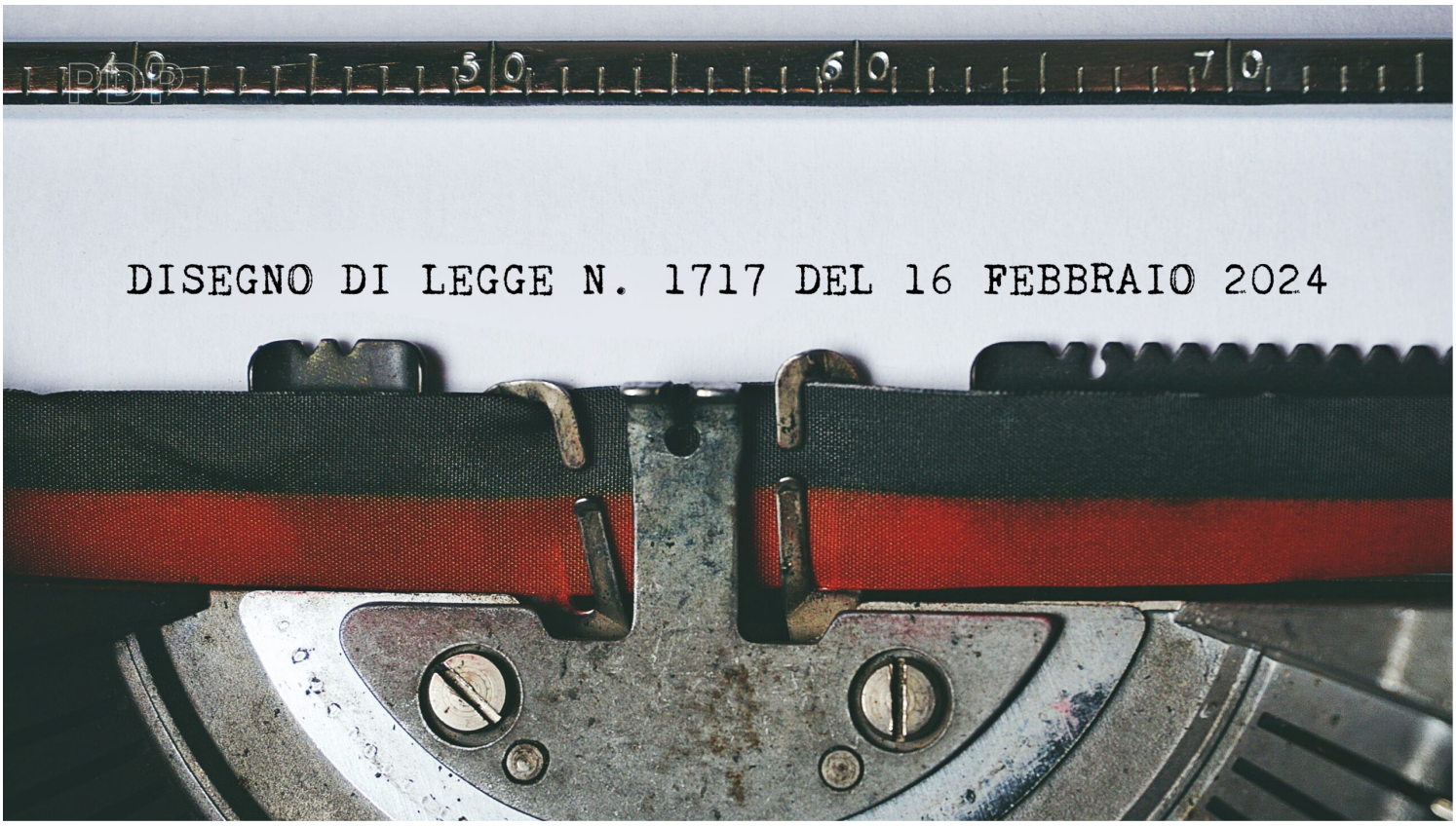
COMMENTO AL DISEGNO DI LEGGE DEL GOVERNO N. 1717 PRESENTATO ALLA CAMERA IL 16 FEBBRAIO 2024

Stefano Aterno



Il 25 gennaio 2023 il Governo italiano ha approvato il disegno di legge con lo scopo di potenziare la lotta e il contrasto agli attacchi informatici verso le infrastrutture critiche e migliorare la cybersicurezza nazionale. Il disegno di legge è stato assegnato alle Camere e incardinato il 16 febbraio 2024.

Dalla lettura del testo approvato dall'esecutivo emerge molto chiaramente la volontà del Governo di rafforzare ulteriormente il livello della cybersicurezza nazionale, della resilienza delle pubbliche amministrazioni, di potenziare il funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché di aumentare notevolmente le pene minime e massime. Novità importante è anche l'intenzione di modificare la

normativa sui contratti pubblici di beni e servizi informatici (impiegati in un contesto connesso alla tutela degli interessi nazionali strategici) al fine di tenere maggiormente in considerazione gli elementi essenziali di cybersicurezza nella valutazione dell'elemento qualitativo e ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione.

Il decreto prevede anche un forte inasprimento delle pene per i reati informatici e un coordinamento tra ACN e Direzione Nazionale Antimafia in caso di attacchi a sistemi informatici e telematici connessi alle infrastrutture critiche.

Giunto alle Camere ha avuto già preliminarmente alcuni ritocchi ma permangono alcune criticità.

Cercheremo di analizzare per punti tutti i passaggi più importanti del decreto partendo proprio dalle modifiche al codice penale in materia di reati informatici e al coordinamento tra l'Agenzia di Cybersicurezza e la DNA.

Il decreto si muove su più direzioni.

Inasprimento delle pene edittali minime e massime dei reati informatici

Il provvedimento normativo reca alcune disposizioni per la prevenzione e il contrasto dei reati informatici, nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici. Si tratta in tutti i casi di inasprimento delle pene edittali nel minimo e nel massimo. Le condotte, salvo quanto si dirà più avanti non subiscono modifiche.

Si interviene, innanzitutto, sul delitto di accesso abusivo ad un sistema informatico, di cui all'articolo 615-ter del codice (comma 1, lettera a)) aumenta la pena edittale per le ipotesi aggravate del reato, precedentemente fissata nella reclusione da uno a cinque anni, ora fissata «da due a dieci anni»; un'altra modifica che mira ad un inasprimento della pena riguarda l'ipotesi aggravata di esecuzione del reato con l'uso della minaccia oltre che con violenza sulle cose o alle persone; si aggiunge inoltre un'aggravante tipica dei casi di attacchi Ransomware ovvero relativa alle condotte di chi sottrae, anche mediante riproduzione o trasmissione, ovvero renda inaccessibili al titolare, i dati, le informazioni o i programmi contenuti nel sistema informatico o telematico.

In un'ipotesi in sui l'intento del Legislatore è quello di tutelare maggiormente le infrastrutture critiche del sistema paese un'altra modifica viene apportata al comma terzo dell'articolo 615-ter c.p., riguardante i casi in cui i fatti di cui ai precedenti commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. In tali casi infatti la pena edittale è aumentata «da tre a dieci anni e da quattro a dodici anni di reclusione» (oggi è punita con una pena che va «da uno a cinque anni e da tre a otto anni di reclusione») alla reclusione.

Se gli attacchi informatici alle aziende e alle pubbliche amministrazioni strategiche per il funzionamento del sistema paese possono essere una giustificazione per tale inasprimento è di tutta evidenza che qui il Legislatore ha dimenticato una clausola di riserva che preveda un doppio binario sanzionatorio per i casi più lievi ovvero i casi nei quali l'accesso abusivo alla Banca Dati pubblica e strategica venga posta in essere non da gruppi hacker al soldo di Stati sovrani o gruppi criminali ma dal *quisque de populo*, spesso neanche per motivi di corruzione bensì di mera curiosità verso un personaggio pubblico, un fatto pubblico, di necessità di verificare un'informazione per gelosia nei confronti di un familiare o di altri casi simili davvero non così gravi da giustificare pene edittali da quattro a dodici anni di reclusione. Sarebbe sufficiente prevedere ad esempio che *"nei casi di minore gravità il giudice possa prevedere diminuzione della pena da X a Y ".* Questa questione dell'inasprimento delle pene che come vedremo colpisce anche altri reati appare ancor più seria se si considera che la norma aggiunge anche un periodo al terzo comma nel quale si prevede che nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89 («Vizio parziale di mente»), 98 («Minore degli anni diciotto») e 623-quater (introdotto dal presente provvedimento, di seguito esaminato), tali circostanze non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti. E' di tutta evidenza che bisogna trovare una soluzione per le ipotesi meno gravi e consentire al giudice di poter valutare meglio, senza essere costretto da pene edittali troppo severe, un miglior contemperamento ed una migliore dosimetria della pena al fatto concreto. Spesso sono proprio infatti meno lievi, quelli che investono dipendenti pubblici che accedono abusivamente alle banche dati quelli che finiscono davanti ai giudici mentre davvero molto pochi i processi ai membri dei gruppi hacker internazionali. Certamente anche le norme entrate in vigore ad ottobre e che potenziano la lotta al cybercrime attraverso la figura dell'infiltrato contribuiranno ad un miglioramento di un certo tipo di indagini e quindi si potrà giustificare un trattamento sanzionatorio così severo per attacchi informatici molto pericolosi e devastanti sotto molti profili. Prevedere però oggi una clausola di salvaguardia per casi di minore gravità è comunque anche un'opera di buon senso.

Oltre all'accesso abusivo viene modificato anche l'articolo 615-quater c.p. ovvero il delitto di «Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici» per potenziare la lotta alla proliferazione dei virus e dei malware. Qui si amplia (dal «profitto» al più generico «vantaggio») il dolo specifico previsto per la configurabilità della fattispecie e anche in questo caso le pene edittali vengono aumentate soprattutto quando la diffusione dei virus o dei ransomware riguarda i sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. In questi casi la pena sale da un minimo di tre ad un massimo di otto anni. Anche in questo caso manca una clausola sui casi di minore gravità e ci si augura che nel dolo specifico del "vantaggio" non ci finiscano anche le aziende piccole o grandi di sicurezza informatiche che studiano per ricerca e per motivi di prevenzione il fenomeno dei virus e dei malware.

Altri inasprimenti di pene riguardano l'articolo 617-quinquies recante «Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche» e l'articolo 617-sexies, recante la fattispecie di reato «Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche».
Nel passaggio del testo alle camere il Governo evidentemente si accorge della dimenticanza e inserisce una norma di minore tenuità del fatto.

Infatti, la lettera h) del Disegno di legge modifica la rubrica del Capo III-bis del Titolo XII, precedentemente rubricato «Disposizioni comuni sulla procedibilità», eliminando il riferimento alla procedibilità in considerazione delle modifiche di cui alla successiva lettera i), che introduce l'articolo 623-quater relativo a due circostanze attenuanti. Si prevede, in particolare, che le pene comminate per i delitti di cui agli articoli 615-ter, 615-quater, 617-quater, 617-quinquies e 617-sexies sono diminuite quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità (comma 1). Ma non è evidentemente sufficiente essendo del tutto, e forse anche troppo, discrezionale, scrivere "sono diminuite" invece di fornire al giudice una maggiore indicazione circa il criterio di diminuzione. Cosa che invece il legislatore dimostra di saper fare poco dopo quando introduce la figura del "ravvedimento o del pentimento dell'hacker" (si veda la modifica dell'articolo 13 del disegno di legge, in particolare, modifica l'articolo 9, comma 2, del decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82), ovvero quando prevede, oltre alle misure di protezione che le pene previste per i suddetti delitti sono invece diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o

degli strumenti utilizzati per la commissione degli stessi (comma 2). Sarà necessario un ulteriore ritocco più preciso e completo.
Inoltre, nella prospettiva del potenziamento degli strumenti investigativi, l'articolo 14 modifica l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, inserendo un comma 3-bis che estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi dall'articolo 371-bis al coordinamento del procuratore nazionale antimafia e antiterrorismo.

La disciplina prevede che le intercettazioni possano essere autorizzate dal giudice per le indagini preliminari sulla base di sufficienti indizi di reato, quando necessarie per la prosecuzione delle indagini, per un termine di quaranta giorni, suscettibile di proroga per ulteriori periodi di venti giorni.

Il coordinamento tra ACN e Magistratura in caso di attacchi informatici

E', come tutte le norme sul coordinamento tra diversi organi dello Stato, una norma molto importante. La disciplina introduce reciproci obblighi informativi tra l'ACN e l'autorità giudiziaria, funzionali ad assicurare l'efficace e tempestivo svolgimento delle attività di ripristino, l'assicurazione delle fonti di prova e il coordinamento del procuratore nazionale antimafia e antiterrorismo per i reati indicati nel novellato articolo 371-bis, comma 4-bis, del codice di procedura penale.

In particolare, l'Agenzia deve informare senza ritardo il procuratore nazionale antimafia e antiterrorismo della notizia di un attacco qualificato (come da definizione che viene data nel comma 4-bis.1 dell'articolo 17), corrispondentemente il pubblico ministero dà tempestiva informazione all'ACN della notizia dei delitti di cui all'articolo 371-bis, comma 4-bis, del codice di procedura penale. Sul punto vale la pena di riflettere se tale tempestiva informazione all'ACN sia per la magistratura un obbligo o una facoltà ma soprattutto il significato di tempestiva. E' di tutta evidenza che l'autorità giudiziaria in relazione a casi specifici potrebbe sostenere motivi di segretezza delle indagini in corso (persone coinvolte) che potrebbero rendere inopportuna tale comunicazione all'ACN.

Viene, infine, introdotta la facoltà per l'ACN, in caso di accertamenti tecnici irripetibili per i delitti di cui all'articolo 371- bis, comma 4-bis, del codice di procedura penale, di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio (comma 4-bis.4).

Coordinamento tra il DIS e l'ACN

Ulteriori e importanti norme sono poste a rafforzare il coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale). Al fine di salvaguardare il lavoro di entrambe gli organismi sono state previste all'art. 5 del disegno di legge alcune disposizioni che consentono all'una e all'altra di differire e di comunicare ai rispettivi vertici il differimento di una o più delle attività di resilienza ove lo ritengano strettamente necessario per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica.

Obblighi di notifica all'ACN

Le pubbliche amministrazioni interessate sono obbligate a segnalare e notificare gli incidenti di sicurezza che rientrano in una tassonomia tecnica indicata all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, soprattutto quando l'evento di sicurezza ha un impatto su reti, sistemi informativi e servizi informatici di pertinenza. Sono tenute alla segnalazione e alla notifica anche le società in house.
Dall'inosservanza dell'obbligo di notifica di cui al presente articolo, consegue una preliminare comunicazione dell'Agenzia per la cybersicurezza nazionale all'interessato, che la reiterazione dell'inosservanza comporterà l'applicazione delle sanzioni indicate nel successivo comma 5, e in ispezioni da parte dell'Agenzie medesima cibernetica, anche al fine di verificare l'attuazione degli interventi di rafforzamento della resilienza loro direttamente indicati dall'Agenzia, ovvero previsti da apposite linee guida adottate dalla stessa.
Nei casi di reiterata inosservanza dell'obbligo di notifica, l'Agenzia per la cybersicurezza nazionale potrà applicare una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000. La violazione di queste disposizioni può costituire causa di responsabilità disciplinare e amministrativo-contabile.

Nasce il referente per la cybersicurezza per le PA interessate dal disegno di legge

Al fine di rafforzare la resilienza delle pubbliche amministrazioni nasce la nuova figura del referente per la cybersicurezza. Le pubbliche amministrazioni individuano, ove non sia già presente, una struttura, anche tra quelle esistenti, che provvede:

a. allo sviluppo delle politiche e procedure di sicurezza delle informazioni;

b. alla produzione e all'aggiornamento di un piano per la gestione del rischio informatico;

c. alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

d. alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

e. alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici.

f. alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;

g. al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Questo referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalle normative settoriali in materia di cybersicurezza cui è soggetta la stessa amministrazione.
Questo referente per la cybersicurezza svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalle normative settoriali in materia di cybersicurezza cui è soggetta la stessa amministrazione.

L'ACN potrà usare l'AI per rafforzare la cybersicurezza nazionale

Il ruolo di Autorità nazionale per la cybersicurezza implica una grande attenzione al mondo degli attacchi informatici e al suo costante sviluppo. Già da molti mesi ormai gli attacchi informatici, soprattutto quelli di un certo rilievo vengono portati a termine avvalendosi di nuove tecnologie che si avvalgono anche dell'intelligenza artificiale e dei primi studi sulle tecniche di attacco con computer quantistici. E' di tutta evidenza che il Legislatore ha dovuto prevedere la possibilità per l'Agenzia di promuovere e sviluppare ogni iniziativa, anche di partenariato pubblico-privato, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della sicurezza e della resilienza cibernetiche nazionali, anche al fine di favorire un uso etico e corretto dei sistemi basati su tale tecnologia. E' su questo tavolo che da domani, anzi già da ieri, si sta

giocando la sfida alla vera capacità di resilienza delle infrastrutture critiche e dell'intero sistema paese. Il cyberterrorismo è come il ghiaccio sporco sulle strade per le auto, non lo vedi ma quando ci sei sopra è ormai troppo tardi.