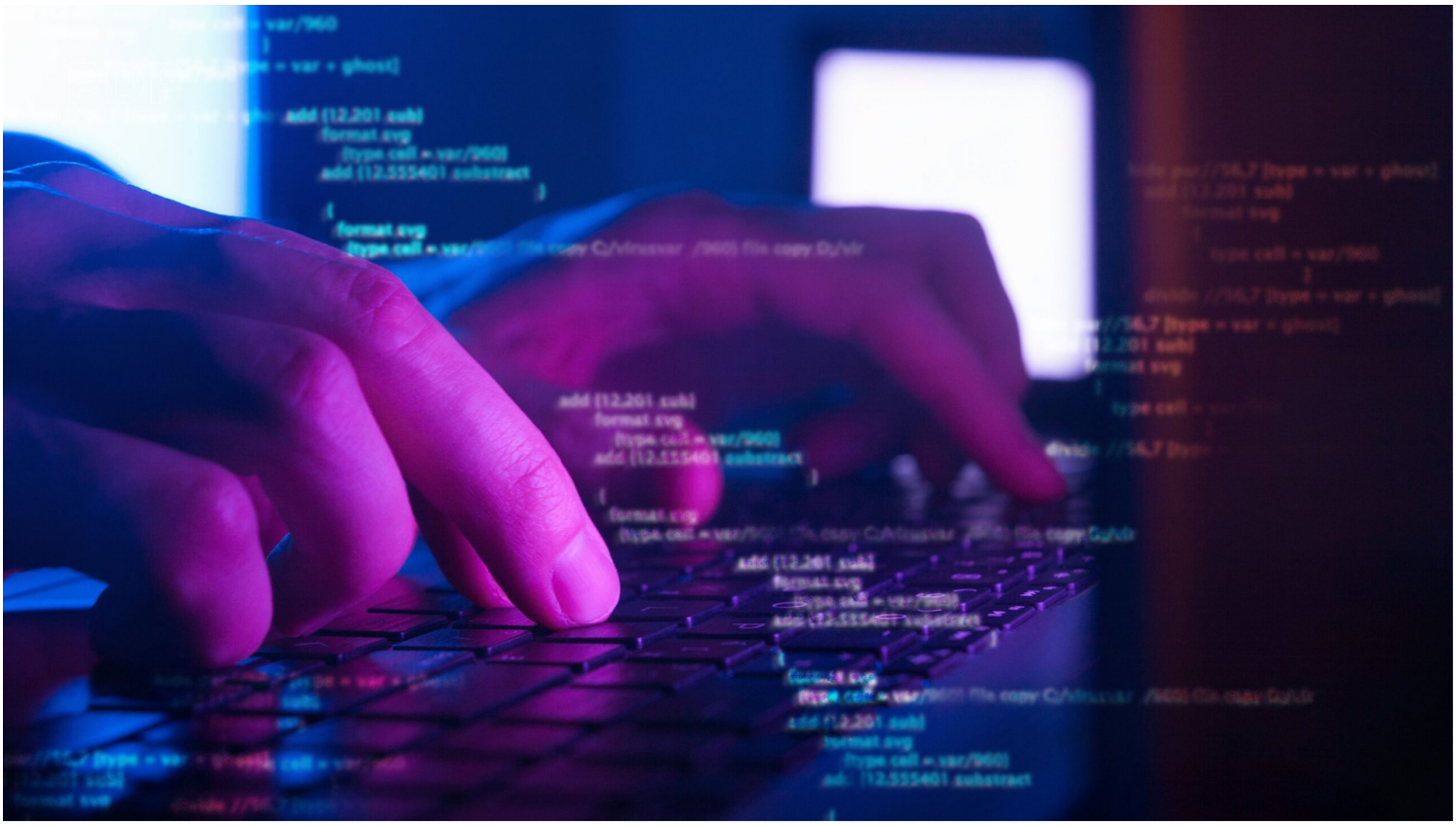
LE NUOVE NORME DI PREVENZIONE E CONTRASTO ALLA CRIMINALITÀ INFORMATICA

Wanda Nocerino



1. Uno sguardo d'insieme

Tra le disposizioni urgenti in materia di processo penale introdotte dal d.l. n. 105/2023, convertito con modificazioni dalla l. n. 137/2023, figura l'art. 2 *bis* – del tutto assente nel testo originario ed introdotto in sede referente –che si prefigge l'obiettivo di innalzare i livelli di cybersicurezza e di implementare gli strumenti di repressione dei crimini informatici.

In particolare, i commi 1 e 2 contengono disposizioni normative volte ad incrementare le capacità nazionali

di prevenzione e di gestione degli incidenti e degli attacchi informatici attraverso l'ampliamento delle funzioni dell'Agenzia per la Cybersicurezza Nazionale; i commi 3, 5 e 6, recano previsioni atte ad estendere i poteri e le prerogative del Procuratore Nazionale Antimafia e Antiterrorismo anche ai procedimenti inerenti a taluni gravi delitti di criminalità informatica; il comma 4, infine, contiene disposizioni volte ad espandere l'area operativa delle operazioni *under cover* (con annesse prerogative) anche per il contrasto del *cybercrime*.

Se non si profilano particolari criticità in rapporto alla scelta di implementare i poteri di impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo, sorprende la *voluntas legis* di favorire la circolazione informativa tra organi che sono – o, almeno, dovrebbero essere – estranei alle logiche investigative, acuendo così il rischio di riversare nel processo dati e informazioni raccolti in fase preventiva e, dunque, in un segmento pre-procedimentale svincolato dalle regole che connotano il rito penale.

2. I nuovi compiti dell'Agenzia per la Cybersicurezza Nazionale

Nell'ambito delle norme volte ad ampliare i compiti dell'Agenzia per la Cybersicurezza Nazionale[1], figurano alcune previsioni integrative di inediti meccanismi collaborativi a carico dell'ente.

In primis, il comma 1 dell'art. 2-*bis*, d.l. n. 105/2023, attraverso l'integrazione di un nuovo comma 4-*bis* all'art. 17, d.l. n. 82/2021, prevede che l'Agenzia è tenuta a trasmettere al Procuratore Nazionale Antimafia e Antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni e dei poteri di impulso e coordinamento delle indagini relative a gravi reati informatici, di cui all'art. 371 *bis* c.p.p., come modificato dalla riforma in oggetto.

In secundis, il comma 2 dell'art. 2 *bis*, d.l. n. 105/2023 – integrando l'elenco delle funzioni attribuite all'Agenzia dall'art. 7, d.l. n. 82/2021, con particolare riferimento a quanto stabilito dalla lettera *n* del comma 1[2] –, prevede un dovere di assistenza ai soggetti pubblici e privati che hanno subìto incidenti di sicurezza informatica o attacchi informatici (nuova lettera *n-bis* del comma 1 dell'art. 7, d.l. n. 82/2021).

La norma in parola introduce anche un catalogo di sanzioni da comminare nel caso di mancata collaborazione, mutuandole da quelle già sperimentate dall'art. 1, commi 10 e 14, d.l. n. 105/2019, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica",* ovvero la sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo

nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione e, in caso di dipendenti pubblici, la responsabilità disciplinare e amministrativo-contabile.

Tali sanzioni posso essere applicate solo ai soggetti specificamente indicati nella disposizione per il tramite di rinvii normativi, ossia: a) alle amministrazioni pubbliche, enti e operatori pubblici e privati aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dall'art. 1, comma 2, del c.d. decreto-legge perimetro (ossia i soggetti di cui all'art. 1, comma 2-*bis*, del medesimo decreto); 2) gli operatori di servizi essenziali, pubblici o privati, e i fornitori di servizio digitale, ai sensi dell'art. 3, comma 1, lettere *g* e *i*, d.lgs. n. 65/2018, di attuazione della direttiva dell'Unione europea "NIS"; 3) le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (ossia i soggetti di cui di cui all'art. 40, comma 3, Codice delle comunicazioni elettroniche).

Tuttavia, nell'ottica di mantenere ben saldi i principi che impongono una separazione dei ruoli e delle funzioni, il dovere di collaborazione e le annesse sanzioni, per espressa previsione normativa, non possono investire gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli artt. 4, 6 e 7, l. n. 124/2007 (Dipartimento delle informazioni per la sicurezza – DIS, Agenzia informazioni e sicurezza esterna – AISE, e Agenzia informazione e sicurezza interna – AISI).

3. L'estensione dei poteri di impulso e controllo del Procuratore Nazionale Antimafia e Antiterrorismo

Con riferimento al complesso normativo atto a rafforzare gli strumenti di contrasto alla criminalità organizzata in campo informatico, i commi 3, 5 e 6 dell'art. 2 *bis,* d.l. 105/2023, ampliano le funzioni e i poteri del Procuratore Nazionale Antimafia e Antiterrorismo, tradizionalmente riconosciuti allo stesso in rapporto ai delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.

Le modifiche in parola ruotano intorno alla scelta di introdurre un inedito comma 4 *bis* all'art. 371 *bis* c.p.p., con il quale vengono estesi i poteri di impulso e coordinamento del Procuratore Nazionale Antimafia e Antiterrorismo – compreso quello di avocazione delle indagini – anche con riferimento ai più gravi reati informatici[3], con la specificazione per cui, nel caso di procedimenti aventi ad oggetto i delitti di cui agli artt. 617 *quater*, 617 *quinquies* e 617 *sexies* c.p., "le funzioni del procuratore sono riconosciute limitatamente ai

fatti commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità" (art. 2 *bis,* comma 3, lett. *b,* d.l. 105/2023).

Tale innesto è prodromico ad altre modifiche di assestamento.

Intanto, la novella innova il comma 1 dell'art. 54 *ter* c.p.p., in rapporto ai poteri riconosciuti al Procuratore Nazionale Antimafia e Antiterrorismo in caso di contrasto tra gli Uffici dei pubblici ministeri aventi ad oggetto indagini relative ai reati di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p. Secondo la neo-introdotta previsione normativa, tali prerogative devono essere estese anche con riguardo ai gravi reati informatici, di cui all'art. 371 *bis,* comma 4 *bis,* c.p.p.[4] (art. 2 *bis,* comma 3, lett. *a,* d.l. 105/2023).

Inoltre, il decreto interviene sugli artt. 724 e 727 c.p.p., in materia, rispettivamente, di obbligo di trasmissione delle richieste di rogatoria provenienti dall'estero e delle richieste indirizzate all'estero, con lo scopo di ampliare gli obblighi di trasmissione al Procuratore Nazionale Antimafia e Antiterrorismo degli atti di cooperazione giudiziaria internazionale anche con riferimento ai delitti informaticiindicati nel comma 4 *bis* dell'art. 371 *bis* c.p.p. (art. 2 *bis,* comma 3, lett. *c* e *d,* d.l. 105/2023).

Infine, i commi 5 e 6 della disposizione in parola prevedono, da un lato, il dovere di trasmissione al Procuratore Nazionale Antimafia e Antiterrorismo della copia della richiesta di riconoscimento ed esecuzione di provvedimenti di blocco o di sequestro di beni proveniente da altro Stato dell'Unione europea (modifica dell'art. 5, comma 3, d.lgs. n. 25/2016); dall'altro, che il Procuratore Nazionale sia informato della ricezione di un ordine europeo di indagine penale, ai fini del coordinamento investigativo, anche con riguardo ai reati di cui al comma 4 *bis* dell'art. 371 *bis* c.p.p. (modifica del comma 1 dell'art. 4, d.lgs. n. 108/2017).

4. Le operazioni *under cover* per il contrasto ai reati informatici

Nell'ottica di favorire il ricorso alle operazioni sotto copertura ritenute particolarmente utili al contrasto del *cybercrime*[5], il comma 4 dell'art. 2 *bis,* d.l. 105/2023, interviene sull'art. 9, l. n. 146/2006, con cui sono stati ratificati la Convenzione e i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale (c.d. Convenzione di Palermo).

Intanto, la novella interviene sul comma 1, lett. *a,* dell'art. 9 della Convenzione, con lo scopo di estendere la

clausola di non punibilità prevista per gli ufficiali di p.g. anche alle ipotesi di "pirateria informatica"[6] (art. 2 *bis,* comma 4, lett. *a,* punto 1, d.l. 105/2023).

Poi, attraverso l'interpolazione di un'inedita lett. *b ter* al comma 1 dell'art. 9 della Convenzione, si prevede che sono autorizzati a compiere operazioni sotto copertura – con conseguente estensione dell'operatività della relativa esimente – anche gli ufficiali di p.g. dell'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione che si occupano di contrastare i reati informatici commessi ai danni delle infrastrutture critiche informatizzate[7] (art. 2 *bis,* comma 4, lett. *a,* punto 2*,* d.l. 105/2023).

Infine, la novella – attraverso due interpolazioni che, invero, appaiono alquanto ridondanti – interviene per implementare i doveri comunicativi nei confronti del Procuratore Nazionale Antimafia e Antiterrorismo nel caso in cui vengano disposte operazioni sotto copertura in materia di *cybercrime.* Da un lato, qualora siano disposte operazioni sotto copertura relative ai reati di cui agli articoli 51, commi 3 *bis* e 3 *quater*, c.p.p. e al comma 4 *bis* dell'art. 371 *bis* c.p.p., l'organo responsabile è tenuto a fornire immediata comunicazione alProcuratore Nazionale Antimafia e Antiterrorismo (art. 2 *bis,* comma 4, lett. *a,* punto 2*,* d.l. 105/2023); dall'altro, viene introdotto l'obbligo per il p.m. responsabile delle indagini di comunicare al Procuratore Nazionale ogni provvedimento adottato nell'ambito delle operazioni sotto copertura quando queste riguardino i reati di cui al comma 4 *bis* dell'art. 371 *bis* c.p.p. (art. 2 *bis,* comma 4, lett. *b* e *c,* .l. 105/2023).

5. Qualche riflessione conclusiva

Alla luce del quadro normativo tratteggiato, si possono trarre alcune considerazioni di sistema.

Intanto, è sicuramente pregevole l'avvedutezza del legislatore nell'introdurre apposite previsioni in materia di *cybersecurity* e *cybercrime:* a fronte di un quadro-geopolitico globale che ha accresciuto l'esposizione della Repubblica al pericolo di attacchi informatici alle infrastrutture critiche ed ai servizi essenziali del Paese e della rinnovata fisionomia delle fattispecie criminali, sempre più proiettate alla dimensione cybernetica e transnazionale, si sente forte l'esigenza di intervenire per fornire adeguate risposte per prevenire e contrastare i più gravi reati di criminalità informatica.

Altrettanto pregevole è la scelta di implementare le funzioni del Procuratore Nazionale Antimafia e Antiterrorismo, in ragione della necessità di favorire il coordinamento investigativo anche con riguardo alla

cybersecurity e al *cybercrime* che rappresentano le "nuove emergenze" da contenere.

Tuttavia, nel tipizzare un sistema tutto improntato all'estensione del "doppio binario" anche con riguardo ai gravi reati informatici, il legislatore sembra trascurare i rischi derivanti dalla cooperazione informativo/investigativa tra organi che detengono ruoli e svolgono funzioni diversi.

Ci si riferisce, in particolare, alla scelta di favorire lo scambio informativo tra l'Agenzia per la Cybersicurezza Nazionale e il Procuratore Nazionale Antimafia e Antiterrorismo con lo scopo di facilitare il coordinamento delle indagini relative a reati di cui al comma 4 *bis* dell'art. 371 *bis* c.p.p.

Se è vero che l'Agenzia gode di un complesso di poteri autoritativi di natura amministrativa, funzionali alla sorveglianza e al controllo sul rispetto degli obblighi previsti a carico degli enti inseriti nel perimetro di cybersicurezza o destinatari delle direttive NIS (cfr. art. 7, d.l. n. 82/2021), è altrettanto vero che la stessa non è un organo deputato all'attività investigativa *stricto sensu* intesa.

Con la previsione in parola, invece, il legislatore – imponendo all'Agenzia un dovere informativo in favore del Procuratore Nazionale – finisce per attribuire alla stessa (sia pur indirettamente) un potere di impulso investigativo; si rende in tal modo sempre più concreto il pericolo di una convergenza di ruoli che dovevano essere separati e, di conseguenza, di una sovrapposizione tra la funzione di prevenzione propria dell'Agenzia per la Cybersicurezza Nazionale e quella repressiva propria dell'autorità giudiziaria (c.d. poteri investigativi paralleli)[8].

Ciò non senza conseguenze sul versante processuale. Facilitando lo scambio informativo tra l'Agenzia e la Procura Nazionale, la novella disegna un congegno "diabolico" nel quale i confini tra *pre* e *post delictum* appaiono sfumati, quasi evanescenti, acuendo il rischio di osmosi probatoria tra la fase preventiva e quella processuale.

Ci si trova, così, di fronte ad "nuovo" genere di prevenzione, in cui i confini tra pre-procedimento e indagini sono assai più labili, quasi svaniti ed evanescenti, ricchi di punti di contatto e di scambio. Un concetto di prevenzione 2.0 che, in spregio ai *dicta* normativi che impongono una netta separazione tra *pre* e *post* procedimento, spinge per una circolazione probatoria di dati ed informazioni e per un'implementazione delle indagini proattive che, inevitabilmente, si ripercuotono sugli esiti procedimentali, sia investigativi che dibattimentali.

[1] L'Agenzia per la Cybersicurezza Nazionale (ACN), istituita con d.l. n. 82 del 2021, convertito, con modificazioni, dalla l. n. 109 del 2021, ha il compito di tutelare gli interessi nazionali nel campo della cybersicurezza. Ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

[2] In base all'art. 7, comma 1, d.l. n. 82/2021, l'ACN sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia.

[3] Si tratta, più nel dettaglio, dei delitti di cui all'art. 615 *ter*, comma 3, c.p. (accesso abusivo a 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); all'art. 635 *ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità); all'art. 635 *quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità); all'art. 617 *quater* c.p. (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche); all'art. 617 *quinquies* c.p. (detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche); all'art. 617 *sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche del codice penale).

[4] Dunque, secondo la nuova versione dell'art. 54 *ter* c.p.p., "[Q]uando il contrasto previsto dagli artt. 54 e 54 *bis* riguarda taluno dei reati indicati dall'art. 51, commi 3 *bis* e 3 *quater*, e 371 *bis,* comma 4 *bis,* il Procuratore Nazionale Antimafia e Antiterrorismo: deve essere sentito dal procuratore generale presso la Corte di cassazione ai fini della decisione sul contrasto tra pubblici ministeri appartenenti a distretti diversi; deve essere informato dei provvedimenti adottati dal procuratore generale presso la corte d'appello sul contrasto tra p.m. appartenenti al medesimo distretto".

[5] Cfr. P. Bronzo, *Le indagini* Undercover *nel mondo digitale,* in *questa Rivista*, 19 ottobre 2023.

[6] Ossia i casi in cui gli ufficiali di p.g. "si introducono in sistemi informatici o telematici, li danneggiano, cancellano, alterano o comunque intervengono su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumono il controllo o comunque si avvalgono dell'altrui dominio e spazio informatico comunque denominato o compiono attività prodromiche o strumentali.

[7] Si tratta, più nel dettaglio, di specifiche operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale, nonchè delle attività di cui alla lettera a) ovvero si introducono all'interno di un sistema informatico o telematico, danneggiano, deteriorano, cancellano, alterano o comunque intervengono su un sistema informatico o telematico ovvero su informazioni, dati e programmi in esso contenuti, attivano identità, anche digitali, domini e spazi informatici comunque denominati, anche attraverso il trattamento di dati personali di terzi, ovvero assumono il controllo o comunque si avvalgono dell'altrui dominio e spazio informatico comunque denominato o compiono attività prodromiche o strumentali.

[8] Cfr. Speciale su "*Sicurezza dello Stato e poteri investigativi paralleli*", a cura di D. Curtotti, in *Dir. Pen. Cont.,* n. 1, 2023.