La legge sulla sicurezza cibernetica agisce direttamente sul catalogo 231

La legge di conversione del DL 105/2019 ha opportunamente ricondotto gli illeciti penali previsti all'art. 24-bis comma 3 del DLgs. 231/2001

/ Stefano COMELLINI

La legge 18 novembre 2019 n. 133, in vigore dal 21 novembre scorso, ha convertito in legge con modificazioni il DL 105/2019, recante un complesso di disposizioni urgenti tese ad assicurare un livello elevato di **sicurezza delle reti**, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un "perimetro di sicurezza nazionale cibernetica" e la previsione di misure volte a garantire i necessari e specifici standard di sicurezza.

La *ratio* del provvedimento è nella necessità e urgenza di predisporre adeguate misure di sicurezza a fronte della realizzazione, in Italia al pari di altri stati europei, di complessi impianti tecnologici e di telecomunicazione con **infrastrutture** diffuse sul territorio. Di qui, l'esigenza di individuare organi, procedure e sicurezze, anche con riferimento alla nuova tecnologia 5G, sia sotto il profilo dell'analisi del rischio che della capacità di impedire l'interruzione delle comunicazioni.

All'art. 1 si individua il "**perimetro** di sicurezza nazionale cibernetica", riferendolo, in maniera analitica, alle reti, ai sistemi informativi e ai 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 e interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

L'inclusione nel perimetro di tali soggetti, pubblici o privati, verrà determinata con decreto del Presidente del Consiglio, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR). I soggetti così individuati avranno l'obbligo di osservare le prescritte misure di sicurezza e di redigere, con cadenza almeno annuale, l'**elenco delle reti**, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, a rischio vulnerabilità, con una completa mappatura dei rischi del sistema nazionale di connettività. Le conseguenze di tale onere possono prevedersi assai gravose per le amministrazioni pubbliche, dotate spesso di strumenti e sistemi informatici obsoleti.

Con altro regolamento dovranno essere definite le modalità attraverso le quali notificare alle autorità competenti gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici.

Nell'ambito della complessiva ricerca di sicurezza, è anche prevista l'**elaborazione** di schemi di certificazione cibernetica, avuto riguardo agli standard definiti a livello internazionale, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

Sempre ad un regolamento da emanarsi con DPCM è demandata la definizione delle **procedure**, delle modalità e dei termini ai quali devono attenersi i soggetti, pubblici e privati, 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 a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'elenco sopra indicato.

Sono poi previste disposizioni dettate per assicurare il raccordo tra questo provvedimento e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione **a banda larga** basati sulla tecnologia 5G (art. 3), nonché (art. 4-*bis*) di modifica del DL 21/2012 in tema di poteri speciali del Governo sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (c.d. golden power).

Infine, è previsto un articolato sistema **sanzionatorio** che contempla illeciti amministrativi e penali; questi ultimi (art. 1 comma 11) integrati dal fornire informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici impiegati, o ai fini delle comunicazioni preventive al Centro di valutazione e certificazione nazionale, o per lo svolgimento di specifiche attività ispettive e di vigilanza; ovvero dall'omettere di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto. Il tutto allo scopo di ostacolare o condizionare – secondo lo schema penalistico del dolo specifico – l'espletamento dei procedimenti, descritti nello stesso art. 1, per i quali è imposto l'obbligo di verità.

Si tratta di illeciti penali che costituiscono presupposto della responsabilità amministrativa degli enti, opportunamente ricondotti, in sede di conversione del decreto, all'interno del DLgs. n. 231/2001, all'art. 24-*bis*.

EUTEKNE - RIPRODUZIONE VIETATA - COPIA RISERVATA A STEFANO COMELLINI