Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti

1. È stata pubblicata sulla Gazzetta Ufficiale n. 272 del 20 novembre 2019 la legge 18 novembre 2019, n. 133, di "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica". Come recita il comma 1 dell'art. 1, il provvedimento (che è entrato in vigore il 21 novembre 2019) intende "assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale". Per cui è introdotta un'articolata disciplina che definisce i soggetti pubblici e privati coinvolti, i vari obblighi ed adempimenti cui sono tenuti, i rischi e le misure da adottare per fronteggiarli, i poteri di certificazione, controllo, ispezione, prescrizione delle autorità governative, le norme in materia di acquisizione e utilizzazione delle tecnologie rilevanti, e quant'altro.

2. Sul piano penale introduce all'art. 1 comma 11 una nuova articolata fattispecie a struttura "sanzionatoria" rispetto alla predetta disciplina extrapenale, che così recita:
" *Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni*".

La norma delinea così diversi reati propri, a dolo specifico, sostanziantisi in falsità ideologiche "rilevanti" ai fini della predetta disciplina extrapenale cui è accessoria, ed in un reato di omissione propria, tutti ascrivibili solo ai soggetti - pubblici e privati - aventi sede nel territorio nazionale, che siano inclusi nel "perimetro di sicurezza nazionale cibernetica" quale definito e disciplinato da detta nuova normativa.

3. Le condotte delittuose non sono compiutamente tipizzate nella fattispecie penale, in quanto essa rinvia agli articolati obblighi giuridici, con relativi termini di adempimento, imposti in tema di sicurezza nazionale cibernetica, che dovranno essere definiti nel dettaglio da norme secondarie di attuazione.

In particolare, il comma 2, lett. b), del citato art. 1, stabilisce che entro quattro mesi, con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) siano definiti i criteri:

- con i quali i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica predisporranno e aggiorneranno con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza; è, inoltre, previsto che nei sei mesi dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al periodo precedente i soggetti obbligati comunichino tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico che li inoltreranno al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica.

A sua volta il comma 6 dello stesso art. 1, alle lett. a) e c), prevede che con regolamento da adottare entro dieci mesi siano disciplinati le procedure, le modalità e i termini:

- con cui i soggetti obbligati, che intendano procedere all'affidamento a terzi di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, ne daranno preventiva comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; entro quarantacinque giorni dalla ricezione della comunicazione, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con i soggetti di cui al comma 2, lettera a), secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento.

- con cui la Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico (rispettivamente per gli enti pubblici e per gli enti privati) eserciteranno i poteri d'ispezione e di verifica in relazione a quanto previsto dal comma 2, lett. b), dal comma 3 e dal comma 6 lett. a), ivi compresi i poteri di impartire "specifiche prescrizioni".

4. É da notare che la violazione, pur se meramente colposa, di numerosi ed ulteriori precetti extrapenali, relativi anche alle misure di sicurezza da adottare, nonché l'omessa comunicazione di dati e informazioni rilevanti ai fini dei procedimenti e delle attività ispettive e di vigilanza sopra richiamati, determina l'applicazione delle pesanti sanzioni amministrative previste dal comma 9 dell'art. 1 citato, che sono non solo di natura pecuniaria (varianti fra minimi da 200.000 a 300.000 Euro e massimi da 1.200.000 e 1.800.000 Euro), ma anche di natura interdittiva. L'elemento distintivo di tali illeciti amministrativi punitivi rispetto alle fattispecie penali è dato in particolare dallo scopo specifico di ostacolare o condizionare le attività della autorità ed enti preposti, mentre la clausola "*Salvo che il fatto costituisca reato*" che precede la lista degli illeciti amministrativi dovrebbe far escludere la possibilità di applicazione di entrambe le tipologie di sanzioni.

5. Infine va evidenziato che il comma 11-bis dell'art. 1 in esame, aggiunto in sede di conversione del d. l. n. 105/2019, inserisce le nuove fattispecie delittuose nel catalogo dei reati presupposto, la cui commissione comporta la responsabilità amministrativa da reato dell'Ente, ai sensi del d.lgs. n. 231/2001, con modifica del comma 3 del suo art. 24-bis, riguardante i "delitti informatici", per cui è prevista la sanzione pecuniaria fino a quattrocento quote, oltre alle sanzioni interdittive stabilite dalle lett. c), d) ed e) del comma 2 dell'art. 9.

La legge di conversione ha superato l'anomalia che emergeva dal testo del d.l. n. 105/2019, in cui la responsabilità amministrativa degli enti per gli esaminati delitti era autonomamente prevista, ma senza inclusione espressa nel corpo del d.lgs. n. 231/2001.

6. In sintesi, il provvedimento si inserisce in un quadro strategico non solo europeo, che mira a rafforzare la tutela della cybersecurity. Al riguardo va menzionata la Direttiva 2016/1148/Ue del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, ed il Regolamento di esecuzione 2018/151/Ue della Commissione, del 30 gennaio 2018, recante modalità di applicazione della predetta Direttiva, che fornisce anche la specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi, nonché dei parametri per determinare l'eventuale impatto rilevante di un incidente.
Di fronte alle più recenti tecnologie, comprese le applicazioni della rete 5 G, il legislatore estende ora ad un ampio numero di "operatori" un complesso insieme di obblighi, in un contesto di

"certificazione" della cybersecurity, con penetranti poteri preventivi, prescrittivi e sanzionatori delle Autorità governative.
Per ogni riferimento anche alle varie fonti menzionate, cfr. R. Flor, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo: dalla* CIA-Triad Protection *ai più recenti sviluppi*, in *Diritto di Internet*, 2019, n. 3, p. 443 s.

(Lorenzo Picotti e Rosa Maria Vadalà)

Link alla Gazzetta Ufficiale: https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg