Cybersicurezza: nuova fase con qualche interrogativo

di Renato Caputo

Il Governo ha approvato il Decreto-Aiuti bis e dal testo emergono alcune importanti novità in materia di intelligence. Ad esempio, l'art. 37, dal titolo piuttosto eloquente, "Disposizioni in materia di intelligence in ambito cibernetico", nel modificare la Legge 11 dicembre 2015, n. 198[1], prevede l'introduzione di un articolo specifico[2] che amplierà le "Misure di intelligence di contrasto in ambito cibernetico". Con questa modifica l'Italia passa al contrattacco in ambito cyber.

Gli attacchi cyber russi contro l'Italia

Come denunciato dall'Agenzia per la Cybersicurezza Nazionale (ACN), che si occupa di resilienza cibernetica, il nostro Paese, già da metà gennaio, è entrata nel mirino di una campagna di aggressione cyber da parte di attori russi. Questa serie di attacchi, tutt'ora in corso, si sono peraltro intensificati con l'invasione russa dell'Ucraina e la ferma presa di posizione da parte del Governo italiano che ha condannato la condotta di Mosca.

Le Offensive Cyber Capabilities (OCC)

Partendo dal presupposto che spetti all'intelligence nazionale il compito di neutralizzare, con un'operazione cyber anche preventiva, una possibile minaccia

[1] Legge di conversione, con modificazioni, del decreto-legge 30 ottobre 2015, n. 174, inerente la "Proroga dellemissioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione".

[2] Art. 7-ter.

esterna, l'innovazione normativa apportata con l'approvazione del Decreto-Aiuti bis, introduce due significative novità: la possibilità di avvalersi della cooperazione del Ministero della difesa e di applicare le cosiddette "garanzie funzionali"[3].

Con "garanzie funzionali" si intende la non punibilità del personale dei servizi di informazione per la sicurezza che ponga in essere condotte previste dalla legge come reato, laddove legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi, ed a condizione che ciò avvenga nel rispetto rigoroso dei limiti e delle procedure fissate dalla Legge 124/2007.

Il delicato processo di autorizzazione

Il Presidente del Consiglio dei ministri, acquisito il parere del Comitato parlamentare per la sicurezza della Repubblica, emanerà "disposizioni per l'adozione di misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgano aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale"[4].

Le disposizioni introdotte disciplineranno il procedimento di autorizzazione, le caratteristiche ed i contenuti generali delle misure che potranno essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità.

L'autorizzazione verrà disposta sulla base di una valutazione volta ad escludere, alla luce delle più aggiornate cognizioni informatiche e fatti salvi i fattori imprevisti e imprevedibili, la commissione di delitti diretti a mettere in pericolo o

[3] Articolo 17 della legge 3 agosto 2007, n. 124.

[4] Il Presidente del Consiglio dei ministri provvede al coordinamento delle politiche dell'informazione per la sicurezza, impartisce le direttive e, sentito il Comitato interministeriale per la sicurezza della Repubblica, emana ogni disposizione necessaria per l'organizzazione e il funzionamento del Sistema di informazione per la sicurezza dellaRepubblica (articolo 1, comma 3, della legge 3 agosto 2007, n. 124).

a ledere la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone[5].

I soggetti operativi: Aise e Aisi

Le misure di contrasto in ambito cibernetico autorizzate, verranno attuate dall'Agenzia Informazioni e Sicurezza Esterna (AISE) e dall'Agenzia Informazioni e Sicurezza Interna (AISI), sotto il coordinamento del Dipartimento delle Informazioni per la Sicurezza (DIS)[6]. Il Presidente del Consiglio dei ministri informerà, entro trenta giorni dalla data di conclusione delle operazioni, il Comitato parlamentare per la sicurezza della Repubblica, così come previsto dall'articolo 33, comma 4, della legge n. 124 del 2007. Al personale delle Forze armate impiegato nell'attuazione delle attività di Cyber Attacco contro minacce esterne si applicheranno le "cause esimenti"[7] previste dall'articolo 19 della legge 21 luglio 2016, n. 145.

Altra importante innovazione, riguarda anche soggetti non organici alle Agenzie ed alle Forze Armate. Nel caso in cui, ricorrendone i presupposti per particolari condizioni di fatto e per eccezionali necessità, le attività siano state svolte da persone non addette ai servizi di informazione per la sicurezza, in concorso con uno o più dipendenti dei servizi di informazione per la sicurezza, e risulti che il ricorso alla loro opera da parte dei servizi di informazione per la sicurezza era indispensabile ed era stato autorizzato secondo le procedure fissate dalla normativa vigente, tali persone sono equiparate, ai fini dell'applicazione della speciale causa di giustificazione, al personale dei servizi di informazione per la sicurezza[8].

Controllo parlamentare sulle operazioni Cyber

[5] Articolo 17, comma 2, della legge 3 agosto 2007, n. 124.
[6] Articolo 4, comma 3, lettera d-bis), della legge n. 124 del 2007.

[7] Le "circostanze che escludono la pena" o "esimenti". Scriminanti o cause di giustificazione sono quelle circostanze che escludono la pena pur in presenza di un fatto di reato che, in teoria, sarebbe punibile. "Non è punibile il personale che, nel corso delle missioni internazionali, in conformità alle direttive, alle regole di ingaggio ovvero agli ordini legittimamente impartiti, fa uso ovvero ordina di fare uso delle armi, della forza o di altro mezzo di coazione fisica, per le necessità delle operazioni militari".

[8] Articolo 17, comma 7, della legge n. 124 del 2007.

Il Comitato parlamentare per la sicurezza della Repubblica trascorsi ventiquattro mesi dalla data di entrata in vigore della modifica in materia di "Misure di intelligence di contrasto in ambito cibernetico", trasmetterà alle Camere una relazione sull'efficacia delle nuove disposizioni di legge adottate in materia.