Commissioni Affari Costituzionali e Giustizia Camera dei Deputati
Audizione del 22 marzo

Disegno di legge C. 1717 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"

Sollevano forti perplessità le soluzioni di intervento legislativo delineate nel disegno di legge C. 1717 Governo, recante "*disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".*

Più in particolare, la Direttiva NIS 2 dell'UE pubblicata sulla Gazzetta Ufficiale europea e rivolta agli Stati Membri, cui è ispirato il DDL in oggetto, nulla dice o consiglia in merito alla necessità di adeguare la legislazione interna degli Stati in ordine all'impianto repressivo penale, mediante l'introduzione di nuove fattispecie di reato e/o di aggravanti speciali con relativo meccanismo limitativo di bilanciamento tra circostanze.

La condivisibile esigenza di implementare le sovrastrutture di sicurezza a presidio dei sistemi pubblici e privati di cybernetica che ispira l'intervento riformatore, per rispondere alla crescente offensività delle aggressioni realizzate con mezzi informatici e telematici verso gli apparati statali, non richiedeva di intervenire, quantomeno non in misura prevalente, sul sistema sanzionatorio penale.

Come evidenziato nel rapporto Clusit 2024, che lamenta un incremento significativo in Italia degli "attacchi gravi globali" (11% del 2023, rispetto al 7,6% del 2022, per un totale di 310 attacchi), il nostro Paese appare sempre più nel mirino dei cyber criminali e necessità di un adeguamento delle dotazioni di sicurezza preventiva degli apparati pubblici e privati, al fine di scongiurare il rischio "collasso del sistema".

D'altra parte, il complesso articolato di norme delineato nel DDL in oggetto affida il raggiungimento dell'obiettivo "sicurezza cybernatica interna" all'irrobustimento della risposta repressiva dei fenomeni criminali, con nuovi reati ed aumento significativo delle pene, col rischio di non centrare affatto il medesimo obiettivo di scopo.

Proprio per questi reati, infatti, gli strumenti investigativi appaiono, il più delle volte, insufficienti ad identificarne gli autori, magari nascosti dietro reti VPN allocate in "Paesi ombra", con ciò rendendo inefficace, se non addirittura inutile, il deterrente della sanzione penale, rispetto a processi di difficile costruzione probatoria.

Analizzando il testo del DDL agli artt. 11, 12 e 14, si rinviene una sequenza ininterrotta di nuove ipotesi di reato ovvero di nuove circostanze aggravanti ovvero di rimodulazione consistente delle pene previste per tutte tali ipotesi, peraltro con l'implementazione del catalogo dei reati informatici suscettibili di intercettazione telematica con automatismi tutti da ben meditare.

Il dubbio circa la bontà e l'efficacia di tale intervento repressivo rispetto all'ampiezza e complessità del fenomeno criminale induce l'avvocatura penalistica a suggerire ulteriori riflessioni circa l'opportunità di concentrare gli sforzi sui processi preventivi di adeguamento dell'apparato di sicurezza, piuttosto che demandare alla deterrenza della sanzione penale tutto il compito di garantire i presidi pubblici e privati in ambito cybernetico.

L'inasprimento delle pene e la proliferazione di nuove fattispecie di reato paiono, pertanto, privi di nesso causale con l'auspicata riduzione del fenomeno criminoso che vorrebbero astrattamente contrastare.

A ben vedere, tali provvedimenti assumono un carattere meramente simbolico e hanno l'esclusiva finalità di marcare l'intervento delle istituzioni sulla problematica, pur senza incidervi efficacemente in senso riduttivo.

In altri termini, come più volte affermato dall'Unione delle Camere Penali Italiane e dalla più autorevole Accademia, va censurata ogni forma di ricorso al "diritto penale simbolico", che finisce col

nascondere la polvere sotto il tappeto, così trasmettendo, invece, la sensazione di non riuscire a fronteggiare in modo concreto e preventivo i fenomeni criminali nell'interesse della collettività.
"*E' invalsa nella collettività e nell'ambiente politico la convinzione che nel diritto penale si possa trovare il rimedio giuridico ad ogni ingiustizia e ad ogni male sociale*" ("Il diritto penale totale", Filippo Sgubbi, Il Mulino, 2020).
Senza nessuna pretesa di esaustività, si rappresentano alcune delle criticità specifiche rilevate dall'analisi del testo del DDL:
1) il meccanismo inerente il divieto di prevalenza e/o equivalenza ex art. 69 c.p. delle circostanze attenuanti sulle varie aggravanti di nuovo conio è già stato a più riprese e recentemente bocciato dalla Corte Costituzionale in diverse sentenze che hanno dichiarato l'illegittimità costituzionale di simili interventi repressivi riguardanti la parte generale del codice penale (si vedano le sentenze n. 201 del 2023, 188 del 2023, 141 del 2023, 94 del 2023, 55 del 2021 e 143 del 2021);
2) l'introduzione della facoltà per l'ACN, in caso di accertamenti tecnici irripetibili per i delitti di cui all'articolo 371-*bis*, comma 4-*bis* c.p.p. (come novellato proprio dal disegno di legge), di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio. Orbene, questa previsione desta particolare preoccupazione, in considerazione dei rapporti che sussistono fra l'ACN e i servizi di intelligence. Non si può difatti non ricordare che, oltre all'alta direzione e alla responsabilità generale delle politiche di cybersicurezza, al Presidente del Consiglio dei Ministri è attribuito il compito di nominare e revocare i vertici dell'ACN; in questa sede, non si può tacere il fatto che tali nomine vengono fatte previa informativa al COPASIR e che vi sono stretti rapporti fra l'ACN e le Agenzie di informazione e sicurezza interna e esterna (rispettivamente, AISI e AISE). Ne discende che, qualora il provvedimento venisse approvato nella sua attuale formulazione, verrebbe introdotta nell'ordinamento italiano una previsione del tutto singolare, che consentirebbe all'ACN di acquisire e trasmettere informazioni presidiate da garanzie funzionali all'esercizio dei diritti dei soggetti del procedimento penale, in primis del diritto di difesa dell'indagato;
3) l'art. 14 del DDL amplia l'applicazione della disciplina delle intercettazioni in caso di criminalità organizzata (derogatoria ai presupposti stringenti previsti per le intercettazioni ordinarie) ai reati informatici rimessi al coordinamento del Procuratore nazionale antimafia e antiterrorismo.
Il D.L 152/1991, oggetto di recente (e criticata) modifica con DL 105/2023, è ispirato all'idea che nel bilanciamento tra la tutela della riservatezza dei cittadini e la tutela dell'ordine pubblico, prevalga sempre la seconda. Solleviamo forti perplessità in merito, come già evidenziato dall'On. Costa nell'intervento dello scorso 19 marzo. Vero è, come ribadito dal sottosegretario Mantovano in quella riunione, che reati che presuppongono elevata capacità informatica richiedono strumenti informatici altrettanto sofisticati, ma occorre riflettere accuratamente prima di rinunciare, in nome della sicurezza, a fette sempre più ampie del diritto alla riservatezza dei cittadini, soprattutto in un contesto in rapidissima evoluzione come quello informatico. Riflessione strettamente collegata a quella più ampia sull'opportunità stessa del mantenimento di un c.d. doppio binario per i reati di criminalità organizzata (che oggi vorrebbe estendersi ai reati informatici), sintomo di una deriva autoritaria del processo, come già denunciato dalla Giunta dell'Unione Camere Penali (v. *Doppio binario: una deriva autoritaria del processo su cui iniziare una seria riflessione*, Documento della Giunta dell'Unione delle Camere Penali Italiane 28.10.2008).

La Giunta
L'Osservatorio Scienza Processo e Intelligenza Artificiale