Sicurezza delle infrastrutture digitali e potenziamento del contrasto alla criminalità informatica. Fra nuovi poteri e difficili equilibri di sistema*

di *Raffaello Magi*

1. L'art. 2 dl n. 105/2023: infrastrutture digitali interdistrettuali e processo attuativo

La fragilità strutturale delle dotazioni digitali in tema di intercettazioni e dei relativi approvvigionamenti, in termini di sicurezza, riservatezza e affidabilità (fra altre, vds. vicenda *Exodus*[1]) ha condotto all'introduzione di un nuovo sistema tecnologico, volto anche a dare concreta attuazione all'istituzione dell'archivio digitale, già previsto dagli artt. 269, comma 1, cpp e 89-*bis* disp. att. cpp.

Sistema, questo, che fa perno sulla creazione delle nuove «infrastrutture digitali interdistrettuali» previste dall'art. 2 del decreto-legge n. 105/2023[2].

Il provvedimento d'urgenza – contenente una

---

* Pubblicato su *Questione giustizia online* il 4 giugno 2025 (www.questionegiustizia.it/articolo/sicurezza-delle-infrastrutture-digitali).

1. A. Alizzi, *Intercettazioni abusive con "Exodus", le società utilizzatrici dello spyware escono dall'inchiesta di Napoli*, *Il Dubbio*, 12 marzo 2024; *Id.*, *Il caso "Exodus" a un punto di svolta: archiviazione per le società che usavano il software spia creato a Catanzaro,* in *www.lacnews24.it* del 12 marzo 2024.

2. Art. 2 («*Istituzione delle infrastrutture digitali centralizzate per le intercettazioni nonché modifica alla disciplina in materia di registrazione delle spese per intercettazioni*»):
«1. Al fine di assicurare i più elevati e uniformi livelli di sicurezza, aggiornamento tecnologico, efficienza, economicità e capacità di risparmio energetico dei sistemi informativi funzionali alle attività di intercettazione eseguite da ciascun ufficio del pubblico ministero, sono istituite apposite infrastrutture digitali interdistrettuali.
2. Con decreto del Ministro della giustizia, da adottare entro sessanta giorni dalla data di entrata in vigore del presente decreto, sono individuate le infrastrutture di cui al comma 1 e sono definiti i requisiti tecnici essenziali al fine di assicurare la migliore capacità tecnologica, il più elevato livello di sicurezza e l'interoperabilità dei sistemi.
3. Con ulteriore decreto del Ministro della giustizia, da adottare entro i novanta giorni successivi alla scadenza del termine di cui al comma 2, sono definiti i requisiti tecnici specifici per la gestione dei dati, che assicurino l'autenticità, l'integrità e la riservatezza dei dati medesimi anche in relazione al conferimento e ai sistemi di ripristino, ed è disciplinato il collegamento telematico tra le infrastrutture di cui al comma 1 e i luoghi di ascolto presso le procure della Repubblica, garantendo il massimo livello di sicurezza e riservatezza.
4. I requisiti tecnici delle infrastrutture garantiscono l'autonomia del procuratore della Repubblica nell'esercizio delle funzioni di direzione, organizzazione e sorveglianza sulle attività di intercettazione e sui relativi dati, nonché sugli accessi e sulle operazioni compiute sui dati stessi. Fermi restando il segreto investigativo e le garanzie di riservatezza e sicurezza dei dati, il Ministero della giustizia assicura l'allestimento e la manutenzione delle infrastrutture nel rispetto delle predette funzioni e, in ogni caso, con esclusione dell'accesso ai dati in chiaro.
5. Con successivo decreto del Ministro della giustizia, da adottare entro il 1° marzo 2024, è disposta l'attivazione presso le infrastrutture di cui al comma 1, previo accertamento della loro piena funzionalità, dell'archivio digitale di cui agli articoli 269, comma 1, del codice di procedura penale e 89-*bis* delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271.

pluralità di disposizioni eterogenee, con buona pace del principio di intrinseca coerenza che dovrebbe caratterizzare lo strumento del decreto-legge[3] – oltre ai richiamati aspetti tecnico-logistici – non privi comunque di possibili riflessi su funzioni e connessi equilibri sistematici – risponde, poi, a un indirizzo di politica legislativa che avrà seguito con la legge n. 90/2024, inteso ad affidare la reazione ordinamentale ai fenomeni di criminalità informatica alla regia del procuratore nazionale antimafia e antiterrorismo attraverso un'azione – nel dover essere – sinergica con le altre forze in campo (Agenzia per la cybersicurezza nazionale *in primis*), non priva invero di potenziali criticità sul piano della chiarezza sui ruoli e le prerogative fra funzione giudiziaria, in prospettiva processuale, e compiti di prevenzione e resilienza, in materia esercitati da organi dell'esecutivo.

Con riguardo agli aspetti tecnici, le nuove infrastrutture a livello interdistrettuale vengono incontro all'esigenza di mantenere più elevati e omogenei livelli di sicurezza ed efficienza, oltre a una maggiore capacità di risparmio energetico dei sistemi informativi funzionali alle attività di intercettazione, e ciò a fronte delle denunciate problematiche (rappresentate dalla procura nazionale antimafia e antiterrorismo e da numerose procure della Repubblica) connesse alla previsione del citato archivio digitale con riguardo alla sua gestione, alla capienza e alla necessità di garantirne l'assoluta sicurezza[4]. Si rammenta, al riguardo, che l'istituzione dell'archivio delle intercettazioni trova ragione proprio nel riscontrare i richiami del Garante della *privacy* (provvedimento del 18 luglio 2013) circa la disomogeneità verificata nelle diverse procure in rapporto alla protezione dei dati personali e dei sistemi di gestione di tali dati, con grave rischio per i diritti fondamentali, anche in considerazione del costante mutamento tecnologico in atto.

Il percorso individuato dall'art. 2 in commento presenta una *road map* che ha previsto l'adozione di tre decreti ministeriali in via successiva, fino alla costruzione dell'archivio digitale unico.

Il primo decreto, adottato il 6 ottobre 2023[5], ha individuato le infrastrutture digitali interdistrettuali, ponendo i requisiti tecnici essenziali «al fine di assicurare la miglior capacità tecnologica e il più elevato livello di sicurezza e interoperabilità dei sistemi» (art. 2 cit.).

In particolare, il provvedimento colloca le infrastrutture in *data center* del Ministero della giustizia ubicati nei capoluoghi dei distretti di Corte d'appello di Milano, Napoli, Roma e Palermo.

Come evidenziato nel parere del Csm al decreto in parola (delibera del 4 ottobre 2023), «in questo

6. Dalla data di entrata in vigore del decreto di cui al comma 5, sono autorizzati la migrazione dei dati dalle singole procure della Repubblica e il conferimento dei nuovi dati. I tempi, le modalità e i requisiti di sicurezza della migrazione e del conferimento sono definiti con decreto del Ministro della giustizia. Le operazioni sono effettuate dalla direzione generale per i sistemi informativi automatizzati, di intesa con i singoli procuratori della Repubblica.
7. Le attività di cui all'articolo 89-*bis* delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, sono effettuate presso la procura della Repubblica che ha disposto le operazioni di intercettazione.
8. Le intercettazioni relative ai procedimenti penali iscritti successivamente alla data del ((31 dicembre 2025)) sono effettuate mediante le infrastrutture digitali di cui al comma 1.
9. I decreti di cui al presente articolo sono adottati sentiti il Consiglio superiore della magistratura, il Garante per la protezione dei dati personali e il Comitato interministeriale per la cybersicurezza. Ciascuno dei pareri è espresso entro venti giorni dalla trasmissione della richiesta, decorsi i quali il provvedimento può essere comunque adottato.
9-*bis*. Dopo il comma 3 dell'articolo 168-*bis* del testo unico delle disposizioni legislative e regolamentari in materia di spese di giustizia, di cui al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, è aggiunto il seguente:
"3-*bis*. L'importo delle spese relative alle operazioni di intercettazione è specificamente annotato nel foglio delle notizie di cui all'articolo 280".
10. Per l'attuazione delle disposizioni di cui al presente articolo è autorizzata la spesa di 43 milioni di euro per l'anno 2023 e di 50 milioni di euro per ciascuno degli anni 2024 e 2025, per la realizzazione delle infrastrutture informatiche e di 3 milioni di euro annui a decorrere dall'anno 2023 per la gestione, la manutenzione evolutiva e l'assistenza informatica dedicata, cui si provvede:
a) quanto a 43 milioni di euro per l'anno 2023 e a 50 milioni di euro per ciascuno degli anni 2024 e 2025, mediante corrispondente riduzione dello stanziamento del fondo speciale di conto capitale iscritto, ai fini del bilancio triennale 2023-2025, nell'ambito del programma «Fondi di riserva e speciali» della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2023, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia;
b) quanto a 3 milioni di euro annui a decorrere dall'anno 2023, mediante corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2023-2025, nell'ambito del programma «Fondi di riserva e speciali» della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2023, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia.
11. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio».

3. In tal senso vds. A. Celotto, *Sulla conversione in legge del decreto-legge 10 agosto 2023, n. 105 (disposizioni urgenti in materia di processo penale),* in *Giurisprudenza penale*, n. 9 /2023, pp. 1-6 (www.giurisprudenzapenale.com/wp-content/uploads/2023/09/Celotto_gp_2023_9.pdf).

4. *Cfr*. Senato della Repubblica, XIX Legislatura, *Dossier n. 126/1.*

5. Decreto ministeriale 6 ottobre 2023, recante «*Infrastrutture digitali per le intercettazioni, ai sensi dell'articolo 2, comma 2, del decreto-legge 10 agosto 2023, n. 105*», in *Bollettino Ufficiale del Ministero della giustizia*, n. 19, 15 ottobre 2023.

primo *step,* in vista della realizzazione dell'archivio unico, è stato previsto che i dati che in esso confluiranno siano cifrati – ovverosia criptati, in modo da non consentire la leggibilità a prima vista – e memorizzati in aree logiche distinte e segregate per ciascun ufficio. Tali dati saranno quindi accessibili solo da parte dei soggetti legittimati secondo le regole ordinarie del codice di procedura penale e delle relative disposizioni attuative» (p. 2). In tal senso, è stato espresso un giudizio di adeguatezza delle disposizioni attuative (con riferimento alla trasmissione dei dati, alle modalità di registrazione, memorizzazione e conservazione dei dati) con gli obiettivi, seppure da verificare in concreto attraverso le successive fasi d'implementazione del nuovo sistema.

Il secondo passaggio attuativo si è concretizzato con l'adozione del decreto ministeriale del 5 gennaio 2024, recante «Requisiti tecnici specifici per la gestione dei dati presso le infrastrutture digitali interdistrettuali, ai sensi dell'articolo 2, comma 2, del decreto-legge 10 agosto 2023, n. 105»[6].

Lo scopo è quello di prevedere misure idonee a garantire l'autenticità e integrità dei dati, la riservatezza e disciplinare il collegamento telematico fra le stesse infrastrutture e gli impianti installati nelle procure della Repubblica «attraverso l'utilizzo di canali di comunicazione su linee dedicate, fisicamente o logicamente, o comunque su collegamenti basati su Virtual Private Network» (art. 5).

Tuttavia, proprio in relazione alle disposizioni in materia di autenticità e integrità dei dati sembra prefigurarsi una possibile criticità, messa in evidenza dal Csm nel richiesto parere sul provvedimento ministeriale e rimasto, invero, inascoltato.

Si tratta del disposto dell'art. 3, comma 3, in cui si prevede che ogni intervento attuato dal Ministero sui sistemi che possa incidere sulla funzionalità degli stessi è preceduto da un'interlocuzione (non meglio definita) con il procuratore della Repubblica, a cui è comunque assicurata la tracciabilità e l'immediata e diretta conoscibilità di ogni accesso o intervento per manutenzione o assistenza od altra attività che comporti trattamenti, acquisizioni o recupero di dati.

A tal riguardo, il cennato parere dell'Organo di autogoverno aveva puntualmente segnalato che la sola interlocuzione con il procuratore per procedere a operazioni potenzialmente idonee a incidere sulla funzionalità dei sistemi non appariva in grado di garantire allo stesso gli spazi necessari per un intervento incisivo in presenza di ragioni, ad esempio, connesse alla natura delle indagini o al rispetto di termini essenziali, in modo da sospendere o fissare una diversa programmazione di tali interventi tecnici. Perciò sarebbe stato auspicabile prevedere – quantomeno – il rilascio di un nulla osta all'esecuzione delle operazioni in parola, ai fini delle richiamate esigenze investigative e/o procedimentali (vds. Cm, delib. 20 dicembre 2023, pp. 4-5).

Il percorso individuato dal legislatore ha trovato esito nel terzo decreto ministeriale, adottato in data 26 febbraio 2024, recante «attivazione archivio digitale intercettazioni»[7].

Il provvedimento ha previsto l'attivazione dell'archivio *de quo* a far data dal 1° marzo 2024, disciplinando tempi e modi della migrazione dei dati dalle singole procure verso le infrastrutture digitali interdistrettuali, i relativi requisiti di sicurezza, le regole per il conferimento dei dati delle intercettazioni, misure tecnico-organizzative per il funzionamento del sistema e, infine, la titolarità del trattamento dei dati, affidata alle procure procedenti nell'ambito dei procedimenti che richiedono l'esecuzione di intercettazioni e al Ministero a soli fini dell'allestimento e della manutenzione delle infrastrutture, comprendendo l'attivazione dei nuovi archivi centralizzati.

Anche in questo caso va segnalato un passaggio delicato, messo in evidenza nel parere del Csm, riguardante facoltà e prerogative del procuratore della Repubblica interessato. Il punto attiene alle operazioni di conferimento (materiale trasferimento dei dati relativi alle intercettazioni dagli impianti di registrazione dei fornitori all'Archivio digitale delle intercettazioni - ADI - e dagli impianti della procura all'archivio centralizzato), per le quali le disposizioni attuative prevedono un doppio binario: di regola, l'operazione dovrebbe avvenire attraverso rete telematica, ma ove presso le procure sussistano «particolari condizioni di natura tecnica, anche con riferimento all'organizzazione degli edifici, che impediscano ostacolino la realizzazione della rete telematica di cui al comma 2, lettera a), il trasferimento delle intercettazioni dagli impianti di registrazione dei fornitori a ADI potrà avvenire attraverso l'utilizzo di supporti fisici, che rispettano tutti i requisiti di sicurezza di cui all'articolo 5» (art. 3, comma 3).

Va rilevato, cioè, che a fronte delle descritte criticità tecniche nessuno spazio valutativo è lasciato al dirigente dell'ufficio requirente, anche in presenza di scelte che possono incidere potenzialmente in modo pregiudizievole sulla conservazione dei dati delle intercettazioni. Il tutto è quindi lasciato a un'opzione

6. In *Bollettino Ufficiale del Ministero della Giustizia*, n. 1, 15 gennaio 2024.

7. In *Bollettino Ufficiale del Ministero della Giustizia*, n. 4, 29 febbraio 2024.

meramente tecnica non scevra da possibili insidie, una volta abbandonata la via telematica principale.

Nel concludere l'*excursus* sui descritti provvedimenti attuativi, una nota sembra opportuna – e forse significativa – sul previsto *iter* formativo dei decreti, dove la relativa adozione passa comunque per l'acquisizione di tre pareri: del Csm, del Garante della *privacy* e del Comitato interministeriale per la cybersicurezza. Se i primi due rappresentano espressione – rispettivamente – di autonomia della funzione giudiziaria/giurisdizionale e di garanzia per il giusto trattamento dei dati personali, il terzo organo, introdotto dal dl n. 82/2021, presieduto dal Presidente del Consiglio, con la partecipazione dell'Autorità delegata per la sicurezza della Repubblica di cui alla l. n. 124/2007 e i Ministri dei dicasteri competenti negli ambiti connessi a tutti gli aspetti potenzialmente toccati dalla minaccia cibernetica (Interno, Difesa, Esteri ed altri), esprime gli indirizzi generali del Governo e opera l'alta sorveglianza in materia di cybersicurezza, costituendo in qualche modo l'espressione parallela – specifica per la suddetta materia – dell'altro Comitato interministeriale dedicato, sul piano generale, alla sicurezza della Repubblica (CISR), di cui ha anche ereditato talune competenze con il trasferimento dal comparto *intelligence* (DIS, AISE e AISI) all'ACN delle prerogative in tema di cybersicurezza.

Eppure, il provvedimento riguardava in buona parte aspetti squisitamente giudiziari con effetti processuali. Il dato, come meglio emergerà in seguito, è sintomo di un indirizzo – non più tanto sotterraneo – volto al superamento di divisioni connaturali al piano ordinamentale e sistematico, per funzioni e missioni costituzionali, per favorire, al contrario, una sorta di cogestione – difficile da realizzare, invero – dove giudiziario ed esecutivo si mescolano in scenari dichiaratamente collaborativi ma confusi e potenzialmente prevaricatori, in ogni caso tendenti a una centralizzazione non sempre sinonimo di efficienza ed efficacia[8].

2. L'art. 2-*bis* dl n. 105/2023: difficili equilibri fra diverse funzioni istituzionali e scriminanti "di attacco"

E qui veniamo all'altra disposizione in commento (art. 2-*bis* dl n. 105)[9], che della precedente osservazione può costituire un "indizio", introducendosi, nei

8. Si è evidenziato, in relazione alla legislazione in esame, che «ciascun operatore risponde ad un'entità governativa secondo regole specifiche, non necessariamente coerenti con quelle delle altre strutture che intervengono nello stesso momento. Questa situazione potrebbe inibire la circolazione di informazioni vitali fino al punto di trasformarsi in un blocco operativo che minerebbe lo scopo stesso della norma, che è invece quello di dare una risposta coordinata ed efficace alle necessità di difesa e sicurezza dello Stato» (A. Monti, *Sicurezza e/o democrazia? Le debolezza strutturali nelle norme italiane sulla cybersecurity*, *La Repubblica*, 3 novembre 2023).

9. Art. 2-*bis* («*Disposizioni urgenti in materia di contrasto della criminalità informatica e di cybersicurezza*»):
«1. Per la medesima finalità, di cui all'articolo 2, comma 1, del presente decreto, di assicurare i più elevati e uniformi livelli di sicurezza, aggiornamento tecnologico, efficienza ed economicità dei sistemi informativi, nonché a fini di contrasto della criminalità informatica, dopo il comma 4 dell'articolo 17 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è inserito il seguente:
"4-*bis*. Fermo restando quanto previsto dal comma 4, l'Agenzia trasmette al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di cui all'articolo 371-*bis* del codice di procedura penale".
2. All'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, dopo la lettera n) è inserita la seguente:
"n-*bis*) nell'ambito delle funzioni di cui al primo periodo della lettera n), svolge 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 subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi 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 articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124".
3. Al codice di procedura penale sono apportate le seguenti modificazioni:
a) all'articolo 54-ter, comma 1, le parole: "nell'articolo 51, commi 3-*bis* e 3-*quater*," sono sostituite dalle seguenti: "negli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*,";
b) all'articolo 371-*bis* è aggiunto, in fine, il seguente comma:
"4-*bis*. Il procuratore nazionale antimafia e antiterrorismo esercita le funzioni di impulso di cui al comma 2 anche in relazione ai procedimenti per i delitti di cui agli articoli 615-*ter*, terzo comma, 635-*ter* e 635-*quinquies* del codice penale nonché, quando i fatti sono 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, in relazione ai procedimenti per i delitti di cui agli articoli 617-*quater*, 617-*quinquies* e 617-*sexies* del codice penale. Si applicano altresì le disposizioni dei commi 3 e 4 del presente articolo";
c) all'articolo 724, comma 9, le parole: "all'articolo 51, commi 3-*bis* e 3-*quater*" sono sostituite dalle seguenti: "agli articoli 51, commi 3-bis e 3-quater, e 371-bis, comma 4-bis";
d) all'articolo 727, comma 8, le parole: "all'articolo 51, commi 3-*bis* e 3-*quater*," sono sostituite dalle seguenti: "agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*,".
4. All'articolo 9 della legge 16 marzo 2006, n. 146, sono apportate le seguenti modificazioni:
a) al comma 1:

primi due commi, nella delicata fase dell'acquisizione della *notitia criminis* – invero, punto dolente della materia – con l'apparente soluzione, come si vedrà, del «fermo restando… », comoda tecnica per il redigente, ma foriera di confusione, difficoltà interpretative e conseguentemente applicative, soprattutto in un settore dove sono coinvolti soggetti appartenenti a funzioni assolutamente diverse e rispondenti ad altrettanti poteri; che la gestione dell'informazione di un incidente informatico fra esigenze di resilienza, *intelligence* e giudiziarie sia complessa appare già evidente dalla necessità di successive novelle intese a trovare un equilibrio nel disciplinare la trattazione "a più mani" dell'eventuale ipotesi di reato. E dunque il decreto-legge in argomento va letto inevitabilmente in relazione al risultato che si trae dal corpo normativo "madre" (dl n. 82 del 2021), oggetto anche di più recenti modifiche (vds. legge 28 giugno 2024, n. 90).

Considerando tutto ciò, il quadro vigente della materia, sul punto, sembra delinearsi nel modo seguente.

In sintesi, le pubbliche amministrazioni, gli enti locali, compresi i comuni di maggiore entità, le aziende sanitarie, le società di trasporto pubblico sono obbligati a segnalare e successivamente a notificare secondo le procedure previste sul sito *web* dell'ACN gli incidenti avente impatto su reti, sistemi informativi e servizi informatici. La segnalazione deve avvenire senza ritardo e comunque entro il termine massimo di 24 ore dal momento in cui i soggetti obbligati sono venuti a conoscenza dell'incidente a seguito delle evidenze comunque ottenute; la notificazione dovrà poi avvenire, completa di tutti gli elementi informativi disponibili, entro 72 ore dal predetto momento di conoscenza (vds. art. 1 l. cit., n. 90/2024[10]).

L'Agenzia per la cybersicurezza è dunque destinataria dell'informazione primaria e avvia le attività

---

1) alla lettera b) sono aggiunte, in fine, le seguenti parole: "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";
2) dopo la lettera b-*bis*) è aggiunta la seguente:
"b-*ter*) gli ufficiali di polizia giudiziaria dell'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, i quali, nel corso di specifiche operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale e, comunque, al solo fine di acquisire elementi di prova, anche per interposta persona, compiono le 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";
b) al comma 4, primo periodo, sono aggiunte, in fine, le seguenti parole: "nonché, nei casi di cui agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, del codice di procedura penale, al procuratore nazionale antimafia e antiterrorismo";
c) al comma 8, secondo periodo, le parole: "all'articolo 51, comma 3-*bis*" sono sostituite dalle seguenti: "agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-bis, comma 4-*bis*".
5. All'articolo 5, comma 3, del decreto legislativo 15 febbraio 2016, n. 35, le parole: "all'articolo 51, commi 3-*bis* e 3-*quater*" sono sostituite dalle seguenti: "agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*,".
6. All'articolo 4, comma 1, secondo periodo, del decreto legislativo 21 giugno 2017, n. 108, le parole: "all'articolo 51, commi 3-*bis* e 3-*quater*," sono sostituite dalle seguenti: "agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*,"».

10. Art 1 («*Obblighi di notifica di incidenti*»):
«1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali segnalano e notificano, con le modalità e nei termini di cui al comma 2 del presente articolo, gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.
2. I soggetti di cui al comma 1 segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale.
3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società in house che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite

di resilienza, come indicate, *in primis*, nell'art. 7 dl n. 82/2021[11], integrato dall'art. 2-*bis* in commento,

ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, gli obblighi di cui ai commi 1 e 2 del presente articolo si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge.
4. Qualora i soggetti di cui al comma 1 effettuino notifiche volontarie di incidenti al di fuori dei casi indicati nella tassonomia di cui al medesimo comma 1, si applicano le disposizioni dell'articolo 18, commi 3, 4 e 5, del decreto legislativo 18 maggio 2018, n. 65.
5. Nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica all'interessato che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle disposizioni di cui al comma 6 e può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Le modalità di tali ispezioni sono disciplinate con determinazione del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella Gazzetta Ufficiale.
6. Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale applica altresì, nel rispetto delle disposizioni dell'articolo 17, comma 4-*quater*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, introdotto dall'articolo 11 della presente legge, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti di cui al comma 1 del presente articolo. La violazione delle disposizioni del comma 1 del presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.
7. Fermi restando gli obblighi e le sanzioni, anche penali, previsti da altre norme di legge, le disposizioni del presente articolo non si applicano:
a) ai soggetti di cui all'articolo 3, comma 1, lettere g) e i), del decreto legislativo 18 maggio 2018, n. 65, e a quelli di cui all'articolo 1, comma 2-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
b) agli 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 e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124».

11. Art. 7 («*Funzioni dell'Agenzia per la cybersicurezza nazionale*»):
«1. L'Agenzia:
a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;
b) predispone la strategia nazionale di cybersicurezza;
c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;
d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere d) ed e), del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;
d-*bis*) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera g), del decreto legislativo NIS;
d-*ter*) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera i), del decreto legislativo NIS;
e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:
1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;
2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera b), del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente legge, al rilascio del certificato europeo di sicurezza cibernetica;
((e-*bis*) è Autorità competente per l'esecuzione dei compiti previsti dal regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio))
f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:
1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;
2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;
3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;
g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;
h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica,

di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera c), del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;
i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro; (2)
l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;
m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;
m-*bis*) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera b), allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia *blockchain*, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge;
m-*ter*) provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;
n) 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 di cui all'articolo 2, comma 1, lettera i) del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;
n-*bis*) nell'ambito delle funzioni di cui al primo periodo della lettera n), svolge 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 subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, i soggetti essenziali e i soggetti importanti di cui all'articolo 6 del decreto legislativo NIS, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi 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 articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;
n-*ter*) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;
o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;
p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;
q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;
r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.
L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;
s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

per cui l'ACN «svolge 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 subito incidenti di sicurezza informatica o attacchi informatici».

Sarà solo nel 2024 (con la già citata l. n. 90, che riscrive l'art. 17, comma 4 del dl n. 82 cit.)[12] che il personale dell'Agenzia verrà espressamente indicato quale pubblico ufficiale tenuto all'adempimento di cui all'art. 331 cpp con la trasmissione «immediata» delle «notifiche» ricevute dal CSIRT Italia[13] (dopo 72 ore?) all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'art. 7-*bis* dl n. 144/2005.

Ed ecco che, «fermo restando» quanto previsto dal precedente disposto – così come risultante dalla successiva novella del 2024 –, l'ACN è tenuta a trasmettere al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di cui all'art. 371-*bis* cpp[14].

L'altro protagonista della materia e delle novelle in argomento – oltre ACN – è dunque il procuratore nazionale, i cui poteri (impulso, coordinamento, avocazione, intervento in caso di contrasto tra pubblici ministeri, trasmissione delle richieste rogatorie dall'estero e per l'estero) sono estesi anche all'ambito

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;
u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;
v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;
v-*bis*) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;
z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;
aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.
1-*bis*. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere r), s), t), u), v), z) e aa), presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.
2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.
3. *Comma abrogato dal d.lgs. 4 settembre 2024, n. 138.*
4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.
5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica».

12. Art. 17, comma 4: «Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione immediata delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale».

13. Il CSIRT Italia («*Computer Security Incidente Response Team*»), ovvero gruppo di gestione degli incidenti di sicurezza informatica, svolge funzioni di monitoraggio degli incidenti a livello nazionale, con competenza in relazione all'emissione degli allarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti.

14. Al riguardo, sono state sollevate perplessità nel senso che il ruolo di impulso informativo verso la Procura nazionale da parte di un organo non deputato all'attività investigativa porta a configurare un «congegno diabolico» dove i confini fra *pre* e *post delictum* si confondono, «acuendo il rischio di osmosi probatoria tra la fase preventiva e quella processuale» (W. Nocerino, *Le nuove norme di prevenzione e contrasto alla criminalità informatica*, in *Pen. dir. proc.*, 9 novembre 2023). Più in generale, sulla fase antecedente alle rituali indagini preliminari, vds. A. Scalfati (a cura di), *Pre-investigazioni (espedienti e mezzi)*, Giappichelli, Torino, 2020.

di gravi reati informatici declinati nel nuovo comma 4-*bis* dell'art. 371-*bis* cpp (accesso abusivo a sistemi informatici, danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o comunque di rilievo pubblico, intercettazioni abusive o interruzione di comunicazioni, detenzione, diffusione e installazione abusiva di apparecchiature idonee a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; falsificazione, alterazione o soppressione di comunicazioni informatiche/telematiche).

Così è che – sempre nella previsione della novella del luglio 2024 – fermo restando quanto previsto dal citato art. 17, comma 4 (comunicazione agli organi di polizia giudiziaria), quando l'Agenzia ha notizia di un attacco ai danni di uno dei sistemi informatici di cui all'art. 371-*bis* cpp e in ogni caso quando l'interessato è uno dei soggetti del cd. "perimetro" (enti con infrastrutture sensibili per la sicurezza del Paese), procede con le proprie attività di analisi e ripristino e ne informa senza ritardo il procuratore nazionale.

Dall'ulteriore norma introdotta dalla legge n. 90/2024 nel dl n. 82/2021 (art. 17, comma 4-*bis*.2)[15], risulta evidente il ruolo di *dominus* dell'Agenzia, anche in presenza di una notizia di reato e di una conseguente quanto obbligatoria attività giudiziaria. E infatti, ove un pubblico ministero dovesse acquisire la notizia di un delitto *ex* art. 371, comma 4-*bis* cpp, deve darne tempestiva informazione all'ACN e deve assicurare il raccordo informativo con l'organo del Ministero dell'interno per la regolarità dei servizi di telecomunicazione (che dovrebbe essere, come visto, destinatario dell'informazione da parte del personale della stessa Agenzia).

Il pubblico ministero deve dare disposizioni affinché le attività giudiziarie di accertamento urgente tengano conto delle attività di competenza dell'Agenzia a fini di resilienza, con una clausola di salvezza, ossia disporre un differimento di queste ultime con provvedimento motivato per evitare un grave pregiudizio alle indagini (art. 17, comma 4-*bis*.3 dl n. 82/2021).

Ancora, quando il pm procede ad accertamenti tecnici irripetibili o anche se si procede nelle forme dell'incidente probatorio nell'ambito di indagini per i delitti di cui al richiamato art. 371-*bis*, comma 4-*bis* cpp, l'Agenzia va informata senza ritardo e può partecipare agli atti con propri rappresentanti.

Si è intervenuto dunque sul momento essenziale e più delicato della funzione giudiziaria e della sequenza procedimentale – l'acquisizione delle notizie di reato e il conseguente avvio delle indagini –, finendo con alterare l'ordine costituzionale, prima ancora che processuale, che vede il pubblico ministero quale riferimento per assumere il prima possibile le segnalazioni di condotte rilevanti penalmente, così da condurre con efficacia e immediatezza gli accertamenti e le attività necessarie per le proprie determinazioni. E infatti, le segnalazioni massimo entro le 24 ore deve riceverle l'ACN (organo dell'esecutivo) – e non chi è deputato all'esercizio dell'azione penale –, che solo successivamente, e dopo aver avviato attività di resilienza, dovrà notificare i fatti all'organo di polizia giudiziaria dedicato.

Tanto appare capovolto l'ordinario *modus procedendi*, che tocca (= obbligo) al pubblico ministero che per caso ha assunto per primo la *notizia criminis* darne subito informazione all'Agenzia *cyber*. Tutto ciò pone senz'altro delle criticità rispetto alla regola *ex* art. 331 cpp e alla tenuta del segreto d'indagine (329 cpp), nonché alla praticabilità, in una materia di evidenze soprattutto tecniche da cogliere in tempi brevi, di un'indagine seria e producente, atteso il precedente e poi contemporaneo intervento della ACN. Il disordine normativo si evidenzia ancor più se si tiene conto della difficoltà per il pubblico ufficiale appartenente a un'amministrazione tenuta alla segnalazione all'ACN di conciliare ciò con il dovere di cui al 331 cpp: *quid iuris*? Quale obbligo deve prevalere? Salomonicamente, si potrebbe suggerire di adempiere entrambi, ma in tal caso non avrebbe senso la successiva notifica alla polizia giudiziaria da parte dell'Agenzia, e le indagini sarebbero comunque compromesse.

Non si tratta, qui, del fenomeno – pure non opportuno – di "ipertrofia delle indagini", con attività di inchiesta preliminare da far rientrare in modo utile nel processo a discapito dei principi fondamentali che reggono la prova nei sistemi democratici (*in primis*, formazione in contraddittorio fra le parti)[16], ma piuttosto di relegare a un ruolo quasi ancillare la funzione

15. Art. 17, commi:
«4-*bis*.2. Fuori dei casi di cui al comma 4-*bis*.1, quando acquisisce la notizia dei delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, il pubblico ministero ne dà tempestiva informazione all'Agenzia e assicura, altresì, il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione ai fini di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.
4-*bis*.3. In ogni caso, il pubblico ministero impartisce le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'Agenzia, a fini di resilienza, di cui all'articolo 7, comma 1, lettere n) e n-*bis*), e può disporre il differimento di una o più delle predette attività, con provvedimento motivato adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini».

16. In tal senso vds. A. Scalfati, *Il fermento pre-investigativo*, in *Id.* (a cura di), *Pre-investigazioni*, *op. cit.*, pp. 1 ss.

giudiziaria rispetto a finalità e organi del tutto estranei cui sono offerte prerogative idonee a pregiudicare ogni indagine giudiziaria in tema di *cyber crime*.

Coerente con ciò è l'originale posizionamento di tecnici – si presume – dell'ACN nell'ambito degli accertamenti *ex* art. 360 cpp o nella formazione della prova attraverso l'incidente probatorio. Una presenza spuria nell'ambito – in un caso – di tipiche attività giudiziarie del pubblico ministero con garanzie difensive – nel secondo – in un atto di formazione anticipata della prova in cui, oltre alle parti, per esigenze estranee alla giurisdizione, dovrebbero partecipare rappresentati di una agenzia governativa cui spetterebbe intervenire per prevenire/rimediare, per quanto possibile, ad attacchi *cyber*.

La disposizione, a ben vedere, rafforza la perplessità sull'utilità delle indagini nel sistema previsto. Se si è inteso rendere partecipe nell'atto di accertamento tecnico l'ACN nell'ipotesi – invero – residuale in cui un pubblico ministero acquisisce per primo la notizia di reati (situazione eccezionale per il legislatore, tanto da porvi rimedio con questa previsione), sta a significare che nella normalità dei casi le infrastrutture informatiche oggetto di reati sono trattate dall'Agenzia, nell'immediatezza dei fatti, in modo da rendere problematici gli accertamenti e le verifiche a fini giudiziari.

Lo scenario descritto esprime, tirando le somme, una chiara tendenza a confondere i confini fra prevenzione, attività giudiziaria di accertamento dei reati e giurisdizione, avvicinando pericolosamente organi dell'esecutivo alle funzioni giudiziarie e organi giudiziari ai compiti di prevenzione/*intelligence*. Che questo sia il prezzo da pagare a un'esigenza di rapidità d'intervento in un settore – di certo – nevralgico è tutto da dimostrare.

La comprova di questa linea è riscontrabile anche nell'ultimo argomento della novella in esame, ossia l'ampliamento dell'ambito di operatività della scriminante contenuta nell'art. 9 della legge n. 145 del 2006[17], consentendo alle forze di polizia, con autorizzazione di vertici tecnici, condotte di attacco a

17. Art. 9 («*Operazioni sotto copertura*»):
«1. Fermo quanto disposto dall'articolo 51 del codice penale, non sono punibili:
a) gli ufficiali di polizia giudiziaria della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, appartenenti alle strutture specializzate o alla Direzione investigativa antimafia, nei limiti delle proprie competenze, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti previsti dagli articoli 317, 318, 319, 319-*bis*, 319-*ter*, 319-*quater*, primo comma, 320, 321, 322, 322-*bis*, 346-*bis*, 353, 353-*bis*, 452-*quaterdecies*, 453, 454, 455, 460, 461, 473, 474, ((517-*quater*,)) 629, 630, 644, 648-*bis* e 648-*ter*, nonché nel libro secondo, titolo XII, capo III, sezione I, del codice penale, ai delitti concernenti armi, munizioni, esplosivi, ai delitti previsti dall'articolo 12, commi 1, 3, 3-*bis* e 3-*ter*, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, nonché ai delitti previsti dal testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e dall'articolo 3 della legge 20 febbraio 1958, n. 75, anche per interposta persona, danno rifugio o comunque prestano assistenza agli associati, acquistano, ricevono, sostituiscono od occultano denaro o altra utilità, armi, documenti, sostanze stupefacenti o psicotrope, beni ovvero cose che sono oggetto, prodotto, profitto, prezzo o mezzo per commettere il reato o ne accettano l'offerta o la promessa o altrimenti ostacolano l'individuazione della loro provenienza o ne consentono l'impiego ovvero corrispondono denaro o altra utilità in esecuzione di un accordo illecito già concluso da altri, promettono o danno denaro o altra utilità richiesti da un pubblico ufficiale o da un incaricato di un pubblico servizio o sollecitati come prezzo della mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o per remunerarlo o compiono attività prodromiche e strumentali;
b) gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell'Arma dei carabinieri specializzati nell'attività di contrasto al terrorismo e all'eversione e del Corpo della guardia di finanza competenti nelle attività di contrasto al finanziamento del terrorismo, i quali, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo o di eversione, anche per interposta persona, compiono le 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;
b-*bis*) gli ufficiali di polizia giudiziaria degli organismi specializzati nel settore dei beni culturali, nell'attività di contrasto dei delitti di cui agli articoli 518-*sexies* e 518-*septies* del codice penale, i quali nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova, anche per interposta persona, compiono le attività di cui alla lettera a);
b-*ter*) gli ufficiali di polizia giudiziaria dell'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, i quali, nel corso di specifiche operazioni di polizia finalizzate al contrasto dei reati informatici commessi ai danni delle infrastrutture critiche informatizzate individuate dalla normativa nazionale e internazionale e, comunque, al solo fine di acquisire elementi di prova, anche per interposta persona, compiono le 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.
1-*bis*. La causa di giustificazione di cui al comma 1 si applica agli ufficiali e agenti di polizia giudiziaria e agli ausiliari che operano sotto copertura quando le attività sono condotte in attuazione di operazioni autorizzate e documentate ai sensi del presente articolo. La disposizione di cui al precedente periodo si applica anche alle interposte persone che compiono gli atti di cui al comma 1.

2. Negli stessi casi previsti dal comma 1, gli ufficiali e gli agenti di polizia giudiziaria possono utilizzare documenti, identità o indicazioni di copertura, rilasciati dagli organismi competenti secondo le modalità stabilite dal decreto di cui al comma 5, anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone il pubblico ministero al più presto e comunque entro le quarantotto ore dall'inizio delle attività.
3. L'esecuzione delle operazioni di cui ai commi 1 e 2 è disposta dagli organi di vertice ovvero, per loro delega, dai rispettivi responsabili di livello almeno provinciale, secondo l'appartenenza del personale di polizia giudiziaria impiegato, d'intesa con la Direzione centrale dell'immigrazione e della polizia delle frontiere per i delitti previsti dall'articolo 12, commi 1, 3, 3-*bis* e 3-*ter*, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni. L'esecuzione delle operazioni di cui ai commi 1 e 2 in relazione ai delitti previsti dal testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, di seguito denominate "attività antidroga", è specificatamente disposta dalla Direzione centrale per i servizi antidroga o, sempre d'intesa con questa, dagli organi di vertice ovvero, per loro delega, dai rispettivi responsabili di livello almeno provinciale, secondo l'appartenenza del personale di polizia giudiziaria impiegato.
4. L'organo che dispone l'esecuzione delle operazioni di cui ai commi 1 e 2 deve dare preventiva comunicazione all'autorità giudiziaria competente per le indagini nonché, nei casi di cui agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, del codice di procedura penale, al procuratore nazionale antimafia e antiterrorismo. Dell'esecuzione delle attività antidroga è data immediata e dettagliata comunicazione alla Direzione centrale per i servizi antidroga e al pubblico ministero competente per le indagini.
Se necessario o se richiesto dal pubblico ministero e, per le attività antidroga, anche dalla Direzione centrale per i servizi antidroga, è indicato il nominativo dell'ufficiale di polizia giudiziaria responsabile dell'operazione, nonché quelli degli eventuali ausiliari e interposte persone impiegati. Il pubblico ministero deve comunque essere informato senza ritardo, a cura del medesimo organo, nel corso dell'operazione, delle modalità e dei soggetti che vi partecipano, nonché dei risultati della stessa.
5. Per l'esecuzione delle operazioni di cui ai commi 1 e 2, gli ufficiali di polizia giudiziaria possono avvalersi di agenti di polizia giudiziaria, di ausiliari e di interposte persone, ai quali si estende la causa di non punibilità prevista per i medesimi casi.
Per l'esecuzione delle operazioni può essere autorizzata l'utilizzazione temporanea di beni mobili ed immobili, di documenti di copertura, l'attivazione di siti nelle reti, la realizzazione e la gestione di aree di comunicazione o scambio su reti o sistemi informatici, secondo le modalità stabilite con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia e con gli altri Ministri interessati. Con il medesimo decreto sono stabilite altresì le forme e le modalità per il coordinamento, anche in ambito internazionale, a fini informativi e operativi tra gli organismi investigativi.
6. Quando è necessario per acquisire rilevanti elementi probatori ovvero per l'individuazione o la cattura dei responsabili dei delitti previsti dal comma 1, per i delitti di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, limitatamente ai casi previsti agli articoli 70, commi 4, 6 e 10, 73 e 74, gli ufficiali di polizia giudiziaria, nell'ambito delle rispettive attribuzioni, e le autorità doganali, limitatamente ai citati articoli 70, commi 4, 6 e 10, 73 e 74 del testo unico di cui al decreto del Presidente della Repubblica n. 309 del 1990, e successive modificazioni, possono omettere o ritardare gli atti di propria competenza, dandone immediato avviso, anche oralmente, al pubblico ministero, che può disporre diversamente, e trasmettendo allo stesso pubblico ministero motivato rapporto entro le successive quarantotto ore. Per le attività antidroga, il medesimo immediato avviso deve pervenire alla Direzione centrale per i servizi antidroga per il necessario coordinamento anche in ambito internazionale.
6-*bis*. Quando è necessario per acquisire rilevanti elementi probatori, ovvero per l'individuazione o la cattura dei responsabili dei delitti di cui all'articolo 630 del codice penale, il pubblico ministero può richiedere che sia autorizzata la disposizione di beni, denaro o altra utilità per l'esecuzione di operazioni controllate per il pagamento del riscatto, indicandone le modalità.
Il giudice provvede con decreto motivato.
7. Per gli stessi motivi di cui al comma 6, il pubblico ministero può, con decreto motivato, ritardare l'esecuzione dei provvedimenti che applicano una misura cautelare, del fermo dell'indiziato di delitto, dell'ordine di esecuzione di pene detentive o del sequestro.
Nei casi di urgenza, il ritardo dell'esecuzione dei predetti provvedimenti può essere disposto anche oralmente, ma il relativo decreto deve essere emesso entro le successive quarantotto ore. Il pubblico ministero impartisce alla polizia giudiziaria le disposizioni necessarie al controllo degli sviluppi dell'attività criminosa, comunicando i provvedimenti adottati all'autorità giudiziaria competente per il luogo in cui l'operazione deve concludersi ovvero attraverso il quale si prevede sia effettuato il transito in uscita dal territorio dello Stato ovvero in entrata nel territorio dello Stato delle cose che sono oggetto, prodotto, profitto o mezzo per commettere i delitti nonché delle sostanze stupefacenti o psicotrope e di quelle di cui all'articolo 70 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni.
8. Le comunicazioni di cui ai commi 4, 6 e 6-*bis* e i provvedimenti adottati dal pubblico ministero ai sensi del comma 7 sono senza ritardo trasmessi, a cura del medesimo pubblico ministero, al procuratore generale presso la corte d'appello. Per i delitti indicati agli articoli 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, del codice di procedura penale, la comunicazione è trasmessa al procuratore nazionale antimafia.
9. L'autorità giudiziaria può affidare il materiale o i beni sequestrati in custodia giudiziale, con facoltà d'uso, agli organi di polizia giudiziaria che ne facciano richiesta per l'impiego nelle attività di contrasto di cui al presente articolo ovvero per lo svolgimento dei compiti d'istituto.
9-bis. I beni informatici o telematici confiscati in quanto utilizzati per la commissione dei delitti di cui al libro II, titolo XII, capo III, sezione I, del codice penale sono assegnati agli organi di polizia giudiziaria che ne abbiano avuto l'uso ai sensi del comma 9.
10. Chiunque indebitamente rivela ovvero divulga i nomi degli ufficiali o agenti di polizia giudiziaria che effettuano le operazioni di cui al presente articolo è punito, salvo che il fatto costituisca più grave reato, con la reclusione da due a sei anni.
11. Sono abrogati:
a) l'articolo 10 del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni;
b) l'articolo 12-*quater* del decreto-legge 8 giugno 1992, n. 306, convertito, con modificazioni, dalla legge 7 agosto 1992, n. 356;
c) l'articolo 12, comma 3-*septies*, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286;
d) l'articolo 14, comma 4, della legge 3 agosto 1998, n. 269;
e) l'articolo 4 del decreto-legge 18 ottobre 2001, n. 374, convertito, con modificazioni, dalla legge 15 dicembre 2001, n. 438;
f) l'articolo 10 della legge 11 agosto 2003, n. 228.
f-*bis*) l'articolo 7 del decreto-legge 15 gennaio 1991, n. 8, convertito, con modificazioni, dalla legge 15 marzo 1991, n. 82, e successive modificazioni».

sistemi informatici (danneggiamento, cancellazione, alterazione e altre) più consone ad attività di difesa o di *intelligence* che non finalizzate – come nella specie – alla ricerca probatoria[18].

Al di là dei pregiudizi per le garanzie di difesa, in prospettiva probatoria, che tali condotte possono comportare nell'accertamento in sede giudiziaria delle ipotesi di reato per le quali l'attività scriminata sarebbe posta in essere, un confronto con altra scriminante prevista, quella per le agenzie di informazione per la sicurezza, fa cogliere in pieno le criticità della nuova causa di giustificazione in relazione ai presupposti fondamentali di tale istituto: proporzionalità e bilanciamento dei valori in gioco.

Il fatto è che il tipo di condotte concesso, sul piano tecnico, può condurre ad eventi non sempre prevedibili che possono incidere, come conseguenza ed effetto, anche indiretto, su beni di estremo rilievo, come l'integrità fisica, se non la vita.

Di ciò, appunto, il legislatore, nel disciplinare la garanzia funzionale per l'*intelligence* (art. 37 dl n. 115/2022[19]) era avveduto, tanto da scrivere una norma, pur con carenze sul piano della tassatività, ma che cercava di porre limiti e condizioni: in particolare, per quanto detto, nel prevedere una valutazione volta ad escludere – alla luce delle più aggiornate cognizioni informatiche e fatti salvi i fattori imprevisti e imprevedibili – la lesione degli interessi primari codificati nell'art. 17 l. n. 124/2007[20] quali limiti invalicabili per l'operatività delle garanzie funzionali in favore degli

---

18. In tal senso *cfr*. A. Monti, *Sicurezza*, *cit.*; sull'istituto in generale, *cfr*. L. Ludovici, *L'agente sotto copertura*, in G. Colaiacovo (a cura di), *Sicurezza, informazioni e giustizia penale*, Pacini giuridica, Pisa, 2023, cap. 7, pp. 685-716.

19. Art. 37 («*Disposizioni in materia di intelligence in ambito cibernetico*»):
«1. Al decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, dopo l'articolo 7-*bis* è inserito il seguente:
"Art. 7-*ter* (Misure di intelligence di contrasto in ambito cibernetico). - 1. Il Presidente del Consiglio dei ministri, acquisito il parere del Comitato interministeriale per la sicurezza della Repubblica e sentito il Comitato parlamentare per la sicurezza della Repubblica, emana, ai sensi dell'articolo 1, comma 3, della legge 3 agosto 2007, n. 124, 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 coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale. Le disposizioni di cui al primo periodo prevedono la cooperazione del Ministero della difesa e il ricorso alle garanzie funzionali di cui all'articolo 17 della legge 3 agosto 2007, n. 124.
2. Le disposizioni di cui al comma 1 disciplinano il procedimento di autorizzazione, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità. L'autorizzazione è disposta sulla base di una valutazione volta ad escludere, alla luce delle più aggiornate cognizioni informatiche, fatti salvi i fattori imprevisti e imprevedibili, la lesione degli interessi di cui all'articolo 17, comma 2, della legge 3 agosto 2007, n. 124.
3. Le misure di contrasto in ambito cibernetico autorizzate ai sensi del comma 2 sono attuate dall'Agenzia informazioni e sicurezza esterna e dall'Agenzia informazioni e sicurezza interna, ferme restando le competenze del Ministero della difesa ai sensi dell'articolo 88 del ((codice dell'ordinamento militare, di cui al)) decreto legislativo 15 marzo 2010, n. 66 e le competenze del Ministero dell'interno di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155. Il Dipartimento delle informazioni per la sicurezza assicura il coordinamento di cui all'articolo 4, comma 3, lettera d-*bis*), della legge n. 124 del 2007.
4. Il Presidente del Consiglio dei ministri informa il Comitato parlamentare per la sicurezza della Repubblica ((,)) con le modalità indicate nell'articolo 33, comma 4, della legge n. 124 del 2007, delle misure ((di)) *intelligence* di cui al presente articolo.
5. Al personale delle Forze armate impiegato nell'attuazione delle attività di cui al presente articolo si applicano le disposizioni di cui all'articolo 19 della legge 21 luglio 2016, n. 145, e, ove ne ricorrano i presupposti, ((all'articolo)) 17, comma 7, della legge n. 124 del 2007.
6. Il Comitato parlamentare per la sicurezza della Repubblica trascorsi ventiquattro mesi dalla data di entrata in vigore della presente disposizione trasmette alle Camere una relazione sull'efficacia delle norme contenute nel presente articolo"».

20. Art.17 («*Ambito di applicazione delle garanzie funzionali*»):
«1. Fermo quanto disposto dall'articolo 51 del codice penale, non è punibile il personale dei servizi di informazione per la sicurezza che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi, nel rispetto rigoroso dei limiti di cui ai commi 2, 3, 4 e 5 del presente articolo e delle procedure fissate dall'articolo 18.
2. La speciale causa di giustificazione di cui al comma 1 non si applica se la condotta prevista dalla legge come reato configura delitti diretti a mettere in pericolo o 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.
3. La speciale causa di giustificazione non si applica, altresì, nei casi di delitti di cui agli articoli 289 e 294 del codice penale e di delitti contro l'amministrazione della giustizia, salvo che si tratti di condotte di favoreggiamento personale o reale indispensabili alle finalità istituzionali dei servizi di informazione per la sicurezza e poste in essere nel rispetto rigoroso delle procedure fissate dall'articolo 18, sempre che tali condotte di favoreggiamento non si realizzino attraverso false dichiarazioni all'autorità giudiziaria oppure attraverso occultamento della prova di un delitto ovvero non siano dirette a sviare le indagini disposte dall'autorità giudiziaria. La speciale causa di giustificazione non si applica altresì alle condotte previste come reato a norma dell'articolo 255 del codice penale e della legge 20 febbraio 1958, n. 75, e successive modificazioni.
4. Non possono essere autorizzate, ai sensi dell'articolo 18, condotte previste dalla legge come reato per le quali non è opponibile il segreto di Stato a norma dell'articolo 39, comma 11, ad eccezione delle fattispecie di cui agli articoli 270-*bis*, secondo comma, e 416-*bis*, primo comma, del codice penale.
5. Le condotte di cui al comma 1 non possono essere effettuate nelle sedi di partiti politici rappresentati in Parlamento o in un'assemblea o consiglio regionale, nelle sedi di organizzazioni sindacali ovvero nei confronti di giornalisti professionisti iscritti all'albo.
6. La speciale causa di giustificazione si applica quando le condotte:

agenti dell'AISE e dell'AISI[21]. In più, quella scriminante trova come soggetto autorizzante il Presidente del Consiglio e presupposto uno stato di crisi o di emergenza a fronte di minacce alla sicurezza nazionale non contrastabili solo con azioni di resilienza.

Ora, la sproporzione tra le due previsioni giustificatrici, quella per l'*intelligence* e quella per le forze di polizia, appare evidente e apre un varco anomalo alle ultime che alimenta, ancora una volta, quella sensazione di confusione di ruoli e funzioni rinvenuta in tanti passaggi della nuova normativa descritta in materia *cyber*.

Tema, questo, senz'altro urgente, che sconta ritardi nei confronti di altre realtà nazionali, occidentali e non, ma che andrebbe trattato con maggiore visione sistematica. Al contrario, si ha l'impressione che la normativa *de qua* sia espressione di una "corsa" del legislatore a prevedere procedure, poteri e strumenti condizionato da diverse spinte che rendono difficile la formazione di un percorso coerente e in linea con i valori costituzionali in tema di accertamento e repressione dei reati.

a) sono poste in essere nell'esercizio o a causa di compiti istituzionali dei servizi di informazione per la sicurezza, in attuazione di un'operazione autorizzata e documentata ai sensi dell'articolo 18 e secondo le norme organizzative del Sistema di informazione per la sicurezza;
b) sono indispensabili e proporzionate al conseguimento degli obiettivi dell'operazione non altrimenti perseguibili;
c) sono frutto di una obiettiva e compiuta comparazione degli interessi pubblici e privati coinvolti;
d) sono effettuate in modo tale da comportare il minor danno possibile per gli interessi lesi.
7. Quando, per particolari condizioni di fatto e per eccezionali necessità, le attività indicate nel presente articolo sono 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 risulta 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 dall'articolo 18, tali persone sono equiparate, ai fini dell'applicazione della speciale causa di giustificazione, al personale dei servizi di informazione per la sicurezza».

21. Sulle garanzie funzionali in favore delle agenzie di *intelligence* vds., fra gli altri: F. Marenghi, *Commento all'art. 17*, in *Legislazione penale*, 2007, (Aa.Vv., *La nuova disciplina dei servizi di sicurezza*), pp. 717 ss.; G. Guccione, *Le garanzie funzionali*, in G. Illuminati (a cura di), *Nuovi profili del segreto di Stato e dell'attività di intelligence*, Giappichelli, Torino, 2010, pp. 265 ss.; A. Di Muro, *Garanzie funzionali e status giuridico del personale dei Servizi di informazione per la sicurezza*, in G. Dalia e M. Panebianco (a cura di), *Il segreto di Stato. Una indagine multidisciplinare sull'equo bilanciamento di ragioni politiche e giuridiche*, Giappichelli, Torino, 2022, pp. 261-274; per la genesi storica dell'istituto, in prospettiva processuale, vds. G. De Stefano, *Sicurezza della Repubblica e processo penale*, ESI, Napoli, 2001.