Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di

Raffaella Brighi e Giovanna Adinolfi

Giappichelli

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di
Raffaella Brighi e Giovanna Adinolfi

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111

http://www.giappichelli.it

ISBN/EAN 979-12-211-1735-6
ISBN/EAN 979-12-211-6531-9 (ebook)

Il volume è esito del progetto di ricerca "Ecocyber - Risk management for future cyber-physical ecosystems" nell'ambito dello Spoke 8 del Paternariato esteso SERICS- SEcurity and RIghts in the CyberSpace.
Finanziato dall'Unione Europea – NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 – Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca – D. D. 341 del 15/03/2022, PE7 SERICS – SEcurity and RIghts in the CyberSpace , Codice proposta: PE00000014, CUP: J33C22002810001,finanziato con Decreto n. 1556 del 11/10/2022.
I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, né può l'Unione Europea essere ritenuta responsabile per esse.

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: LegoDigit s.r.l. - Lavis (TN)

Indice

pag.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi

pag.

Capitolo 4

La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*

Giulia Gabrielli

Capitolo 5

Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente

Riccardo Allegri, Giorgio Scichilone

Capitolo 6

Politiche di cybersicurezza e implicazioni strategiche: una lettura politologica

Luigi Martino, Giampiero Giacomello, Oltion Preka

pag.

pag.

Capitolo 9

Profili informatico-giuridici della cybersicurezza nel procurement sanitario

Marco Mancarella

Capitolo 10

Cybersicurezza e *cyber deception*: sfide e prospettive processualpenalistiche

Mariagisa Landolfi

pag.

Parte III

Cybersicurezza e tutela dei diritti fondamentali: una prospettiva critica

Capitolo 11

Polizia, *big data* e società digitale: sicurezza dei dati, sicurezza dai dati

Giulia Fabini

Capitolo 12

Il *Cyber Resilience Act* come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli

Virginia Remondino

pag.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese, Giulia Lasagni

Parte IV

Consapevolezza, educazione e politiche

Capitolo 14

Cybersicurezza e fattore umano: un approccio educativo inclusivo

Antonella Carbonaro, Enrico Gnagnarella

pag.

Capitolo 15

Per un uso consapevole e sicuro delle tecnologie: strategie educative e strumenti di intervento

Valeria Barone, Thomas Casadei

pag.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese [*], Giulia Lasagni [**]

Abstract: L'affidamento che la società ripone nei sistemi informatici acuisce le preoccupazioni del legislatore, europeo e nazionale, a protezione degli stessi. Incidenti e attacchi possono impattare sulla complessiva tenuta del sistema. Col fine di prevenire e, se del caso, reprimere condotte irrispettose degli interessi in gioco, si aumentano i doveri di adeguamento e, correlativamente, anche i poteri delle autorità di controllo. Ritrovare un equilibrio fra tutela delle esigenze statuali e quelle del singolo sottoposto all'accertamento è opera complessa e lo è ancor di più se, per quegli stessi fatti, ne dovesse derivare un procedimento penale. Con questa consapevolezza, il capitolo, ricostruita sommariamente la legislazione rilevante, si pone l'obiettivo di rintracciare un ideale, nuovo punto di equilibrio.

Keywords: Cybersicurezza – Processo penale – Pubblic private cooperation – Acquisizione dei dati

[*] Assegnista di ricerca in Procedura Penale, Dipartimento di Scienze giuridiche, Università di Bologna, antonio.pugliese7@unibo.it. Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea – NextGenerationEU. Pure essendo il capitolo il frutto di una riflessione comune fra gli autori, G. Lasagni è autrice dei paragrafi 3 e 5; A. Pugliese dei paragrafi 1, 2 e 4.

[**] Professoressa Associata di Procedura Penale, Dipartimento di Scienze giuridiche, Università di Bologna, giulia.lasagni6@unibo.it.

1. Introduzione. Cybersecurity, esercizio dei poteri investigativi e responsabilità penale: alcune nuove prospettive

L'attuale crisi politica internazionale, così come alcuni recenti casi giudiziari nazionali e con ampia risonanza nell'opinione pubblica [1], pongono al centro dell'attenzione la tutela degli interessi relativi alla sicurezza informatica e delle reti, quindi della protezione delle infrastrutture. La ragione dei timori connessi alla tutela del cyberspazio è presto spiegata.

La società contemporanea è perennemente interconnessa, affidando alla dimensione digitale una importante fetta delle interazioni necessarie al proprio funzionamento. Anzi, oramai molti ambiti della vita quotidiana hanno piuttosto referenti nella realtà fisica solo in via occasionale, poiché nascono già digitali e in quell'ecosistema si muovono, vengono scambiati e, infine, spesi per gli scopi più disparati.

Tutto ciò ha portato i legislatori a interessarsi ai comportamenti in grado di influire negativamente sulla salvaguardia dei sistemi informatici e sono stati così imposti (qui in termini imprecisi): vasti obblighi di conformità; complesse strutture organizzative di controllo e vigilanza; ampi poteri di ispezione e sanzionatori e numerose forme di cooperazione tra organismi dotati di poteri di vigilanza, non solo a livello nazionale.

A tutela delle infrastrutture informatiche è dispiegato un variegato arsenale e che vede sulla scena non solo l'autorità giudiziaria penale. Un ruolo di primo piano, infatti, è svolto da autorità amministrative: l'Autorità garante per la protezione dei dati personali (qui «Garante» o «Garante privacy») e, ultimo in ordine di tempo, l'Agenzia per la Cybersicurezza Nazionale (di seguito: «ACN»). L'ACN, a sua volta, è attratta in una strutturata rete di interazioni a livello europeo, fondate sul principio di "leale collaborazione" fra Agenzie e corpi di vigilanza.

In questo senso, il settore della cybersicurezza si inserisce appieno nella attuale era di prevenzione collaborativa, un frangente temporale in cui si accrescono i doveri di adeguamento in capo ai soggetti destinatari degli obblighi

[1] Per citarne uno di grande impatto, si pensi alla diffusione di immagini dal contenuto sessualmente esplicito all'insaputa delle malcapitate vittime, ovvero con commenti del tutto inappropriati, per usare un eufemismo.

derivanti dalla normativa di settore e, correlativamente, si moltiplicano le autorità di controllo, con immediato aumento dei loro poteri ispettivi, di vigilanza e sanzionatori.

A fronte di questo orizzonte a tinte chiaro-scure, il presente capitolo analizzerà ciascuno degli ambiti appena citati, alla ricerca di possibili implicazioni che il dispiegamento dei poteri amministrativi di vigilanza può avere nel procedimento penale e di come il ruolo crescente dei privati stia contribuendo a ridisegnare i modelli di accertamento. Sotto questo versante, vanno al tempo stesso considerate sia la severità delle sanzioni previste dalla più recente legislazione in materia di sicurezza informatica, sia il potenziale utilizzo dei dati raccolti durante le operazioni di ispezione e sorveglianza in sede amministrativa (di vigilanza) nel contesto processuale penale, ove alla violazione delle norme di sicurezza si accompagni una condotta perseguibile anche penalmente [2]. La pervasività degli strumenti di controllo riconosciuti all'ACN e alle sue varie componenti operative (ad esempio, il Computer Security Incident Response Team o CSIRT-Italia) pone con forza la questione del rispetto dei diritti dei soggetti

[2] Si tratta di tecnica legislativa non nuovissima, quella di devolvere ad autorità amministrative di vigilanza compiti ispettivi o, per certi versi, latamente investigativi e anche sanzionatori. Anzi, quello della sicurezza informatica è solo l'ultimo dei settori caratterizzati da questa prassi. Volendo citare almeno un altro campo in cui, in Italia, si sperimenta lo stesso approccio, si può pensare alla legislazione antimafia, d.lgs. n. 159/2011 (cfr., per esempio, la c.d. "informazione interdittiva antimafia", art. 84 ss. e, in particolare, l'art. 93).

In dottrina la produzione in argomento è amplissima, sia nel diritto amministrativo, sia in quello penale. Fra i molti contributi, si rinvia al recente V. MANES, *La resistibile ascesa della "prevenzione mite"*, in *Diritto di difesa*, al link: https://dirittodidifesa.eu/wp-content/uploads/2025/07/MANES-LA-RESISTIBILE-ASCESA-DELLA-PREVENZIONE-MITE.pdf; M. ARBOTTI, *Interdittive antimafia e prevenzione patrimoniale non ablativa: tra funzioni manifeste e latenti*, in *Diritto di difesa*, al link: https://dirittodidifesa.eu/wp-content/uploads/2025/08/ARBOTTI-INTERDITTIVE-ANTIMAFIA-E-PREVENZIONE-PATRIMONIALE-NON-ABLATIVA-TRA-FUNZIONI-MANIFESTE-E-LATENTI.pdf. Si veda poi E. BIRRITTERI, *L'eccezionalismo italiano nella lotta al crimine organizzato: vantaggi, insidie e prospettive della prevenzione antimafia "cooperativa"*, in *Arch. pen.*, 1, 2025; G. D'ANGELO-G. VARRASO, *Il decreto legge n. 152/2021 e le modifiche in tema di documentazione antimafia e prevenzione collaborativa*, in *Dir. pen. cont.*, 2, 2022, p. 12 ss.; F. GIACALONE, *Il nuovo volto dell'informazione antimafia dopo le novelle del D.L. n. 152/2021: verso la definitiva consacrazione del "diritto amministrativo dell'emergenza criminale"?*, in *Dir. econ.*, 2, 2023, p. 37 ss.; S. IPPEDICO, *Le interdittive antimafia tra collaborazione e contraddittorio: nuove contraddizioni?*, in *Cass. pen.*, 12, 2023, p. 4337 ss.; F. GIACALONE, *L'influenza eurounitaria sull'espansione del contraddittorio nei procedimenti amministrativi nazionali*, in *Dir. pubbl. europeo*, Rassegna online speciale, 1, 2024, al link: https://iris.unipa.it/retrieve/51266380-fa9f-4555-a262-61f8a8c03703/GIACALONE%20-%20DPE.pdf; M. MAZZAMUTO, *Profili di documentazione amministrativa antimafia*, in *Giust. amm*., 3, 2016. Sia consentito anche il rinvio a A. PUGLIESE-M. ZITO, *L'ultimo volto dell'interdittiva antimafia: una nuova forma di "compliance" amministrativa*, in *Arch. giur. Filippo Serafini*, 4, 2022, p. 967 ss.

sottoposti al controllo nei contesti amministrativi e, non meno importante, della possibile rilevanza e utilizzabilità dei dati così raccolti in eventuali procedimenti penali, qualora l'elemento fosse considerato utile.

Non per ultimo, come già accaduto in altri rami, all'orizzonte appaiono sempre più rilevanti, anche in questo settore, forme di partnership pubblico-private. Ambiti come quello dell'antiriciclaggio e dell'antiterrorismo già lo hanno sperimentato e, fra questi ultimi e quello della cybersicurezza v'è più d'una somiglianza. Su tutte: gli ampi doveri di segnalazione posti in capo ai soggetti sottoposti alla vigilanza delle autorità di settore e che spingono i privati verso nuove soluzioni [3].

Queste, in estrema sintesi, sono le sfide con cui deve rapportarsi anche l'interprete e nel presente capitolo, a seguito di una sommaria ricostruzione normativa – che toccherà i soli lembi legislativi utili all'approfondimento – si analizzeranno le prospettive, i rischi o i vantaggi che si stagliano all'orizzonte di questa lunga era di prevenzione collaborativa.

2. Quadro giuridico dell'UE e italiano in materia di cybersicurezza e Agenzia per la Cybersicurezza Nazionale (ACN): poteri di ispezione e di vigilanza

Alle fondamenta dell'odierno dibattito sulla sicurezza cibernetica, si pone la Direttiva NIS 1 (1148/2016) [4], recepita in Italia con il d.lgs. n. 65/2018 [5]. Non

[3] Sia consentito un rinvio a G. LASAGNI, *Public private partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?*, in *Dir. pen. contemporaneo*, rivista trimestrale, 3, 2021, p. 153 ss. Nello scritto si sosteneva, seppure per altri rami dell'ordinamento, e si è osservata «una crescente tendenza verso l'"esternalizzazione" delle funzioni di accertamento penale, tradizionale dominio della parte pubblica». Su questa stessa lunghezza d'onda, anche M. CAIANIELLO, *Poteri dei privati nell'esercizio dell'azione penale*, Torino, 2003. Per una analisi in ambito comparato, si veda B. VOGEL, *Reinventing Eu Anti-Money Laundering. Towards a Holistic Legal Framework*, in B. VOGEL-J.B. MAILLART (eds), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Intersentia, Cambridge-Antwerp-Chicago, 2020.

[4] Direttiva del Parlamento Europeo e del Consiglio relativa a misure per un elevato livello comune di sicurezza informatica in tutta l'Unione, che abroga la direttiva (UE) 2016/1148. A livello europeo, la cosiddetta direttiva NIS 1 (Dir. UE 1148/2016) è il primo atto legislativo dell'UE in materia di sicurezza informatica. La direttiva ha attuato la prima strategia dell'UE in materia di sicurezza informatica con l'obiettivo di rafforzare la sicurezza delle reti e dei sistemi informativi.

[5] La ricostruzione a seguire sarà mirata ai soli lembi legislativi più rilevanti e necessari per una corretta comprensione dell'argomento e terrà conto dell'attuale panorama legislativo, influenzato

occorre entrare nel merito dell'atto, sia perché non è specifico oggetto del presente contributo, sia in ragione delle evoluzioni legislative recenti, su tutte il recepimento della Direttiva 2555/2022 c.d. NIS 2 (d.lgs. n. 138/2024). Va detto, però, che il d.lgs. n. 65/2018 è stato solo il primo di una serie più articolata di provvedimenti e oggi rimane ancora un referente significativo per diversi dei principi che enuclea.

Oggi, con l'Agenzia per la Cybersicurezza Nazionale (istituita a mezzo del d.lgs. n. 82/2021), i poteri e le funzioni un tempo distribuiti tra diversi Ministeri si vedono confluiti in un unico organismo. Il recente recepimento della Direttiva NIS 2 (*ex* d.lgs. n. 138/2024), aumenta ulteriormente l'insieme delle funzioni preventive, investigative e sanzionatorie di questo organo. Riprendendo la bipartizione già presente nella Direttiva NIS 1, gli operatori di servizi essenziali sono stati invitati ad adottare misure adeguate e appropriate per gestire i rischi associati alla fornitura dei loro servizi, al fine di ridurre al minimo i rischi informatici connessi agli stessi (secondo il cosiddetto principio di minimizzazione del rischio). A questo proposito, è stato posto l'onere su tali operatori di notificare al CSIRT gli "incidenti" con un impatto significativo [6]. In estrema sintesi, si tratta di un quadro normativo che, per fasi, ambisce a coprire le reti e i sistemi informativi (e in ogni fase) da fattori esterni potenzialmente in grado di impattare negativamente sui primi e ciò include: obblighi strutturali, sino a quelli volti a ridurre al minimo i rischi, ovvero agli obblighi di notifica al CSIRT. Inoltre, già prima dei recenti interventi legislativi, il d.lgs. n. 65/2018 aveva conferito significativi poteri di ispezione alle autorità di vigilanza. Pertanto, i sottoposti al controllo potevano e possono incorrere in sanzioni amministrative significative, per le violazioni degli obblighi gravanti sugli stessi e non è escluso che la condotta non costituisca anche un reato, inasprendo ulteriormente il panorama sanzionatorio [7].

Di seguito al d.lgs. n. 65/2018, veniva promulgato il d.l. n. 105/2019, c.d. "Decreto Perimetro". L'atto ha rafforzato, tra l'altro, la risposta sanzionatoria nel settore della cybersicurezza, introducendo le sue violazioni tra quelle che

---

dal recente recepimento della direttiva NIS 2 (n. 2555/2022, per il tramite del d.lgs. n. 138/2024). Inoltre, si vedranno necessari alcuni brevi richiami alla l. n. 90/2024, sul rafforzamento delle infrastrutture informatiche e sull'apporto di modifiche sia al codice penale sia a quello di procedura penale.

[6] In argomento, appare utile la *guida alla notifica degli incidenti al CSIRT-Italia*, reperibile sul sito istituzionale dell'ACN e al link: https://www.acn.gov.it/portale/documents/20119/552690/ACN_Guida_Notifica_Incidenti_CLEAR.pdf/e7a1b3df-fac0-9b10-fb4d-c08be31061ad?t=1722593115655.

[7] Questa prospettiva è testualmente confermata dal d.lgs. n. 138/2024, che recepisce la direttiva NIS 2 e mantiene l'assetto così sommariamente evocato. Si tratta dell'art. 38 del d.lgs. n. 138/2024 e 34 della Direttiva NIS 2.

possono comportare una responsabilità per fatto di reato dell'ente [8]. Tra le disposizioni degne di nota ai fini della presente analisi vi è l'art. 1, commi 11 ss., sempre del Decreto Perimetro, nella misura in cui vengono introdotti delle fattispecie di reato, per coloro che ostacolano le attività di ispezione o di vigilanza (anche su richiesta di dati o metadati) [9].

Disposizioni simili, peraltro, sono stati oggetto di questioni di costituzionalità e legittimità in sede europea, in ambiti di accertamento affini, come quello finanziario (su cui si veda, più compiutamente, il par. 3).

L'ultimo provvedimento legislativo da menzionare è il d.l. n. 82/2021, che istituisce l'Agenzia Nazionale per la Cybersicurezza (ACN). Il decreto chiarisce il significato di "sicurezza informatica" nell'ambito dell'ordinamento giuridico italiano, ovvero «l'insieme delle attività (…), necessari[e] per proteggere le reti, i sistemi informativi, i servizi informatici e le comunicazioni elettroniche dalle minacce informatiche(…)». Gli obiettivi delineati rivestono notevole importanza e interesse per i massimi livelli di governo, in particolare per le responsabilità assegnate alla Presidente del Consiglio dei Ministri (o alla sua autorità delegata) e al Comitato Interministeriale, che la Presidente del Consiglio dei Ministri continua a presiedere. L'Agenzia è responsabile della salvaguardia della sicurezza e della resilienza nel cyberspazio, della prevenzione e della mitigazione del maggior numero possibile di attacchi informatici e della promozione del raggiungimento dell'autonomia tecnologica.

2.1. Gli incidenti cibernetici, gli obblighi di notifica e il potere investigativo di ACN

Cruciale nel sistema è quindi la definizione del concetto di «incidente». Stando alla definizione che ne dà la Dir. NIS 2 (art. 6) è «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi». Rientrano nelle «gestione degli incidenti», sempre secondo l'art. 6, «le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso». Al verificarsi di un incidente e, fra tutti, in presenza di «incidenti che hanno un impatto significativo» (art. 23 NIS 2, c.d. incidente significativo, e art. 25, d.lgs. n. 138/2024), sorge l'obbligo di segnalarli [10]. Prendono piede da questa segnalazione tutta una

[8] Intervenendo anche sul d.lgs. n. 231/2001 (art. 24-*bis*, comma 3).

[9] Citati anche nel d.lgs. n. 231/2001 (sempre art. 24-*bis*, comma 3).

[10] L'art. 25 del d.lgs. descrive come segue cosa debba intendersi per incidente significativo, ed è «considerato [tale] se: a) ha causato o è in grado di causare una grave perturbazione

serie di doveri d'accertamento in capo alle Autorità variamente interessate, fra le quali un ruolo di spicco va riconosciuto al CSIRT. La segnalazione è poi favorita da un costrutto normativo nient'affatto di agevole definizione, benché non nuovo alle "cronache" normative recenti.

Su tutto, fra i profili maggiormente significativi, il particolarissimo bilanciamento "costi-benefici" enucleato dalla normativa di settore. A scorrere la NIS 2 si intuisce bene l'incentivo alle segnalazioni. Da un lato, se anche se ne dovesse presentare una quando non sarebbe appropriato, non ne deriverebbero effetti pregiudizievoli [11], mentre, al contrario, chi dovesse omettere di segnalare quando invece avrebbe dovuto si espone a sanzioni di significativo impatto. Insomma, accedendo a un usurato parallelismo, si incentiva una medicina difensiva. Non è infatti un caso se, osservando l'ultima relazione annuale di ACN disponibile, tutti i parametri di riferimento siano in forte crescita. Solo ad osservare le notifiche, queste si vedono aumentate su base annua del 28% circa, le comunicazioni ricevuta da CSIRT dell'oltre 80%.

Si tratta di un trend già noto in altri ambiti. Il settore dell'antiriciclaggio ha già dato prova di impennate nelle segnalazioni, tanto che «[p]ur di non incorrere nelle sanzioni previste dalla normativa, sono sempre più numerose le (…) segnalazioni (…), anche in mancanza di adeguate verifiche o approfondimenti. L'uso difensivo delle [segnalazioni di operazioni sospette], altrimenti detto fenomeno degli *umbrella reports* (…)» [12] è talvolta accompagnato da una minore qualità delle "denunzie", ciò che rischia di annacquare il sistema, conducendolo, in alcuni casi, verso una faticosa battaglia contro i mulini a vento [13].

Forse è presto per giungere a soluzioni di questo tipo anche nello specifico ambito della cybersicurezza, ma non lo è abbastanza per non immaginare, in un futuro già alle porte, lo sviluppo di simili problematiche, tipiche di modelli in cui l'azione del privato assume preminenza nell'accertamento [14]. Anche l'opera degli attori pubblici si legherà al successo che i servizi a sostegno della

operativa dei servizi (…) b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche (…)». Si tratta di una descrizione che, per quanto vada migliorando nella lett. b) rimane pur sempre ancorata a giudizi di valore e ciò potrebbe suggerire, in via cautelativa, di denunciare anche quando, a ben vedere, non dovesse trattarsi di incidenti significativi.

[11] Vale a dire: sempre meglio una segnalazione in più che in meno.

[12] G. LASAGNI, *Public private partnerships*, cit. p. 157.

[13] Senza fine, come quella de Don Chisciotte nell'omonimo romanzo di Miguel de Cervantes.

[14] L'azione del privato prenderà presumibilmente piede anche dal punto di vista tecnico, per esempio con l'adozione di servizi volti a schermare i dati aziendali da attacchi esterni, ovvero, al tempo stesso, con l'obiettivo di raccogliere, se possibile, elementi utili per l'identificazione del profilo dell'attaccante. Ne sono esempio le tecniche di *cyber deception*. In questa opera, M. LANDOLFI, *Cybersicurezza* e *cyber deception: sfide e prospettive processualpenalistiche*.

sicurezza delle imprese saranno in grado di recare. Di per sé, si tratta di fenomeno del tutto compatibile con le disparate logiche aziendali. Seppure per il tramite di una semplificazione di certo imprecisa, si potrebbe finanche arrivare a dire che non v'è poi troppa differenza tra il lucchetto posto a presidio del cancello di ingresso alla fabbrica e la serie di chiavi informatiche poste a tutela dei sistemi aziendali. Ciò che muta, forse, è il contesto, l'ecosistema in cui i due approcci vanno calandosi. Solo in un caso, il secondo, quella difesa privata si iscrive in un crocevia di poteri statuali (e, ancor prima: interessi).

Il panorama diviene ancor più sfidante ove si consideri che l'art. 25, d.lgs. n. 138, nel declinare l'obbligo di segnalare gli incidenti di sicurezza informatica, ne sottolinea il potenziale collegamento con attività criminali e chiarisce il ruolo del CSIRT-Italia in questo tipo di casi: «[s]e si sospetta che l'incidente significativo sia di natura criminale, il CSIRT Italia fornisce inoltre alla parte notificante indicazioni sulla segnalazione dell'incidente (…)» alle autorità di contrasto (art. 25, comma 8). L'esito di un interessamento così ramificato e diffuso verso il medesimo fatto storico (l'incidente) accende l'interesse del processualista interessato a conoscere della formazione di elementi di prova poi, un giorno, spendibili anche in un futuribile processo penale, quello che dovesse prendere le mosse proprio dalle medesime condotte. Il timore, neppure troppo remoto, è che si dia vita a "un entità investigativa a più teste", il cui impatto può essere più significativo proprio quando si rifletta di far refluire le conoscenze acquisite altrove in possibili processi penali. Ciò rende doverosi i quesiti in punto di compatibilità con una acquisizione extraprocessuale diffusa di questo tipo e la spendita procedimentale del dato [15].

Prima di procedere oltre, dunque, si rende necessario analizzare i poteri di vigilanza che il d.lgs. n. 138/2024 ha riconosciuto all'ACN. L'obiettivo è quello di individuare, nella legislazione applicabile, le interazioni rilevanti tra le indagini amministrative (cioè quelle condotte dall'ACN) e i procedimenti penali, che potrebbero derivare dagli stessi fatti, se questi costituissero anche un reato ai sensi del diritto penale italiano. La domanda persistente è se gli elementi, gli atti, i documenti e le dichiarazioni raccolte dall'autorità amministrativa nel corso dei propri procedimenti – senza le tutele di un processo penale – possano essere utilizzati anche in quest'ultimo [16].

---

[15] Di nuovo, non è affatto un caso se fra i compiti d ACN, come descritti sul sito istituzionale, vi siano anche quelli afferenti alla «gestione rapporti con Autorità Giudiziaria, Polizia Giudiziaria e Direzione Nazionale Antimafia e Antiterrorismo [ciò che] assicura i rapporti di collaborazione (…)».

[16] *Ex* art. 34, d.lgs. n. 138/2024, «[l]'Autorità nazionale competente NIS monitora e valuta il rispetto da parte dei soggetti essenziali e dei soggetti importanti degli obblighi previsti (…), svolgendo attività di vigilanza attraverso: a) il monitoraggio, l'analisi e il supporto ai soggetti

Le rinnovate capacità investigative e i poteri sanzionatori, sempre più ampi, richiedono un esame approfondito proprio alla luce del recentissimo d.lgs. n. 138/2024. Il punto di partenza è l'art. 34 ss., che identifica i poteri ispettivi e di vigilanza dell'ACN. In primo luogo, la disposizione specifica i principi generali che regolano i poteri esecutivi dell'ACN: monitoraggio, verifica e ispezioni, adozione di misure di sicurezza e imposizione di sanzioni. Come si può dedurre dalla lettura di tali poteri, essi mostrano un crescente grado di afflittività, che copre l'intera gamma delle possibili attività ispettive, dalla prevenzione alle indagini vere e proprie e, quindi, all'irrogazione delle sanzioni. Questo aspetto chiarisce anche l'importanza di riflettere sulla portata concreta delle prerogative dell'ACN, data la gravità delle punizioni che possono essere irrogate. Inoltre, il terzo comma dell'art. 34 chiarisce la rilevanza dei poteri affidati all'ACN, introducendo i principi di «efficacia, proporzionalità e dissuasività» delle indagini in quella sede svolte. Ne consegue che l'esercizio delle prerogative ispettive si concretizza attraverso attività di una certa rilevanza, che assumono ancora più importanza se si considerano le possibili e non remote implicazioni. Vale a dire che dalle informazioni raccolte durante le indagini amministrative potrebbero emergere indizi di reato e, quindi, anche elementi utili alle indagini penali, che sarebbero così alimentate dai risultati delle ispezioni effettuate durante le indagini amministrative (di vigilanza). La questione diventa più delicata se si considera che alcune delle attività ispettive sono particolarmente invasive, sollevando seri dubbi sul rispetto dei diritti delle persone indagate.

Come ormai comune negli ambiti di accertamento ufficialmente o latamente punitivi, la semantica della legislazione in commento, poi, suggerisce come i legislatori europei e nazionali siano stati ispirati, almeno in parte, anche dal processo penale e dall'effetto dissuasivo solitamente associato alle sanzioni ivi previste. Ne è prova l'art. 34, comma 6, del d.lgs. n. 138, in cui si chiarisce che «[l]e attività e i poteri (…) sono rispettivamente svolti ed esercitati nel rispetto dei diritti della difesa e tenendo conto delle circostanze di ciascun caso (…)».

---

essenziali e (…) importanti; b) la verifica e le ispezioni; c) l'adozione di misure di esecuzione; d) l'irrogazione di sanzioni amministrative pecuniarie e accessorie». La questione ha già dato ampiamente da discutere in settori in parte affini, quali l'antiriciclaggio. Si guardi, ad esempio a Corte cost., ord. n. 117 del 10 maggio 2019 e poi a Corte di Giustizia, (Grande Sezione), 2 febbraio 2021, C-481/19. Numerosi, al tempo, gli interessamenti ermeneutici. Fra questi, A. LOGLI, *Nota a Corte costituzionale, 10 maggio 2019, n. 117*, in *Giurisprudenza commerciale*, 2, 2020, p. 230 ss.; S. CONFALONIERI, *Il nemo tenetur se detegere nel labirinto delle fonti. Riflessioni a margine di Corte Cost., ord. n. 117 del 2019*, in *Riv. trim. dir. pen. cont*., 1, 2020, pp. 108-140; M. ARANCI, *Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia. Nota a CGUE, sent. 2 febbraio 2021, C-481/19, Consob*, in *Sist. pen*., 2, 2021, pp. 73-98; ovvero, sia consentito il rinvio a G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la corte costituzionale conferma)*, in *Giurisprudenza commerciale*, fasc. 6, 2021, p. 1177 ss.

L'art. 36 del decreto, inoltre, funge da guida per le ispezioni individuali. La disposizione identifica quali tipi di attività investigative può svolgere l'ACN. Viene quindi chiarito in che modo l'Agenzia può ordinare, nell'ambito di applicazione del decreto: «a) verifiche della documentazione (…); b) ispezioni in loco e a distanza (…); c) richieste di accesso a dati, documenti e altre informazioni (…), indicando lo scopo della richiesta (…)». I poteri conferiti sembrano seguire un principio di tipicità quando si tratta di misure investigative. Tuttavia, data l'ampia portata degli stessi, diventa difficile definire chiaramente i limiti del potenziale coinvolgimento dell'Agenzia [17].

Peraltro, il suo esercizio in concreto può essere influenzato da una serie di fattori, tutti indicati nell'art. 34, comma 6, del decreto e fra i quali vengono in rilievo i presupposti che, aggravando la posizione del soggetto controllato, consentono parallelamente un aumento dei poteri dell'Agenzia. Tra queste circostanze, vanno menzionate quelle connesse a una sorta di recidiva («violazioni ripetute») e quelle connesse alla mancata collaborazione durante l'attività ispettiva («ostacolo alle attività di vigilanza (…)» e «fornitura di informazioni false o gravemente inesatte relative agli obblighi previsti dal presente decreto»). Infine, come regola di salvaguardia, «il livello di cooperazione delle persone fisiche o giuridiche ritenute responsabili dall'autorità NIS competente».

Quest'ultimo passaggio evidenzia diversi aspetti critici che devono essere esaminati. Innanzitutto, è opportuno chiarire in che misura uno scenario di attacco informatico possa costituire anche un'ipotesi di reato, ovvero un caso di responsabilità amministrativa, ma derivante da reato, delle società. Ipotesi penali rilevanti, per essere chiari, potrebbero essere quelle commesse da terzi non collegati alla struttura "sotto attacco". Ciò riflette la logica alla base non solo del d.lgs. n. 138, ma pure della l. n. 90/2024, che ha modificato anche il codice penale, inasprendo o inserendo reati specifici in materia, nessuno dei quali, tuttavia, è di natura colposa. Poiché i delitti contestati sono dolosi, il legislatore intenderebbe punire comportamenti tenuti da soggetti esterni alla compagine o all'amministrazione oggetto di attacco informatico. Tuttavia, come insegna anche l'esperienza con l'art. 615-*ter* c.p. sul tema dell'accesso non autorizzato a un sistema informatico, ciò non costituirà la totalità dei casi possibili. Certamente si verificheranno attacchi compiuti da un "intraneus" alla persona giuridica che appare sotto attacco. Le valutazioni di cui sopra, per ciò solo, però, non

[17] Sul punto, poi, va ulteriormente rimarcata la circostanza che, in una prima fase, queste attività vengono poste in essere in sede amministrativa (di vigilanza). Dalla prospettiva del processo penale, i limiti di criticabilità di un'eventuale azione ispettiva "irregolare" sono davvero stretti e, al massimo, rileverebbero sotto il profilo della violazione del diritto al silenzio. Fuori da ipotesi di questa natura, non parrebbe invocabile una generica e per questo non tassativa (come invece pretenderebbero le invalidità processuali penali) irregolarità acquisitiva, specie se dovesse ricadere su fonti documentali (*infra*, parr. 3.2; 4).

cambiano la fisionomia della legislazione. Quindi, almeno formalmente, sarà comunque richiesta la massima cooperazione a chi, oltre ad essere, in ipotesi, soggetto apicale dell'ente, rischi pure di ritrovarsi indagato [18]. Il contesto così delineato può influire sulla formazione degli elementi istruttori, ampiamente intesi e in ogni sede, favorendone l'emersione anche quando sarebbe lecito che il sottoposto opponesse un rifiuto a collaborare. Se si osserva il fenomeno in altri settori del sistema giuridico, peraltro, l'intuizione sembra confermata.

Alcune brevi osservazioni possono servire a illustrare la realtà così come si presenta oggi all'osservatore interessato a comprendere i punti di contatto fra l'ambito amministrativo e quello penale. Sempre più settori, in cui i rischi sembrano essere numerosi, continuano a orientarsi verso una logica partecipativa nelle procedure di accertamento di natura amministrativa. L'esempio più eclatante – oggi – è la normativa antimafia, il d.lgs. n. 159/2011, come da ultimo modificato dal d.lgs. n. 152/2021 [19]. I punti di contatto con la cybersicurezza sono molti e alcuni accenni sono necessari. In primo luogo, la delicatezza dell'area coperta dalle rispettive discipline. La cybersicurezza pone la sfida di mantenere numerosi interessi, e tutti contemporaneamente: (i) l'ordine costituzionale, di fronte al timore di attacchi dolosi; ma anche (ii) l'ordine economico, a causa della capacità di infiltrarsi in questo e alterarne l'equilibrio e, infine, (iii) i diritti dei cittadini, compreso il diritto alla protezione dei dati personali, esposti nel tumultuoso mondo di Internet, a sua volta afflitto dai temuti attacchi informatici.

Di fronte a queste preoccupazioni, come verrà discusso più dettagliatamente nelle sezioni seguenti, i legislatori europei e nazionali hanno quindi ideato un sistema articolato di prevenzione e controllo, in cui sono coinvolte diverse autorità: l'autorità giudiziaria, l'autorità per la sicurezza informatica e, non per ultimo, l'autorità competente per la protezione dei dati personali.

A tal proposito, appare nuovamente utile un confronto con le norme antimafia. Anche alla luce delle più recenti modifiche alla normativa in materia di lotta alla criminalità organizzata (d.lgs. n. 152/2021), è possibile trarre alcuni spunti utili, sebbene con le dovute distinzioni. Si configura, infatti, una tripartizione

---

[18] Ponendo questioni simili a quelle che già si pongono rispetto all'incompatibilità a testimoniare del "nuovo" rappresentante dell'ente. Si veda art. 44, d.lgs. n. 231/2001 e la dottrina formatasi in merito, tra cui G. VARRASO, *Il "compromesso" delle sezioni unite in tema di costituzione ed esercizio dei diritti difensivi dell'ente "incolpato" nel procedimento*, in *Cass. pen.*, fasc. 1, 2016, p. 73.

[19] Cfr. M. VULCANO, *Le modifiche del decreto-legge n. 152/2021 al codice antimafia: il legislatore punta sulla prevenzione amministrativa e sulla compliance 231 ma non risolve i nodi del controllo giudiziario*, in *Giur. pen. web*, 2021, 11, p. 11; G. D'ANGELO-G. VARRASO, *Il decreto legge n. 152/2021 e le modifiche in tema di documentazione antimafia e prevenzione collaborativa*, cit.; e anche A. PUGLIESE-M. ZITO, *L'ultimo volto dell'interdittiva antimafia: una nuova forma di compliance amministrativa*, cit.

dell'esercizio del potere repressivo in senso astratto, sia in ambito antimafia che in materia di cybersecurity. Se si guarda alla legislazione antimafia, si possono individuare una serie di possibili interventi: in ambito penale, per i comportamenti che sfociano nel reato; in ambito amministrativo, come misura cautelare estrema e con lo scopo di evitare l'infiltrazione criminale nel tessuto economico (la cosiddetta informazione interdittiva antimafia, che ha l'effetto di colpire con una incapacità giuridica temporanea e parziale l'impresa); in ambito preventivo, con riferimento alle misure di prevenzione, la cui competenza spetta tuttavia al giudice penale, sezione misure di prevenzione, e che ha invece il compito di condurre la società fuori dalla palude mafiosa in cui rischia di impantanarsi. È utile notare che i controlli effettuati dall'ACN e i poteri conferitigli dalla legge non sono molto diversi. Anch'essi sono caratterizzati da un collegamento con il processo penale ogni volta che si verifica un reato; sono caratterizzati da ampi poteri preventivi, esercitati attraverso attività di monitoraggio e supervisione; e, non da ultimo, da reali poteri repressivi in ambito amministrativo anche attraverso il ricco e severo sistema sanzionatorio. Questa breve sintesi delinea il rapporto tra le indagini in campo amministrativo, le questioni di cybersicurezza e le loro potenziali implicazioni procedurali penali, sulle quali si tornerà nel par. 4.

La questione deve riguardare l'identificazione del momento oltre il quale sarebbe necessario acquisire prove che abbiano già la garanzia del codice di procedura penale. E ancora, occorre riflettere attentamente sulla funzione repressiva delle sanzioni che possono essere imposte dall'ACN nei casi in cui il soggetto controllato eluda o non collabori alle ispezioni. Ciò può porre la parte controllata di fronte a un difficile bivio, già emerso in altri settori: collaborare e rischiare di testimoniare contro se stessi o non collaborare e affrontare sanzioni più severe?

Ciò, però costituisce solo una faccia della medaglia. L'altra attiene a ciò che accade puramente nella sede amministrativa ma che, di nuovo, in un futuro, potrà pure avere rilevanza per un accertamento penale. La prevenzione collaborativa, come si diceva, non è solo nel rapporto tra controllore e controllato, ma pure fra le Autorità coinvolte, nel contesto europeo, dalla tutela dei sistemi informatici e, non per ultimo, nei possibili rapporti funzionali che potranno crearsi con le realtà private.

3. Raccolta e scambio di dati e informazioni nelle attività di vigilanza: tra public-private partnerships e cooperazione fra Autorità. Introduzione

Si tratta di un tema fra i più sfidanti dell'intera disciplina e comprende almeno due versanti di ricerca. Il primo emerge direttamente dalla legislazione di

settore e riguarda la cooperazione tra le numerose autorità astrattamente coinvolte nel campo della cybersicurezza. Il secondo, invece, seppure immediatamente non percepibile [20], risulta essere l'esito prevedibile delle pretese che l'ordinamento oggi pone in carico ai privati interessati dell'adeguatezza cibernetica: una cooperazione pubblico-privata anche ai fini investigativi.

Le due tipologie di cooperazione mantengono una fisionomia ben distinta, almeno in principio, e possono pure condurre a considerazioni di diversa natura. Quella fra autorità, per esempio, pone oggi sfide significative soprattutto con riguardo alle possibili triangolazioni fra i molteplici organi che, nei singoli Stati membri, assicurano il rispetto della legislazione eurounitaria nell'ambito della sicurezza dei sistemi informatici. Da un lato, ciò pone questioni sulla efficacia delle forme di cooperazione; dall'altro, più il sistema è efficace, più si rischia di esacerbare la asimmetria informativa fra autorità pubbliche e soggetti sottoposti ad accertamento – il che, quando l'accertamento lambisce o si tramuta in indagine penale, è ovviamente un versante alquanto sensibile. Nel caso della cooperazione pubblico-privata, invece, i principali dubbi riguardano innanzitutto la opportunità di stabilire forme di partenariato pubblico-privato che, come si dirà, sempre più si identificano in forme di esternalizzazione di attività di indagine.

Le differenti prospettive consigliano di trattare separatamente i due volti della medaglia.

3.1. Cooperazione fra le autorità

In merito alla cooperazione tra autorità, questa va intesa come almeno di due tipi: (i) interna al singolo ordinamento e fra organismi impegnati in ambiti apparentemente diversi ma accomunati da alcuni scopi comuni di vigilanza; (ii) esterna al singolo Stato e calata in un più ampio contesto europeo o internazionale.

In entrambi i casi, il principio guida di settore si rinviene nell'art. 14 [21] del d.lgs. n. 138, il quale elenca la gamma di possibili coordinamenti tra chi sia potenzialmente incaricato di "investigare" sugli attacchi informatici e delinea un particolarissimo scenario per le aree amministrative interessate dalle ispezioni, alludendo a un complesso meccanismo di sorveglianza, con diversi attori

[20] O nascosto nelle maglie della NIS 2, al Considerando n. 55, ai sensi del quale «[i] partenariati pubblico-privato (PPP) nell'ambito della cibersicurezza possono fornire il quadro appropriato per lo scambio di conoscenze (…). I PPP possono sfruttare le competenze dei soggetti del settore privato per assistere le autorità competenti nello sviluppo di servizi e processi all'avanguardia, compresi, lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza».

[21] Non solo questa norma. Si vedano anche, ad esempio, gli artt. 15, 17, 18, 20, 39.

coinvolti. Ciò modella in modo specifico i connotati del sistema, che finisce per rassomigliare – anche solo sul piano interno – a un cane a tre teste: l'ACN con il suo braccio operativo, il CSIRT; la magistratura e, non da ultimo, l'Autorità garante per la protezione dei dati personali [22].

È fondamentale ricordare che, ai sensi dell'art. 15 del d.lgs. n. 138, il CSIRT Italia può instaurare rapporti di cooperazione con i team nazionali di risposta agli incidenti informatici di paesi dell'UE. Nell'ambito di tali rapporti di cooperazione, questo organo «facilita uno scambio di informazioni efficace, efficiente e sicuro con [i] CSIRT nazionali (…), utilizzando i protocolli di condivisione (…). Il CSIRT italiano può scambiare informazioni rilevanti con i team nazionali di risposta (…) di paesi terzi (…), compresi i dati personali (…)».

Si delineano quindi, nella normativa di settore, una serie di nuovi equilibri, che ancora non trovano, spesso, adeguati riscontri in ottica processuale. L'ordinamento interno, infatti, si è perlopiù interessato di normare l'afflusso di elementi utili e raccolti in sede amministrativa di vigilanza, ma non si è ancora spinto sino ad immaginare, dalla prospettiva di una indagine penale, di potere eventualmente acquisire elementi raccolti secondo uno schema "diagonale" di collaborazione fra autorità penali e autorità amministrative di settore e di diverse nazioni [23].

In linea tendenziale, pertanto, quando un procedimento penale deve alimentarsi anche di elementi probatori esteri, lo fa secondo schemi tendenzialmente orizzontali e che, a seconda dei casi, si poggiano o sulle norme in tema di rogatoria, oppure, in ordine ad attività investigative europee, all'Ordine Europeo di Indagine; con l'unica eccezione, limitata però al suo ristretto ambito di azione, del meccanismo di cooperazione diagonale in cui si muove l'Ufficio europeo per la lotta antifrode (OLAF) [24].

Più specificamente, da un lato, la norma generale cui tipicamente si demanda il compito di disciplinare il contatto fra accertamenti in sede amministrativa e

---

[22] *Ex* art. 14, comma 2, d.lgs. n. 138/2024, «[a]i fini della cooperazione e della collaborazione (…) l'Autorità nazionale competente NIS coopera con il Garante per la protezione dei dati personali (…) nei casi di incidenti che comportano violazioni di dati personali (…)».

[23] Va subito precisato che ciò non significa che non vi siano, o non vi possano essere, dei protocolli fra autorità relativi allo scambio di informazioni; qui si intende solo dire che il codice di rito italiano non interviene in punto di regola acquisitiva di documenti che la P.A. italiana dovesse ricevere da altra amministrazione europea, per poi venire introitata in un procedimento penale italiano.

[24] Sull'argomento, anche a livello della sua effettiva applicazione in altri Stati UE, si vedano i risultati del recente progetto di ricerca FACILEX (sito: https://site.unibo.it/facilex/en), i cui risultati sono compendiati in G. LASAGNI-M. CAIANIELLO-G. CONTISSA, *Facilitating Judicial Cooperation in the EU A Computable Approach to Mutual Recognition in Criminal Matter*, Brill, 2024, al link: https://brill.com/edcollbook-oa/title/70688?srsltid=AfmBOorfB5gDZpGu7ZIqs0hDtRGE382P8DnylL26QzmPk945vm0aHyzu.

indagini penali, ossia l'art. 220 disp. att. c.p.p. (che si tratterà in seguito, par. 4.), ha pur sempre un ambito territoriale ben definito: si applica entro i confini della Repubblica e non immagina, almeno non come ipotesi generale, di potere applicarsi anche allo scambio di informazioni fra Amministrazioni di più Stati [25].

D'altro canto, le normative di settore, che spesso delineano alcuni tratti dello scambio di informazioni fra autorità (spesso, fra autorità amministrative e penali) sono estremamente eterogenee e raramente si spingono a definire anche profili essenziali come quelli della ammissibilità o utilizzabilità in giudizio. L'ambito della cybersicurezza conferma questa tendenza, con gli artt. 15 e 34 del d.lgs. n. 138 e l'art. 32 della NIS 2, che, appunto, non contengono regole specifiche riguardo l'ammissibilità nel processo penale degli elementi raccolti eventualmente anche a seguito di scambi di informazioni fra amministrazioni di più Stati.

È in questo contesto che l'apporto conoscitivo rappresentato dai "dati", con la loro valenza potenzialmente pluriespressiva (notizia di reato, elemento di prova, prova), mette in crisi i modelli di cooperazione tradizionali. Detto altrimenti, in mancanza di disposizioni esplicite sul tema, i dati raccolti dalle autorità italiane di cybersicurezza possono essere utilizzati se sono stati richiesti legittimamente ad altre autorità europee nell'ambito della cooperazione speciale prevista dal decreto 138?

La risposta sembra essere affermativa, per lo meno alla luce del quadro normativo attuale. Da un lato, nell'ambito di vigilanza amministrativa, lo scambio di informazioni è supportato dalla base giuridica vigente, senza che si pongano particolari questioni in termini di utilizzabilità all'interno di quel contesto.

Dall'altro, naturalmente, molto più problematica è la situazione in cui tali informazioni finiscano in un fascicolo di indagine penale. La pronta disponibilità del dato istruttorio, infatti, lo rende appetibile per l'Autorità giudiziaria e ciò ottimizza le opportunità di indagine per le Procure che dovessero intervenire a seguito dell'interessamento dell'ACN [26].

---

[25] Semplificando, secondo l'art. 220 disp. att. c.p.p. quando nel corso di attività amministrativa di vigilanza dovessero emergere indizi di reato, gli ulteriori elementi di prova dovrebbero essere raccolti secondo le prerogative di cui al codice di procedura penale. La regola di garanzia, però, è ovviamente pensata per le amministrazioni italiane, non potendosi imporre alcun obbligo a quelle straniere. Ne deriva che per le volte in cui si sostenga sempre più una cooperazione trasversale, a livello amministrativo e fra più Stati, maggiori sono i rischi dell'inutilità della disposizione. Diviene sempre più probabile che quegli elementi, nella cooperazione fra autorità amministrative, giunga fino in Italia e, a quel punto, siano acquisiti sotto forma di documenti nell'ambito di una indagine preliminare (penale). Sul punto, par. 4.

[26] G. Lasagni, *Cooperazione amministrativa e circolazione probatoria nelle frodi doganali e fiscali*, in *Dir. pen. cont*., 2015, https://archiviodpc.dirittopenaleuomo.org/upload/1442824408LASAGNI_2015a.pdf.

Al contempo, i meccanismi tradizionali di tutela, come l'art. 220 disp. att. c.p.p. sono spesso di dubbia applicabilità. In primo luogo, potendosi dubitare della eventualità di conferire qualifica di p.g. alla amministrazione che per prima raccoglie i dati (su cui, si veda nel dettaglio in seguito par. 4). In secondo luogo, considerando che, specie nell'ambito di cui si discute, l'emersione di notizie di reato può essere anche successiva alla indagine su un singolo incidente (ad esempio, emergendo solo a seguito del riscontro di una pluralità di attacchi informatici, magari organizzati) – vanificando in radice l'obiettivo del meccanismo previsto dall'art. 220.

A ciò si aggiungono le disposizioni di cui al d.lgs. n. 138/2024 che, avendo carattere speciale, come indicato, non pongono particolari restrizioni alla circolazione delle informazioni raccolte. Peraltro, le stesse coordinate del codice di procedura penale [27] non vietano e, in certa misura, anzi supportano, almeno sul piano testuale, l'acquisizione dei dati comunque detenuti presso le pubbliche amministrazioni italiane, anche se, a loro volta, fossero stati acquisiti per il tramite di una collaborazione interna agli enti amministrativi con i loro corrispettivi esteri.

Diverse disposizioni mostrano difatti una apertura verso la raccolta dei dati, senza prestare eccessiva attenzione al percorso che li ha resi disponibili. A titolo di esemplificazione, muovono in questo senso gli artt. 234 e 234-*bis* c.p.p., così come la serie di disposizioni sui sequestri, che possono essere pure eseguiti presso amministrazioni dello Stato [28]. Un limite, certo non invalicabile, si rinviene nell'art. 242 c.p.p., che suggerisce un onere di traduzione dell'atto redatto in lingua diversa dall'italiano, se e in quanto necessario, ma che difficilmente si può trasformare in una regola di esclusione probatoria vera e propria [29].

Infine, va pure ricordato che, ai sensi dell'art. 235 c.p.p., è sempre ammessa l'acquisizione di documenti costituenti corpi di reato, a prescindere da chi li detenga e non è uno scenario inverosimile in relazione ad accertamenti di questo tipo.

---

[27] Va ammesso che, in relazione alla velocità delle innovazioni in campo informatico, il codice può essere considerato particolarmente risalente e diversi dei temi qui dibattuti non involsero le riflessioni del legislatore processuale del 1988/89. Nel corso del tempo si è tentato di adeguare il codice alle innovazioni imposte dall'avanzare dell'informatica, ma resistono difficoltà ontologiche e gli ultimi approdi in tema di cybersicurezza comprovano l'assunto. Si assiste, verrebbe da dire, ad una "fuga dalle codificazioni", supportata dalla necessità di disporre di una legislazione sempre aggiornata e dalla corrispondente difficoltà all'adeguamento costante di una struttura complessa come un codice (per sua natura un complesso di norme stabili, in teoria).

[28] Per non parlare del caso in cui il dato è conservato da un privato, su cui si veda la disposizione ampia dell'art. 234-*bis*, così come il recente strumento dell'Ordine di produzione europeo.

[29] Cass., Sez. III, sentenza n. 18136 del 14/05/2025, in argomento, ha recentemente affermato come «[a]ltrettanto infondata appare l'ulteriore eccezione di nullità, proposta con riferimento alla mancata traduzione, dal francese, del verbale di accompagnamento (…) è stata la stessa difesa (…) a sottolineare e a lamentare il carattere meramente formale di quella attestazione di regolarità, con ciò dimostrando di aver ben compreso il contenuto dell'atto non tradotto (…)».

Nell'ambito specifico della cybersicurezza, difatti, in ipotesi, la certificazione di un incidente ad opera del CSIRT potrebbe costituire corpo del reato, così come lo costituirebbe se, per ricostruire lo stesso attacco informatico, la stessa autorità abbia richiesto e ottenuto certificazioni analoghe a un ente corrispettivo presente in altro Stato Membro.

In conclusione, guardando alla tendenza del sistema e alla normativa di settore, si può affermare che i verbali delle operazioni dello CSIRT, poste in essere al di fuori del contesto processuale penale, nasceranno in forma documentale; in questa categoria saranno collocati e, presumibilmente, in quanto tali verrebbero acquisiti al procedimento, con buona pace delle perplessità che potrebbero derivare dalle difformità negli standard acquisitivi.

3.2. Cooperazione pubblico privata

Sull'altro fronte, il crescente dovere di adeguamento di quanti siano sottoposti alla legislazione in materia di cybersicurezza, nonché l'altissimo grado di tecnicismo connesso, conduce inevitabilmente gli attori privati, da un lato, ad essere sempre più coinvolti nel processo di accertamento e, dall'altro e di conseguenza, a innalzare il livello di competenze (giuridiche e tecniche).

Il miglioramento delle loro performances è anche direttamente connesso all'evitare di incorrere in sanzioni rilevanti. Come si è osservato (*supra*, parr. 1 e 2), i soggetti sottoposti alla "giurisdizione" dell'ACN debbono dar prova di aver costruito una struttura "resiliente" [30] contro attacchi esterni, ma pure reattiva, ove non si riuscisse a porre freno a fenomeni intrusivi.

In entrambi i casi, è verosimile che, come in altri ambiti, fra cui il già citato AML/CFT, ciò induca il privato a mettere insieme diverse capacità para-investigative, che possano proteggerlo sia dagli attacchi, sia da possibili sanzioni connesse ad eventuali e riscontrate inefficienze.

Si tratta proprio del meccanismo alla base delle Public-Private Partnerships (PPP), sia in ottica preventiva, sia, in modo molto più controverso, repressiva. La cybersicurezza, infatti, è un settore che trova il proprio punto di forza nel naturale affidamento verso i privati di talune attività investigative, in particolare quelle di raccolta di informazioni su possibili attività sospette [31]. Il quesito di

[30] È poi fra i fattori che, già dagli anni '80, ha guidato prima la nascita e poi lo sviluppo delle Public-Private Partnerships. Si veda per questo, S.J. COLLIER-A. LAKOFF, *The vulnerability of vital systems: How critical infrastructure became a security problem*, in M.D. CAVELTY-K.S. KRISTENSEN (eds), *Securing 'the homeland': Critical infrastructure, risk and (In)security*, Routledge, London, 2008, p. 17.

[31] È poi un tema che la NIS 2 affronta direttamente nel Considerando n. 55), auspicandone la loro diffusione. In tema di PPP, più in generale, si veda B. VOGEL, *Reinventing Eu Anti-Money*

fondo, in relazione ai dati di cui le autorità pubbliche dovessero venire a conoscenza per il tramite di queste partnerships, è quindi riassumibile schiettamente in questi termini: si tratta di una via per aggirare le prerogative processuali? [32]

Sul punto, può essere utile anche tracciare una linea di demarcazione ideale fra le tipologie di PPP ipotizzabili, così come ricostruite dalla dottrina. Due vengono qui in rilievo: (i) una preventiva, c.d. compliance PPP e una (ii) puramente investigativa [33].

Circa la prima, che mira a definire meglio i confini del fenomeno illecito, come la definizione di "incidente", bisogna evitare di cadere in un facile fraintendimento: a fenomeni nei fatti diversi non sempre corrispondono differenziate categorie del diritto. Con ciò si intende dire che le azioni a tutela dei sistemi informatici, in certa misura, non sono poi troppo diverse da quelle che un privato pone in essere a tutela della sua persona e dei suoi interessi. Impianti di videosorveglianza, registrazioni di colloqui in presenza, fotografie, allarmi, investigatori privati segnano già molti procedimenti penali, pure trattandosi di dati nati privatamente, altrove e per fini preventivi. Insomma, va detto che la conoscenza privata non è respinta dal processo e anzi, molte volte l'accertamento di penale responsabilità si fonda su elementi "portati" dal privato. Per questa ragione, si farà fatica a impedire l'acquisizione al processo penale di dati e documenti che il privato avrà formato nel corso delle azioni messe in essere per dar seguito a doveri di compliance aziendale oppure per prevenire rischi specifici del settore merceologico considerato [34]. In questa direzione, a ben vedere, si muove il legislatore europeo, nella misura in cui ritiene che questi

---

Laundering. Towards a Holistic Legal Framework, in B. VOGEL-J.B. MAILLART (eds), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Intersentia, Cambridge-Antwerp-Chicago, 2020, p. 881; ovvero, più ad ampio raggio, B. VOGEL-E. KOSTA-M. LASSALLE, *Law of public-private cooperation against financial crime developing information sharing to counter money laundering and terrorism financing*, United Kingdom, 2024.

[32] Si è già detto più volte nel testo ma è bene ripetere che queste valutazioni sono vere nella misura in cui si dovesse poi approdare a un processo penale. Detto altrimenti, è interesse dello scritto comprendere se, per le volte in cui un attacco cibernetico dovesse costituire anche un'ipotesi di reato, gli elementi raccolti nella sede amministrativa siano spendibili in quella penale e, se sì, a quali condizioni.

[33] B. VOGEL, *Reinventing Eu Anti-Money Laundering*, cit.

[34] Resta in disparte la questione della reale libertà del privato di autodeterminarsi nel mettere insieme le azioni di adeguamento richieste dalla normativa. Come si è già notato in altro scritto, «la partecipazione dei privati a questi meccanismi, così come la condivisione di informazioni specifiche, può essere infatti considerata volontaria solo su un piano formale ed astratto. Nella pratica, invece, l'adesione degli operatori finanziari è spesso fortemente condizionata dalla necessità di mostrarsi cooperativi (…)». Così in G. LASAGNI, *Public private partnerships*, cit., p. 158.

meccanismi di cooperazione possano essere sfruttati dalle autorità, anche al fine di facilitare «lo scambio di informazioni, i preallarmi, le esercitazioni su minacce e incidenti informatici, la gestione delle crisi e la pianificazione della resilienza» (considerando 55, NIS 2).

Diverso è il caso delle PPP con finalità investigativa, di fatto richieste o indotte al privato dalle autorità di controllo e riferite a incidenti specifici. Qui la conoscenza da parte degli organi pubblici della possibilità del privato di svolgere delle indagini può fare la differenza sul piano dell'accertamento e presentare profili innovativi e non regolamentati di acquisizione delle informazioni. L'individuazione delle informazioni rilevanti da parte del privato, infatti, certamente costituisce un vantaggio per l'autorità di controllo, che potrebbe risparmiare risorse per perseguire i propri obiettivi.

Tuttavia, la esternalizzazione delle attività di indagine rischia di bypassare tutte le garanzie procedimentali che le autorità di contrasto dovrebbero altrimenti rispettare nella acquisizione delle informazioni (quelle penali ad un livello più alto, quelle amministrative ad un livello minore, ma sempre più assimilabile a quello penale, specie se dotate di poteri punitivi).

In siffatti frangenti, si può quindi seriamente dubitare della compatibilità di simili modelli acquisitivi e della relativa spendita nel contesto processuale penale degli elementi ottenuti, perlomeno se la azione del privato può essere considerata come determinata dalle richieste (dirette o indirette) delle autorità pubbliche. In questo senso, vengono qui in rilievo, nei termini che si vedranno nel paragrafo subito di seguito, l'art. 220 disp. att. c.p.p. e in generale tutte le garanzie procedurali previste per le fasi dell'accertamento.

Diversamente, laddove il privato agisse di propria iniziativa, anche ove strutturasse sistemi misti, preventivi e investigativi, il panorama muterebbe. Possono esserne un esempio alcuni meccanismi a tutela di eventuali accessi abusivi ai sistemi informatici, come per esempio nell'ambito della *cyberdeception* [35]. Si potrebbe pensare a strutture volte ad intercettare il tentativo di accesso, in grado tuttavia di approntare una difesa contro simili fenomeni e capaci anche di raccogliere dati utili per individuare l'attaccante. La relazione tecnica – privata – che dovesse uscire fuori dalla elaborazione dei dati raccolti dal sistema di difesa potrà certamente corredare, in ipotesi, una denuncia e così entrare nel procedimento penale [36].

---

[35] V., in quest'opera, M. LANDOLFI, *Cybersicurezza e cyber deception: sfide e prospettive processualpenalistiche*.

[36] Con il limite delle attività c.d. provocatorie. Detto altrimenti, alcuni sistemi possono finanche "attrarre" possibili attaccanti, fingendosi vulnerabili e invece ingabbiando il soggetto agente. Il tema, peraltro, è stato recentemente affrontato in giurisprudenza, si veda Cass. Pen., sez. II, n. 10934/2024, ove si è affermato, in linea di continuità rispetto a quanto qui sostenuto, che «[i]nfine,

In questa direzione parrebbe muoversi, come si è visto, anche il legislatore europeo, nel Considerando 55 della NIS 2, incentivando forme di cooperazione pubblico-privata a fini preventivi, così allo stato appare nelle maglie della disposizione europea. Il problema, però, è che risalire alle ragioni che hanno spinto all'azione il privato è tutt'altro che un compito facile, specie in sistemi di cooperazione fluidi e ad alto tasso di informalità, che caratterizzano le Public-Private Partnerships.

4. Art. 220 delle norme di attuazione del codice di procedura penale, atti investigativi misti e comparsa degli indizi di reato

Lo si è visto: le attività amministrative hanno un ruolo da "comprimario" nell'accertamento di talune condotte in contrasto con l'ordinamento. Tuttavia, l'azione del cittadino non rimane necessariamente confinata alla sfera dell'illecito amministrativo. Ciò è particolarmente vero se si considerano le ultime frontiere a cavallo tra sicurezza nazionale, cybersicurezza e violazioni penalmente rilevanti.

Sinora si è data ampia prova di come la criminalità informatica sia oggi il confine più sensibile della società contemporanea. Resta da esaminare un tema, quello del confine, non sempre netto, fra accertamento amministrativo e di natura penale.

Il codice di procedura penale contiene una disposizione alla quale vorrebbe delegare il compito di gestire il difficile passaggio delle prove dal quadro amministrativo, dove talvolta vengono inizialmente raccolte, al contesto processale penale.

La norma in questione è l'art. 220 disp. att. c.p.p. All'origine, la disposizione, occupandosi dell'emergere di indizi di reato in procedimenti extra-penali, sembrava in grado di fornire una risposta completa a tutte le istanze di garanzia che interrogavano la dottrina e la giurisprudenza [37]. Sembra tuttavia che non abbia raggiunto il suo obiettivo, almeno stando agli accesi dibattiti che ancora oggi circondano il tema [38].

---

corretta è la soluzione giuridica relativa alla inapplicabilità, al caso di indagini interne condotte nell'ambito di attività ispettive, dell'art. 220 disp. att. c.p.p. Affinché le cautele ivi previste siano applicate, è necessaria (…) la natura pubblicistica del rapporto tra dichiarante ed esercente la funzione (…)».

[37] Cfr. R.E. KOSTORIS, "*Sub art. 220*", in E. AMODIO-O. DOMINIONI (a cura di), *Commentario del nuovo codice di procedura penale, Appendice*, Milano, 1990, p. 74. Cfr. anche, nella giurisprudenza, Corte Cost., n. 86 del 1968; nn. 148, 149 del 1969; n. 248 del 1983; n. 15 del 1986; n. 330 del 1990.

[38] Si veda, di recente, Cass. Pen., sez. III, n. 43996/2023, ovvero Cass. Pen., sez. III, n. n.

D'altra parte, non potrebbe essere altrimenti se si considera che la questione riguarda diversi fronti del procedimento penale, forse i più importanti e rappresentativi: tutela dei diritti della difesa e dell'efficacia repressiva dell'azione penale. La disposizione si muove in un contesto particolarissimo, ove è ad un tempo probabile che alcuni degli atti compiuti dagli organi amministrativi abbiano anche un valore utilizzabile nei procedimenti penali, nel mentre però emergendo degli indizi di reato.

In breve, può accadere che ciò che viene prodotto in un altro ambito (quello amministrativo) abbia, in realtà, anche un certo valore probatorio (in termini impropri, data la fase) in sede penale. L'affermazione precedente può anche riflettere un risultato fisiologico derivante dall'efficacia delle attività di controllo e di vigilanza svolte dai funzionari pubblici [39]. Tuttavia, può anche accadere che il funzionario della PA, nel corso delle ispezioni, si avveda dell'emersione di uno o più indizi, ciò che accende l'interesse del legislatore processuale, interessato a disciplinare il passaggio di fase, senza soluzione di continuità. Diverso resta il caso del procedimento penale postumo rispetto alle attività di vigilanza disposte in sede amministrativa e ove non emergevano indizi di reato (*supra*, par. 3).

La contestualità fra i due accertamenti, in breve, concorre quale elemento di disequilibrio e acuisce l'importanza dei limiti di utilizzabilità degli atti formati in sede amministrativa di vigilanza. L'aspetto che per primo lascia emergere molte preoccupazioni si riconduce alla circostanza in base alla quale le azioni investigative poste in essere in questa sede esulano dalle tutele stabilite dal codice di procedura penale.

L'argomento si presta a molte considerazioni, non tutte esplorabili in questa

---

6594/2016 o ancora Cass. Pen., SS.UU., n. 45477/2001. In ambiti diversi ma affini, T. RAFARACI, *Reati tributari con soglia di punibilità e applicazione dell'art. 220 disp. att. c.p.p.: la Cassazione rimarca i diritti della difesa*, in *Rivista della Guardia di Finanza*, 3, 2015, p. 674, ovvero anche M. GUERNELLI, *Aspetti operativi e processuali dell'attività di p.g. nel nuovo c.p.p.*, in *Arch. nuova proc. pen*., 1991. Sia consentito poi il rinvio a A. PUGLIESE, *Atto di provenienza amministrativa e prova penale*, in *Rassegna dell'Avvocatura dello Stato*, fasc. 1, 2017.

Sul tema specifico, si vedano gli spunti in G. CORASANITI, *Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica*, in *Dir. inform. e infor*., fasc. 1, 2025, p. 19; ovvero L. MAGLI, *La protezione dei dati personali contro i rischi del digitale*, in *Riv. trim. dir. pubbl.*, fasc. 2, 2025, p. 401 e M. MACCHIA-G. SFERRAZZO, *Sicurezza e rischio tecnologico. La funzione di cybersecurity*, in *Dir. amm*., fasc. 1, 2025, p. 109.

[39] Quanto si è sin qui scritto testimonia ciò. È qui in discussione un frangente specifico, inerente proprio al passaggio senza soluzione di continuità tra procedimento amministrativo e penale. I differenti casi sono stati invece affrontati prima nel testo e afferiscono, più che altro, al refluire di conoscenze tra procedimenti amministrativi e penali ma quando questi altri si aprano in un secondo momento rispetto ai primi. La distinzione non è così marcata, eppure da ciò passano numerose garanzie.

sede, è perciò necessario circoscrivere il campo d'azione. La questione più urgente è il rapporto tra gli atti cosiddetti misti e le garanzie difensive previste dal codice di procedura penale. Nello specifico, si tratta di esaminare «i limiti che l'ammissibilità di tali [atti] incontra nelle norme relative» [40] alla formazione della prova nel giudizio penale.

Gli atti a finalità mista [41] trovano un punto d'appoggio normativo nell'art. 220 disp. att. c.p.p.: si tratta degli atti prodotti dai funzionari amministrativi in un contesto molto particolare, ovvero quando la loro attività si muove sui confini sottili e non sempre chiaramente visibili tra l'illecito amministrativo e il reato.

Il problema connesso a ciò è immediatamente individuabile. Occorre garantire, con un ragionevole grado di certezza, che le attività svolte dalla P.A. non si muovano in spregio ai diritti di difesa tutelati dal codice di procedura penale e, ancor prima, dalla Costituzione. La questione è tutt'altro che indifferente alle dinamiche di un accertamento penale e (ancora oggi) non ha sempre trovato un'interpretazione unanime nella giurisprudenza [42].

Infatti, l'art. 220 disp. att. c.p.p. identificherebbe di già il momento oltre il quale si dovrebbe ritenere superato il procedimento amministrativo e iniziato quello penale. Esso stabilisce che «quando nel corso delle attività di ispezione o di vigilanza (…) emergono indizi di reato, gli atti necessari per garantire le fonti di prova (…) sono compiuti in conformità alle disposizioni del codice di procedura penale». Ebbene, il punto più critico risiede proprio nell'individuazione del momento in cui un indizio di reato possa ritenersi "emerso". Diversi sono gli interrogativi. Ci si può domandare se, ad esempio, sia necessario attendere che il reato si mostri completamente, ovvero se si debba giungere a potere abbinare al presunto reato una persona determinata (attribuzione soggettiva).

Va osservato che l'intero sistema di garanzie che il codice di procedura prevede deriva dalla risposta a interrogativi come questi, così come la questione dell'ammissibilità in giudizio delle prove raccolte durante la fase amministrativa. Procrastinare eccessivamente il momento a partire dal quale si ritiene che sia emerso un indizio di reato, potrebbe significare indebolire il contenuto delle tutele della difesa. Si ritiene per queste ragioni più in linea con le esigenze del caso, nonché più coerente con la ragion d'essere stessa della norma, fare riferimento a una concezione quasi embrionale del termine, a una mera *possibilità di*

---

[40] R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale*, Giuffrè, 1992, p. 156.

[41] Per l'ampiezza dell'opera, si può rinviare sempre a R. ORLANDI, *Atti e informazioni della autorità amministrativa*, cit.

[42] Ad esempio, Cass. Pen., n. 1973 del 2015 e n. 4919 del 2015.

reato. È quindi plausibile ritenere che l'art. 220 disp. att. c.p.p. sia destinato ad operare quando la «pubblica amministrazione – nelle sue attività di ispezione e vigilanza – viene a conoscenza di un possibile reato» [43].

Va infatti tenuto presente che non tutti gli atti amministrativi sono "ambigui" e, per il momento, dando per scontata la possibilità che l'amministrazione produca solo atti propri, senza che questi tendano necessariamente al penale, si può evitare un malinteso: non a tutti gli atti si applicano le stesse regole di ammissibilità.

Date le premesse di cui sopra, si può procedere a un controllo delle condizioni che i cosiddetti atti misti devono soddisfare per poter essere ammessi al processo, entrando anche nei fondamenti logici della decisione. Sembra opportuno illustrare qui tutti i problemi che, in termini pratici, possono venire alla luce. Si analizzeranno le seguenti categorie: dichiarazioni (da parte di persone che possono essere sospettate di un reato o possibili testimoni), accessi documentali e ordini di cooperazione.

Conviene iniziare con gli atti dichiarativi e, in particolare, con gli atti contenenti le dichiarazioni di coloro che potrebbero diventare, nel corso del processo, prima indagati, poi imputati. Lo scenario è facile da immaginare. Durante un'attività ispettiva, una persona si trova nella posizione di dover "collaborare" con l'Amministrazione, ma così facendo rischia di rilasciare dichiarazioni autoincriminanti. I dubbi che possono sorgere appaiono intuitivi: *quella persona deve essere ascoltata in base alle norme del codice di procedura o è legittimo rimanere al di fuori di esse?* È qui che emerge la necessità di dare una corretta lettura degli "indizi di reato" di cui all'art. 220. Se si aspettasse una *notitia criminis* meglio configurata, si dovrebbe procedere a prescindere dalle garanzie del codice: si applicherebbe ancora il principio *nemo tenetur se detegere*? La risposta alla domanda verrà dalla prassi che si formerà sulle disposizioni precisamente dedicate alla tutela dei sistemi informatici [44]. Nel frattempo, però, si debbono trarre alcune considerazioni intermedie.

Dal punto di vista del codice di procedura penale, gli elementi raccolti dall'ACN si prestano ad essere ricondotti all'art. 234 c.p.p., ovvero alle prove documentali. È il caso del documento che si riferisce a fatti preesistenti al processo penale e formatosi altrove. Da questo punto di vista, la descrizione sembrerebbe applicarsi perfettamente anche ai documenti raccolti dall'ACN durante

---

[43] R. ORLANDI, *Atti e informazioni della autorità amministrativa nel processo penale*, Giuffrè, 1992, p. 156.

[44] Così come in passato, G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la corte costituzionale conferma)*, cit., nonché G. LASAGNI, *Prendendo sul serio il diritto al silenzio. Commento a Corte cost. ord. n. 117 del 10 maggio 2019*, in *Dir. pen. cont*., 2, 2020, pp. 135-162.

le attività di prevenzione e intervento a fronte di attacchi informatici. Ad esempio, i dati raccolti durante le attività preventive, che riguardano la necessaria conformità alle normative di settore, potrebbero essere inclusi in eventuali e futuri procedimenti penali relativi a quegli stessi attacchi informatici. Il caso è diverso se i funzionari dell'ACN e/o del CSIRT Italia, definiti come pubblici ufficiali dalla l. n. 90/2024, art. 22, dovessero raccogliere informazioni su persone potenzialmente sospettate di un reato.

In tal caso, ci sarebbero almeno due possibili considerazioni. In primo luogo, sembrerebbe che la NIS 2 e la l. n. 90/2024 abbiano lo scopo di facilitare l'emergere di informazioni (anche) penalmente rilevanti, identificando così una possibile transizione tra attività di vigilanza amministrativa e procedimenti penali. D'altra parte, le dichiarazioni rese da una persona passibile di incriminazione sollevano la questione: (i) del rispetto del diritto di difesa; (ii) dell'attendibilità delle dichiarazioni rese da chi sia interessato a difendersi. In questa prospettiva, infine, non aiuta la disarmonia che emerge dalla normativa NIS 2, secondo la quale la mancanza di collaborazione può essere valutata nell'imposizione della sanzione e tuttavia, secondo il diritto processuale, alla stessa persona andrebbe riconosciuto il diritto di non autoincriminarsi e quindi a non collaborare. Una dicotomia difficile da sanare, aggravata dall'estrema severità delle sanzioni previste dalla disciplina NIS 2, solo in parte mitigata dal considerando n. 131 della Direttiva, che invoca il rispetto del principio del *ne bis in idem*. Frase più che allusiva e che potrebbe anche sottendere alla necessità di non imporre due sanzioni di natura (sostanzialmente) penale, come quelle contenute nella Direttiva e nel decreto di recepimento italiano potrebbero essere catalogate, secondo i principi dettati, tra l'altro, da oramai noti precedenti, quali A. B. c. Norvegia (CEDU) o Menci, Garlsson e De Puma (CGUE) [45], in ossequio agli standard – meglio noti come "criteri" Engel [46]. Da qui, quindi, l'importanza di garantire la piena operatività dell'art. 220 disp. att. c.p.p.

Oltre a ciò, l'attuazione della norma dipende dalla qualifica che può essere attribuita ai funzionari dell'ACN, quando dispiegano i loro poteri di vigilanza. In sintesi, l'ambito di applicazione dell'art. 220 sarebbe ancora più ampio se costoro fossero considerati in grado di sommare funzioni di polizia giudiziaria. Ciò significherebbe che gli stessi funzionari sommerebbero la funzione di polizia giudiziaria al primo emergere di un "indizio di reato", con il conseguente obbligo di acquisire gli elementi probatori, da quel momento in poi, secondo le norme e le garanzie del codice di procedura penale. Altrimenti, in attesa di capire in quale direzione si muoverà la prassi, in tutti i casi, quegli stessi

[45] Corte EDU, nn. 24130/11 e 29758/11. CGUE, caso *Menci* (C-524/15); *Garlsson Real Estate* (C-537/16) e causa *Di Puma* (C-596/16 e C-597/16).

[46] Corte EDU, n. 5100/71, Engel e altri c. Paesi Bassi.

funzionari, espressamente definiti come pubblici ufficiali dall'art. 22, l. n. 90/2024, avrebbero l'obbligo immediato di denuncia.

In ogni caso, tuttavia, data anche la gravità delle possibili sanzioni amministrative (e che si teme possano avere una consistenza penale), il soggetto sottoposto al controllo, aggrappandosi ai criteri Engel [47], avrebbe ugualmente motivi per opporsi a una forma più lieve di collaborazione, o per non collaborare affatto, appellandosi all'esercizio di un diritto e, in particolare, quello di difesa.

La conclusione, allo stato dell'elaborazione in materia, resta di matrice speculativa; eppure, può ritrovare in altri ambiti utili agganci. Le riflessioni sui procedimenti CONSOB, per esempio, hanno restituito, in un passato affatto remoto, ricostruzioni dottrinali e giurisprudenziali degne di nota, mosse dal fine di evitare patenti contorsioni processuali. Le particolarità che possono essere proprie del settore che occupa questo scritto, si rivedono anche nella vicenda che, a su tempo, impegnò la Corte di Giustizia dell'UE [48] e ciò fortifica le conclusioni cui qui si è pervenuti.

Nell'ambito della cybersicurezza il rischio maggiore si ha quando la medesima condotta costituisca sia violazione della disciplina di settore, sia fattispecie incriminatrice. Il rischio, però, è confinato a ipotesi non necessariamente così ricorrenti. Con questo si vuole dire che le varie fattispecie disseminate nel codice penale, o in leggi speciali, e qui di rilievo sono di matrice dolosa. In molti casi il potere ispettivo e sanzionatorio dell'ACN prescinde dal verificarsi di una fattispecie di reato.

Consistenti sanzioni, infatti, si applicano all'ente che dovesse, per esempio, omettere l'obbligo di notifica in caso di incidente, ovvero in caso di scarsa collaborazione ai test che dovessero essere indetti dagli organismi predisposti (art. 1, comma 8, d.l. n. 105/2019, richiamato *ex* art. 24-*bis*, d.lgs. n. 231/2001). Non necessariamente in ognuno di questi casi si deve presupporre l'esistenza di un reato e, soprattutto, seppure dovesse esservi, sono rari i casi in cui l'entità sotto attacco abbia al suo interno un soggetto apicale che, operando da *intraneus* ma contro l'ente che dirige, ad esempio si adoperi per una esfiltrazione dei dati. Sono casi siffatti ad accendere la serie di allarmi evidenziati soprattutto nell'ultimo paragrafo. Negli altri, si tratterà di applicare, grossomodo, quanto esplorato nella

---

[47] G. LASAGNI, *Prendendo sul serio il diritto al silenzio. Commento a Corte cost. ord. n. 117 del 10 maggio 2019*, in *Dir. pen. cont.*, 2, 2020, pp. 135-162.

[48] Di nuovo, per brevità, sia consentito il rinvio a G. LASAGNI, *La corte di giustizia riconosce il diritto al silenzio*, *op. cit*., ove, a p. 1180, richiamandosi alla vicenda, si rammenta come il ricorrente «si era ripetutamente rifiutato di presenziare alle audizioni della Consob e, una volta comparso, aveva opposto alle richieste di informazioni la facoltà di non autoincriminarsi. All'esito del procedimento, l'accusato veniva condannato non solo per la condotta di insider trading, ma anche a norma dell'art. 187-*quinquiesdecies* TUF, per il comportamento poco collaborativo».

parte precedentemente nella trattazione. Come che sia, le modalità operative concesse dalla normativa di settore ampliano l'orizzonte conoscitivo delle pubbliche autorità, anche oltre i confini nazionali e secondo assetti collaborativi che – al netto di resistenze politiche pure ipotizzabili – potrebbero rivelarsi efficaci e questo è un fatto, col quale conviene cimentarsi, potendosi immaginare la sua crescente rilevanza in futuro.

5. Conclusioni

Le considerazioni sopra esposte chiariscono la complessità delle prospettive di fronte alle quali si trova l'interprete quando si tratta di cybersicurezza. È stata compresa l'importanza di dare un significato adeguato all'art. 220 c.p.p., al fine di garantirne l'effettiva operatività.

È chiaro che un'interpretazione estensiva del termine «indizi di reato» si allinea meglio con la logica della norma e le esigenze del sistema. In breve, la condizione di cui all'art. 220 dovrebbe essere considerata soddisfatta ogniqualvolta gli organi investigativi e amministrativi abbiano già raccolto elementi che consentano loro, anche con un margine di dubbio molto ampio, di considerare astrattamente la rilevanza penale di un fatto.

D'altra parte, i "nostri indizi" non solo sono inadeguati a costituire la base di un giudizio di responsabilità, ma possono essere – ed è qui che emerge il carattere marcatamente garantista della norma – anche in riferimento a una possibile incriminazione. Essi devono solo essere in grado di orientare quella che era iniziata come un'indagine amministrativa verso la strada dell'indagine preliminare. Per quanto riguarda la presunta distinzione tra polizia amministrativa e giudiziaria, in termini generali, la distinzione ha senso; ma ha senso fino a quando è soddisfatta la condizione di cui al 220 disp. att. c.p.p. [49].

In definitiva, la scarsa percorribilità della distinzione fra i modelli di accertamento (penale/amministrativo – pubblicistico/privatistico) è sempre riconducibile all'emergere dei suddetti indizi. Una volta raggiunto tale stadio, si verificherebbe una tale commistione di poteri e funzioni che qualsiasi teoria sulla loro diversità avrebbe scarsa credibilità. In conclusione, ci troviamo di fronte a un dilemma finale: fino a che punto si possono anticipare le prerogative del codice? Tutte le analisi e le valutazioni dell'ACN devono attenersi alle prerogative della legge processuale penale? Fino a che punto, ed eventualmente come procedimentalizzare le indagini puntuali svolte dai privati? E come distinguere

[49] Si veda anche F.N. RICOTTA, *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria*, in *Dir. pen. cont.*, 1, 2023.

i casi in cui il privato agisce quale longa manus dell'autorità e quando invece di propria iniziativa?

La prospettiva di estendere le prerogative codicistiche può apparire allettante, ma occorre meditare attentamente. Se si procedesse in questo modo, si rischierebbe di creare una situazione di ingiustizia non distante da quella che invece si vorrebbe censurare. Si moltiplicherebbero i procedimenti penali, anche quando non necessario, con conseguente aggravio per l'autorità giudiziaria e, dall'altro lato, più individui si vedrebbero costretti a sostenere anche i costi "di immagine" conseguente all'essere iscritto nel registro degli indagati [50]. La distinzione che si è posta, fondata sulle diverse possibili situazioni ipotizzabili, mira a mantenere un ragionevole equilibrio fra le molteplici istanze con cui deve di già cimentarsi l'interprete. Appare oramai innegabile una forte compenetrazione fra l'ambito pubblicistico e quello penale e, vista l'iper-specializzazione di molte materie (quella della cybersicurezza è solo l'ultima [51]), si mostra essere una strada senza ritorno. Il processo penale si alimenterà delle conoscenze che proverranno da altri apparati dello Stato e, più di frequente forse, anche di quelle che dovessero essere messe insieme dai privati.

Nulla di nuovo sotto il sole, entro certi limiti. Ciò detto, infatti, andrà disegnato con cura il perimetro della legittimità delle attività para-investigative poste in essere al di fuori del procedimento penale, onde evitare che in queste si ritrovino escamotage per aggirare le prerogative e le legittime aspettative che – ed è bene ricordarlo – nel codice di rito sono costruite tutte attorno a precetti sovralegali. Quando, invece, le stesse ispezioni in sede amministrativa dovessero tramutare in accertamenti sul fatto costituente reato, in quel momento occorrerà garantire il più rigoroso rispetto dell'art. 220 disp. att. c.p.p.

Su questi precari equilibri si giocherà la futura sfida della cybersicurezza, in bilico tra i poteri dell'ACN e l'autorità giudiziaria. L'obiettivo è trovare un nuovo baricentro, che tuteli i vari interessi: la sicurezza della società nel suo complesso, la salvaguardia dei diritti di ogni individuo all'interno di quella società, compresi coloro che dovessero essere sospettati di aver commesso un reato.

---

[50] Per comune esperienza, se è pur vero che un'archiviazione può "riabilitare" l'immagine dell'indagato, è pur vero che sino a quel momento l'iscrizione fra gli indagati può condurre a conseguenze pregiudizievoli sul piano reputazionale.

[51] Solo a mo' d'esempio, si può pensare alla privacy, al settore ambientale, a quello bancario, all'antiterrorismo e altri esempi vi sarebbero.