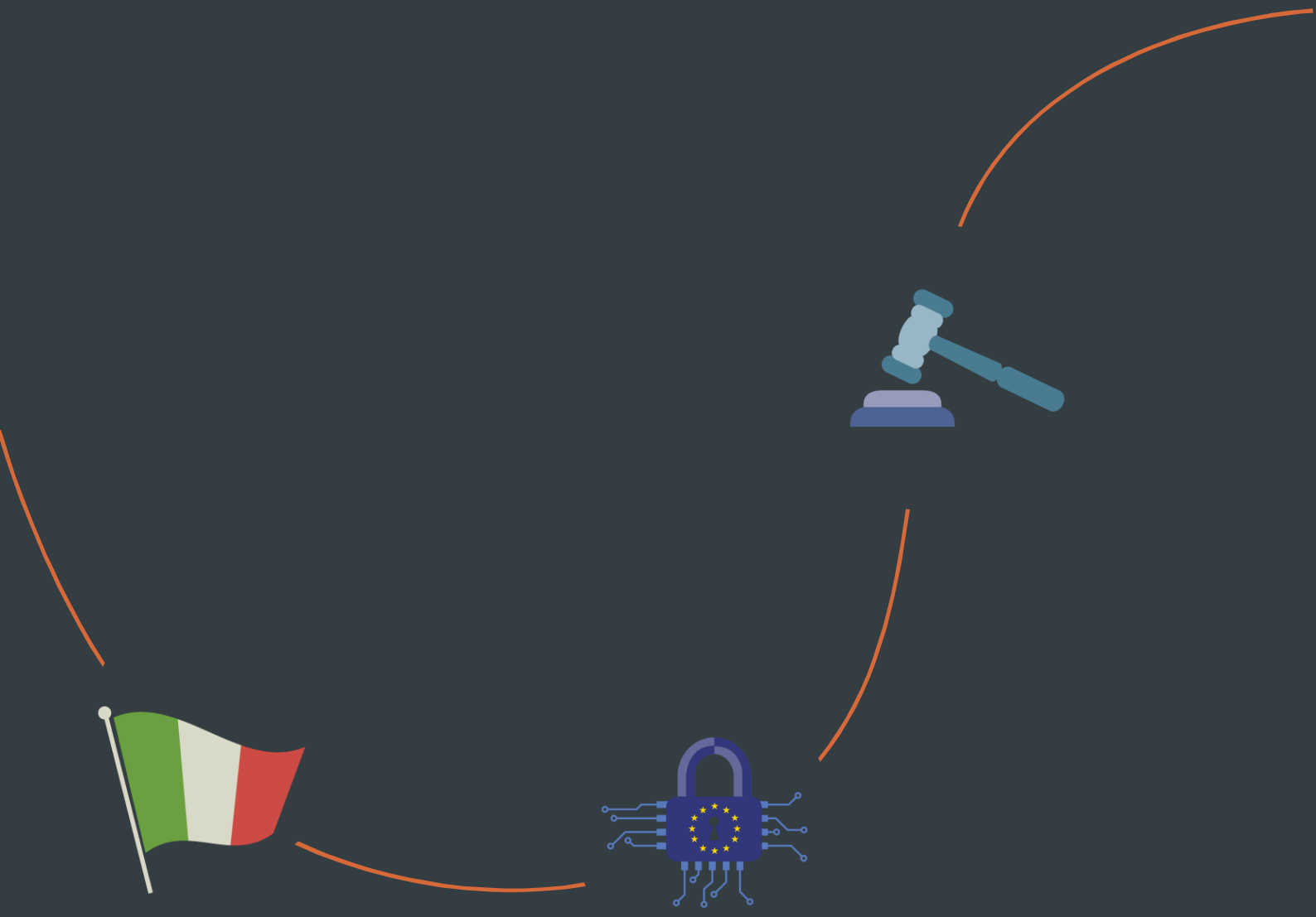
Bird & Bird

# DPCM 131/2020: nuove disposizioni in materia di *Cybersecurity*



# DPCM 131/2020: nuove disposizioni in materia di *cybersecurity*

È stato finalmente pubblicato nella Gazzetta Ufficiale del 21 ottobre u.s. il testo del Decreto del Presidente del Consiglio dei Ministri n. 131/2020, il primo dei decreti attuativi del perimetro di sicurezza nazionale cibernetica (di seguito, il "**Perimetro**") introdotto dal Decreto-legge 105/2019.

Scopo del DPCM, che entra in vigore il 5 novembre 2020, è quello di stabilire i parametri con cui sono individuati dalle autorità preposte i soggetti pubblici e privati che rientrano all'interno del Perimetro, i quali svolgono funzioni o prestano servizi essenziali per lo Stato.

## Definizione e circoscrizione del Perimetro

L'articolo 2 del DPCM identifica così tali soggetti:

1 un soggetto esercita una **funzione essenziale** dello Stato, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti;

2 un soggetto, pubblico o privato, presta un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Successivamente, all'articolo 3 vengono individuati i settori a cui appartengono i soggetti ricompresi nel Perimetro: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro.

## Individuazione soggetti del Perimetro

Per l'individuazione e l'elencazione effettiva dei soggetti rientranti nel Perimetro appartenenti ai suddetti settori, l'articolo 4 prevede che tale attività di individuazione venga svolta dalla specifica Amministrazione pubblica competente per singolo settore (individuata al comma 2 dell'articolo 3).

In particolare, le amministrazioni a cui è richiesta l'attività di individuazione dei soggetti rientranti nel Perimetro, sono tenute innanzitutto a identificare le funzioni e i servizi essenziali erogati da ciascun soggetto (nel proprio settore di competenza) dipendenti da i) reti ii) sistemi informativi e iii) sistemi informatici la cui interruzione o compromissione possano arrecare pregiudizio alla sicurezza nazionale.

Una volta individuati i soggetti, le amministrazioni dovranno anche valutare gli effetti negativi dell'interruzione della funzione o del servizio essenziale e della compromissione, in termini di perdita di disponibilità, integrità e riservatezza dei dati e delle informazioni.

È previsto anche un ulteriore criterio di valutazione, basato sulle tempistiche di mitigazione, cioè una stima dei tempi di ripristino necessari per ristabilire l'erogazione della funzione/servizio in condizioni di sicurezza, sia integralmente, sia "*temporaneamente,*

*con modalità prive di supporto informatizzato ovvero anche parzialmente da altri soggetti*".

Le amministrazioni predispongono quindi la lista di soggetti così individuati (per il proprio settore di competenza) e lo trasmettono al CISR tecnico, per le valutazioni di sorta. L'elencazione dei soggetti è contenuta in un atto amministrativo, adottato e periodicamente aggiornato dalla Presidenza del Consiglio dei Ministri, su proposta del CISR. Spetta poi al DIS comunicare al soggetto la sua inclusione nel Perimetro, entro trenta giorni dall'avvenuta iscrizione. Nella comunicazione vengono indicati la funzione essenziale o il servizio essenziale in relazione al cui espletamento il soggetto è stato incluso nell'elenco.

È importante notare come similmente a quanto fatto con gli OSE (Operatori di Servizi Essenziali) individuati a norma del Decreto-legislativo 65/2018 e della Direttiva NIS, l'elenco dei soggetti rientranti nel Perimetro non è soggetto a pubblicazione (restando di fatto secretato), fermo restando che a ciascun soggetto è data, separatamente, comunicazione dell'avvenuta iscrizione nell'elenco.

## Obblighi dei soggetti del Perimetro

Ricevuta la comunicazione di iscrizione nell'elenco, a norma dell'articolo 7 i soggetti inclusi nel Perimetro sono chiamati a predisporre e ad aggiornare, con cadenza almeno annuale, l'elenco dei **propri beni ICT** (che secondo la stessa definizione data dal DPCM, ricomprende "*un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura, considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali*"), con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono, secondo i criteri individuati dal comma 2 dello stesso articolo 7.

Allo stesso modo (articolo 8 del DPCM), i soggetti del Perimetro dovranno predisporre un secondo **elenco contenente la descrizione dell'architettura e della componentistica** relativa ai propri beni ICT.

Quindi, come previsto dall'articolo 9, entro sei mesi dalla comunicazione di inserimento nel Perimetro, entrambi questi elenchi dovranno essere trasmessi alla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione (nel caso dei soggetti pubblici) o al Mise (nel caso dei privati).

## Perimetro di sicurezza nazionale cibernetica: cosa manca

Va poi sottolineata la connessione di questo DPCM con i successivi decreti attuativi ancora da emettere.

L'articolo 11 dispone infatti che i soggetti rientranti nel Perimetro dovranno notificare eventuali incidenti al CSIRT, secondo le modalità indicate dal DPCM previste dall'articolo 1 comma 3 del Decreto-legge 105/2019, ancora da scrivere, e probabile oggetto del secondo decreto attuativo.

Ancora più importante risulta invece il collegamento che lo stesso articolo 11 fa con il regolamento (da adottarsi con decreto del Presidente della Repubblica) previsto dall'articolo 1 comma 6 del Decreto-legge 105/2019, in materia di **affidamento di forniture di beni, sistemi e servizi ICT** destinati a essere impiegati dai soggetti rientranti nel Perimetro, che dovranno essere sottoposti al controllo preventivo del Centro di valutazione e certificazione nazionale (CVCN) istituito presso il Ministero dello Sviluppo Economico.

I soggetti del Perimetro che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT saranno infatti tenuti a rendere una dettagliata comunicazione al CVCN, descrivendo i prodotti e i servizi oggetto della fornitura, e fornendo anche una valutazione del rischio associato all'oggetto della fornitura, in relazione all'ambito di impiego.

Il CVCN, a sua volta, potrà effettuare verifiche preliminari e imporre condizioni e *test,* sia *hardware* che *software*, sui prodotti e servizi oggetto della fornitura.

Appare evidente come tale previsione, già contenuta nel Decreto-legge 105/2019 e in attesa di ulteriori chiarimenti nel prossimo decreto attuativo, sposti l'attenzione sui servizi o prodotti ICT di qualunque fornitore, sottoponendoli ad un controllo rigoroso e preventivo al fine individuare potenziali punti deboli e *backdoor*, con ovvie conseguenze sulle responsabilità definite nei contratti di fornitura: d'altronde gli stessi fornitori sono chiamati ad assicurare al CVCN la propria collaborazione per l'effettuazione dei *test* di *hardware* e *software* sostenendone i conseguenti oneri economici.

## Direttiva NIS e Perimetro

Resta poi da approfondire il rapporto tra Perimetro e Direttiva NIS. Il Decreto-legge 105/2019 prevede

che in caso di individuazione di un soggetto del Perimetro che sia contemporaneamente OSE o FSD (fornitori di servizi digitali) secondo la direttiva NIS, questi sia tenuto ad osservare le misure di sicurezza previste dalla disciplina NIS se di livello almeno equivalente alle misure adottate per attuare il Perimetro.

Al tempo stesso, è anche previsto che la Presidenza del Consiglio dei Ministri (per i soggetti pubblici) e il Mise (per i soggetti privati) possano definire eventuali misure aggiuntive necessarie ad assicurare i livelli di sicurezza previsti per il Perimetro, raccordandosi con le autorità NIS.

Da valutare poi anche il sistema delle notifiche. È infatti previsto che l'assolvimento da parte dei soggetti del Perimetro di notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici costituisca anche adempimento dell'obbligo di notifica previsto dal Decreto-legislativo 65/2018 e della direttiva NIS. Le notifiche saranno successivamente inoltrate dal CSIRT anche alla competente autorità NIS.

# Contatti


Roberto Camilli
Partner

Tel: +390230356000
roberto.camilli@twobirds.com



Gabriele Ferrante
Senior Associate

Tel: +390230356000
gabriele.ferrante@twobirds.com


twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw & Satellite Office: Casablanca