23 Agosto 2021

Perimetro di Sicurezza Nazionale Cibernetica: individuate le categorie di beni, sistemi e servizi ICT soggetti alla procedura di valutazione del CVCN

Nell'ambito del quadro normativo che stabilisce gli obblighi di comunicazione di avvio delle procedure di *procurement* al Centro di Valutazione e Certificazione Nazionale (di seguito "**CVCN**"), unitamente al Decreto del Presidente della Repubblica 54/2021 (di seguito "**DPR 54/2021**"), si inserisce il nuovo Decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante "*l'individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*" (di seguito "**DPCM 3**"), il quale è stato recentemente pubblicato in Gazzetta Ufficiale.

1. Cosa prevede il DPCM 3

Il DPCM 3 individua le categorie in relazione alle quali i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT (*information and communication technology*), destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici inseriti nell'elenco dei beni ICT inseriti nel Perimetro di Sicurezza Nazionale Cibernetica, **effettuano la comunicazione di avvio della procedura di *procurement* al CVCN**.

2. Quali sono le categorie

Le categorie sono individuate sulla base dei criteri tecnici di cui all'articolo 13, comma 1, del DPR 54/2021, e sono indicate nell'elenco di cui all'allegato 1 del DPCM 3.

In particolare, **il legislatore ha deciso di includere le seguenti categorie**:

i) **componenti *hardware* e *software* che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)**.

In tale categoria rientrano i seguenti beni, sistemi e servizi: Router; Switch; Repeater; Bilanciatori di carico; Traffic shaper; Proxy; Ponte radio; Access Network per reti radiomobili; 2G, 3G, 4G, 5G; Gateway Wifi; Network Function Virtualizatio (NFV) tra cui vSwitch, vRouter, Application Function (5G); Optical transmission board; Multiservice Provisioning Platform (MSPP); Automotive ECU switch (Ethernet, CAN, LIN); IoT Edge Gateway.

ii) **componenti *hardware* e *software* che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati**.

In tale categoria rientrano i seguenti beni, sistemi e servizi: Firewall; Security Gateway; Hardware Security Module (HSM); Intrusion Detection System (IDS); Intrusion Prevention System (IPS); Network Function Virtualization (NFV), tra cui Authentication Server Function (5G) e Whitelisting dei processi; Virtual Private Network (VPN); Trusted Platform Module.

iii) **componenti *hardware* e *software* per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali**.

In tale categoria rientrano i seguenti beni, sistemi e servizi: Sistemi SCADA (Supervisory Control And Data Acquisition); Manufacturing Execution Systems (MES); Software Defined Network (SDN) Controller; Sistemi Artificial Intelligence (AI) e Machine Learning (ML) per gestione reti/sistemi; 5G Mobile Edge Computing (MEC); NFV tra cui Network Slice Selection Function (5G), Application Function (5G), Policy Control Function (5G), Unified Data Management (5G), Session Management Function (5G); Management and Orchestration (MANO); IoT orchestrator.

iv) **applicativi *software* per l'implementazione di meccanismi di sicurezza**.

In tale categoria rientrano i seguenti beni, sistemi e servizi: Applicazioni informatiche per la sicurezza, tra cui Public Key Infrastructure (PKI), Single Sign-On (SSO), Controllo Accessi; Moduli software che implementano Web Service mediante API, per protocolli di comunicazione.

3. Aggiornamento delle categorie

Le categorie individuate dal DPCM 3 saranno aggiornate, con decreto del Presidente del Consiglio dei ministri, **con cadenza almeno annuale**, avuto riguardo all'innovazione tecnologica, nonché alla modifica dei criteri tecnici di cui all'articolo 13, comma 1, del DPR 54/2021.

4. Entrata in vigore del DPCM 3

Secondo quanto stabilito dall'articolo 5 del DPCM 3, esso "***entra in vigore il giorno successivo a quello dell'entrata in vigore del DPR 54/2021***".

Pertanto, al fine di rendere coerente l'impianto normativo nella sua interezza, il legislatore ha previsto l'efficacia retroattiva del DPCM 3, prevedendo la sua entrata in vigore il 9 maggio 2021.

5. Decorrenza dell'obbligo di comunicazione al CVCN

In ultimo, si segnala che l'articolo 16, comma 9, del Decreto-legge 14 giugno 2021, n. 82, recante le disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, sancisce che "*l'obbligo di comunicazione al CVCN di avvio della procedura di affidamento sarà efficace a decorrere dal trentesimo giorno successivo alla pubblicazione in Gazzetta Ufficiale di un ulteriore decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesterà l'operatività del CVCN e comunque dal 30 giugno 2022*".

Pertanto, **l'obbligo di comunicazione al CVCN diverrà efficace e applicabile ai soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica solo a seguito dell'emanazione di un ulteriore DPCM, ad oggi non ancora pubblicato, che sancirà l'operatività del CVCN, e comunque in caso di eventuale sua assenza dal 30 giugno 2022**.

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:

Stefano Mele
Partner
Proprietà Intellettuale, TMT e Cybersecurity
Roma/Milano
+39 06 478751/+39 02 763741
smele@gop.it