1. In sede di conversione del d.l. 10 agosto 2023 n. 105 del 2023 da parte della legge n. 137 del 2023 è stato di recente introdotto l'art. 2-bis recante «Disposizioni urgenti in materia di contrasto della criminalità informatica e di cybersicurezza», destinato a innovare profondamente la cooperazione giudiziaria in materia di *cybersecurity* e reati commessi nel cyberspazio.

Le nuove disposizioni introdotte incidono sulle funzioni dell'Agenzia Nazionale per la *Cybersecurity* – istituita nel 2021 – prevedendo nuove competenze e forme di cooperazione tra quest'ultima ed il Procuratore nazionale antimafia ed antiterrorismo in relazione alle nuove ed insidiose forme di *cybercrime* nazionale e transnazionale (Cfr. W. Nocerino).

Al di là delle ripercussioni in materia di repressione della criminalità informatica, anche organizzata, l'intervento costituisce un ulteriore tassello nella progressiva definizione del ruolo e delle funzioni istituzionali dell'Agenzia nazionale per la cybersicurezza e contribuisce ad avvicinare l'ordinamento italiano al modello indicato dall'Unione europea.

2. La Commissione europea ha da tempo individuato nelle minacce provenienti dallo spazio cibernetico un fattore critico che giustifica l'adozione di interventi di prevenzione e repressione. Le minacce *cyber* derivano da attacchi di tipo *ransomware* (controllo di beni e dati contro la richiesta di "riscatto" in denaro), DDoS (negazione di servizi), *malware* e altri attacchi diretti alla funzionalità di internet ovvero al furto di dati, ma anche dal crescente sviluppo del c.d. cyberterrorismo.

Gli attacchi cibernetici, all'epoca della diffusione delle infrastrutture digitali e del c.d. IoT o "*internet of the things*", rappresentano un pericolo attuale e crescente per il corretto funzionamento di processi informatici e informativi dai quali imprese, individui e amministrazioni pubbliche sono sempre più dipendenti. Questi attacchi rilevano per le istituzioni europee anche e soprattutto nella misura in cui comportano un pregiudizio per il Mercato unico. Secondo dati diffusi dal Consiglio, nel 2020 i danni annui derivanti dalla criminalità informatica hanno raggiunto i 5.500 miliardi di euro e sono raddoppiati rispetto a cinque anni prima. La recente aggressione russa dell'Ucraina ha peraltro incrementato gli attacchi cibernetici verso infrastrutture strategiche europee.

La Commissione ha avanzato nel settembre 2022 una proposta di regolamento in materia di cybersicurezza volta a tutelare imprese e consumatori e modificare il regolamento 2019/1020 (UE), la quale ha trovato un accordo su una posizione comune nel Consiglio (cfr. F. Gatta).

La promozione della sicurezza nello spazio cibernetico richiede però anche un efficace sistema investigativo, uno strumentario digitale adeguato e un idoneo apparato repressivo che conti sulla cooperazione transnazionale. La criminalità informatica attuale ha infatti mostrato di saper cogliere appieno le opportunità offerte dal cyberspazio, approfittando dei limiti costituiti dai confini giurisdizionali nazionali. La cooperazione giudiziaria sovranazionale e internazionale rappresenta quindi una frontiera imprescindibile per una corretta risposta preventiva e sanzionatoria rispetto alle minacce *cyber*. Lo dimostrano i recenti sviluppi dell'Unione che, a partire dalla direttiva 2014/41 (UE) del 3 aprile 2014 sull'ordine europeo di indagine, ha rivoluzione le modalità di acquisizione della prova a livello unionale, con un ruolo crescente di Eurojust e una maggiore centralità delle c.d. prove digitali. La direttiva 2016/1148 (UE) del 6 luglio 2016(c.d. Direttiva "NIS"), ha inoltre introdotto misure destinate a promuovere un livello elevato di sicurezza delle reti e dei sistemi informatici nel territorio dell'Unione.

3. A livello europeo l'ENISA (*European Union Agency for cybersecurity*) rappresenta una realtà attiva dal 2004 nell'assistenza alle istituzioni unionali e agli Stati membri in materia di adozione di *policy* e soluzioni normative sui temi cybersicurezza. Inoltre, mentre altri ordinamenti europei hanno da tempo istituito autorità nazionali in materia di *cybersecurity*, l'Italia ha provveduto all'istituzione di un'agenzia nazionale solo nel 2021.

L'ACN (Agenzia per la cybersicurezza nazionale) rappresenta una delle principali innovazioni introdotte dal decreto-legge n. 82 del 14 giugno 2021, convertito con modificazioni dalla l. 4 agosto 2021 n. 109, allo scopo di riordinare l'intera frammentaria normativa italiana in materia, puntando a ottimizzare e semplificare le competenze nazionali esistenti e salvaguardare la sicurezza nazionale.

Il Decreto Legislativo n. 123/ 2022 del 4 settembre 2022, ha inoltre introdotto disposizioni

per l'attuazione del cosiddetto *Cybersecurity Act* Europeo di cui al Regolamento 2019/881 (UE).

All'Agenzia italiana è stato attribuito dal decreto istitutivo il compito di prevenire e ridurre l'impatto degli attacchi informatici nel cyberspazio italiano. Un ruolo attuato tramite l'attività di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026, definita dalla Presidenza del Consiglio dei ministri, che stabilisce gli attuali *target* da raggiungere entro il 2026.

La *cybersecurity* è anche entrata nel PNRR italiano e, segnatamente, nella missione 1, dedicata alla «digitalizzazione, innovazione e sicurezza della pubblica amministrazione». L'obiettivo prioritario delle istituzioni italiane stabilito nel piano è quello di rafforzare il monitoraggio e la gestione delle minacce *cyber*.

Prima dell'introduzione dell'Agenzia, per lungo tempo la regolazione del rischio cibernetico nel nostro ordinamento è stata attuata prevalentemente attraverso la normazione secondaria e, segnatamente, con l'adozione di D.p.c.m. (cfr. i D.p.c.m. 66/2013 e 17 febbraio 2017 e in argomento L. Previti).

In seguito, il d.lgs. n. 65/2018 recepisce la direttiva NIS con la definizione di misure volte a conseguire un elevato livello di sicurezza nelle reti e nei sistemi informativi ed il d.l. 105/2019, convertito in legge n. 133 del 2019 del 18 novembre 2019, istituisce il «Perimetro di sicurezza nazionale cibernetica». Rientrano nel perimetro amministrazioni pubbliche, enti e operatori nazionali, pubblici e privati individuati da specifici D.p.c.m., caratterizzati da un'importanza strategica e aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione o la fornitura di un servizio considerato essenziale per lo Stato e dal cui malfunzionamento può derivare un pregiudizio alla sicurezza nazionale.

4. Tra le varie competenze dell'Agenzia italiana per la *cybersicurezza* si registra l'attribuzione di poteri ispettivi e sanzionatori ai sensi dell'art. 7 del d.l. 82/2021. Secondo tale disposizione, l'ACN è autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto

legislativo attuativo della direttiva NIS e può provvedere «all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto». L'Agenzia è inoltre individuata come autorità nazionale di certificazione della cybersicurezza *ex* art. 58 del Regolamento (UE) 2019/881, potendo anche in questo contesto accertare violazioni e irrogare sanzioni ai soggetti responsabili.

L'attribuzione di poteri ispettivi e sanzionatori alla ACN è stata salutata freddamente da alcuni commentatori in ragione del mancato coordinamento con le attività della magistratura, di cui non si fa cenno nel decreto istitutivo dell'Agenzia italiana (cfr. C. Rossi, che riporta le parole del Procuratore Nazionale Aggiunto della DNA e F.N. Ricotta sui rapporti tra ACN e servizi di investigazione).

L'intervento in commento, attuato con la l. n. 137/2023 in sede di conversione del d.l. 105/2023 (su cui si vedano le considerazioni a prima lettura di L. Gatta), si inserisce proprio in questo contesto, con le principali novità contenute nell'art. 2-bis.

Mentre i primi due commi della disposizione si rivolgono all'attività di coordinamento investigativo e ai rapporti tra l'ACN e la magistratura, i restanti commi incidono direttamente sul Codice di procedura penale e le prerogative del Procuratore Nazionale antimafia e antiterrorismo (cfr. W. Nocerino).

Più in dettaglio, il primo comma dell'art. 2-bis introduce all'art. 17 del d.l. n. 82/2021 un comma 4-bis. Quest'ultimo prevede un meccanismo di trasmissione delle notizie e delle informazioni rilevanti per l'esercizio delle funzioni di cui all'art. 371-bis c.p. da parte dell'ACN al Procuratore Nazionale Antimafia e Antiterrorismo (di seguito "PNAA"), in relazione ad indagini per reati informatici di particolare gravità.

Il secondo comma introduce tra le funzioni di prevenzione e monitoraggio dell'Agenzia quella di svolgere «ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subìto incidenti di sicurezza informatica o attacchi informatici». La mancata collaborazione di questi ultimi soggetti può essere valutata ai fini

dell'applicazione di sanzioni.

Restano esclusi dalla disposizione gli organi statali preposti alla «prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine, della sicurezza pubblica e alla difesa e sicurezza militare dello Stato nonché gli organismi di informazione per la sicurezza». La *ratio* dell'esclusione è quella di evitare il coinvolgimento dei soggetti statali che svolgono attività di prevenzione e repressione dei reati nello spazio cibernetico.

Il terzo comma dell'art. 2-bis interviene direttamente sul Codice di procedura penale, ampliando i poteri del PNAA. Quest'ultimo, a seguito dell'intervento, può esercitare funzioni d'impulso anche per i delitti di cui agli articoli 615–ter, terzo comma, c.p. (accesso abusivo ad un sistema informatico su sistemi di interesse militare, relativi all'ordine pubblico, la sicurezza, la sanità o comunque di interesse pubblico), 635-ter c.p. (danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o di pubblica utilità) e 635-quinquies c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità).

L'art. 2-bis del d.l. 105/2023 interviene anche sulla cooperazione giudiziaria internazionale e, segnatamente, sugli artt. 724 e 727 c.p.p. Vengono così ampliati gli obblighi di trasmissione a carico del PNAA in merito ai reati informatici stabiliti al c. 4-bis dell'art. 371-bis c.p.p. (cfr. W. Nocerino).

Il quarto comma dell'art. 2-bis modifica la disciplina delle operazioni sotto copertura nel contrasto ai crimini commessi nel cyberspazio. Il decreto innova infatti l'art. 9 della legge 146/2006, di ratifica della Convenzione di Palermo contro la criminalità organizzata transnazionale, estendendo la non punibilità degli ufficiali di PG per i casi di pirateria informatica, accesso e danneggiamento di sistema informatico e altre fattispecie penali commesse di operazioni sotto copertura, ritenute particolarmente efficaci nel perseguimento del *cybercrime*.

Gli ultimi due commi, quinto e sesto, dell'art. 2-bis incidono sulla cooperazione giudiziaria nel contesto dell'Unione, prevedendo la trasmissione da parte del PNAA della richiesta di

riconoscimento di un provvedimento di sequestro richiesto da uno Stato membro dell'UE. Il Procuratore deve inoltre venir informato della presenza di un ordine di indagine europeo in caso di reati di cui al comma 4-bis dell'art. 371-bis c.p.p. e, cioè, dei delitti di cui agli artt. 615-ter, 635-ter, 635-quinquies c.p. commessi in danno di un sistema informatico o telematico utilizzato dallo Stato, da altro ente pubblico, ovvero da privati esercenti servizi di pubblica necessità.

5. Complessivamente, l'intervento del legislatore aggiunge un ulteriore tassello verso un approccio più coordinato nella lotta contro il *cybercrime*, incidendo in un settore effettivamente sensibile e in parte caratterizzato da vuoti normativi come quello della cooperazione tra ACN e magistratura.

L'intenzione di rafforzare le sinergie tra l'Agenzia e il Procuratore nazionale antimafia ed antiterrorismo rappresenta un chiaro segnale di come l'Italia intenda lentamente adattarsi ai crescenti pericoli per le istituzioni del Paese provenienti dal *cybercrime*, per il momento con riguardo alle ipotesi più gravi e di maggior allarme sociale.

Dal punto di vista costituzionale, l'art. 2 bis del d.l. 10 agosto 2023 n. 105 del 2023 desta interesse nella misura in cui contribuisce a definire il ruolo nel sistema di un'Agenzia di recente istituzione come l'ACN e, al contempo, ne accresce le competenze, rendendola un interlocutore di primo piano anche per la magistratura.

L'efficacia delle nuove misure introdotte, peraltro, dipenderà in larga parte dall'abilità di coordinare gli sforzi a livello nazionale e internazionale, assicurando che le istituzioni coinvolte possano beneficiare delle risorse adeguate ad affrontare minacce in continuo mutamento.

L'approntamento di risposte normative e giudiziarie efficaci è del resto quantomai urgente come dimostra il recente attacco al *Data Center* di Westpole del dicembre 2023, già definito «uno dei peggiori attacchi cibernetici contro la Pubblica amministrazione italiana della storia recente» (Il Foglio, 20 dicembre 2023). L'azienda Westpole fornisce servizi in *cloud* tra gli altri a PA Digitale, società che gestisce gli applicativi informatici di oltre mille

pubbliche amministrazioni a livello nazionale.

L'attacco, rivendicato da un gruppo di *hacker* di probabile provenienza russa, ha comportato numerosi disservizi e rischi di ritardi nei pagamenti degli stipendi per molte amministrazioni coinvolte (tra le quali ANAC e AGCOM), oltre a rilevanti perdite di dati.

In ogni caso, di fronte a un quadro che vede l'Italia tra i paesi più colpiti da attacchi di tipo *ramsonware* (L'Identità, 20 dicembre 2023), la difesa cibernetica italiana resta ancora una sfida in larga parte aperta.