RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0195 • articolo sottoposto a peer review • pubblicato in anteprima il 19 dic. 2024

Federico Niccolò Ricotta

Vulnerability disclosure e *penetration testing*: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2

Il contributo analizza le principali questioni giuridiche connesse all'adozione di politiche di cosiddetta *vulnerability disclosure*, espressione con la quale si designa il processo di comunicazione e correzione delle falle nella sicurezza, e i cosiddetti *penetration test*, attività che simula un attacco informatico proprio allo scopo di far emergere le vulnerabilità nella sicurezza. Da un lato, l'interesse pubblico alla sicurezza cibernetica delinea gli oneri dei soggetti pubblici e privati per correggere, ma soprattutto comunicare le vulnerabilità; dall'altro, l'attività di *penetration test*, laddove sia condotta da soggetti diversi dal titolare del sistema, può costituire reato. Da qui, la ricerca di un possibile bilanciamento, che consenta di salvaguardare la sicurezza cibernetica attraverso la repressione penale degli illeciti commessi in quest'ambito, senza però disincentivare l'emersione di situazioni di vulnerabilità, attraverso la segnalazione da parte di quanti sono stati in grado di testare le fragilità dei sistemi informatici. Tale disamina sarà effettuata pure in prospettiva comparata, tenendo conto della soluzione adottata nella Repubblica Francese.

Crimini informatici – Vulnerabilità – Test di sicurezza – Recepimento NIS 2 – Notizia di reato

Vulnerability disclosure and penetration testing: relevant legal profiles for the adoption of a national policy compliant with the NIS 2 Directive

The paper examines the main legal issues related to the adoption of so-called vulnerability disclosure policies, a term that refers to the process of communicating and addressing security flaws, and penetration testing, an activity that simulates a cyberattack with the specific aim of identifying security vulnerabilities. On one hand, the public interest in cybersecurity outlines the responsibilities of public and private entities to not only address but also communicate vulnerabilities; on the other hand, penetration testing, when conducted by individuals other than the system owner, may constitute a criminal offense. This raises the need to find a possible balance that ensures cybersecurity by penalizing unlawful acts in this area, while avoiding discouragement of the reporting of vulnerabilities by those capable of testing the weaknesses of IT systems. This analysis will also include a comparative perspective, taking into account the solution adopted in the French Republic.

Vulnerability disclosure – Penetration testing – NIS 2 – Hacking – Cyber crimes

L'Autore è dottore di ricerca in Procedura penale e assegnista di ricerca in SEcurity and RIghts in the CyberSpace

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

Sommario: 1. Introduzione. – 2. Vulnerabilità e *penetration testing*. – 3. I modelli di *vulnerability disclosure*. – 4. CSIRT e politiche di *coordinated vulnerability disclosure*. – 5. Esenzione di responsabilità dell'attività di *penetration testing*. – 6. La politica di CVD adottata nella Repubblica Francese. – 7. Una scriminante procedurale come possibile porto sicuro per i *penetration tester*?- 8. Anonimato delle segnalazioni e comunicazione della notizia di reato e controllo giudiziario sulle condotte autorizzate. – 9. L'anonimato attraverso l'assenza di comunicazione della notizia di reato. – 10. L'anonimato e le garanzie funzionali. – 11. Conclusioni.

1. Introduzione

L'art. 12 della direttiva NIS 2 prevede l'istituzione di una banca dati europea delle vulnerabilità e, soprattutto, prescrive che, in sede di attuazione nazionale, ciascuno Stato membro adotti una propria politica di regolazione delle modalità di rilevamento delle vulnerabilità dei sistemi informatici.

L'adozione d'una politica di coordinated vulnerability disclosure, d'ora in poi CVD, conforme ai desiderata della NIS 2 richiede tre adempimenti strutturali, che saranno analizzati nei paragrafi che seguono: la tipologia di vulnerability disclosure che definisca il coordinamento tra i soggetti pubblici e privati interessati dalla procedura ed una duplice garanzia per il tester di sicurezza in termini di esenzione da responsabilità e anonimato della segnalazione.

Come si vedrà, le disposizioni legislative di recepimento, adottate in Italia con il d.lgs. 4 settembre 2024 n. 138, hanno regolamentato soltanto l'organo competente a ricevere e gestire le segnalazioni di vulnerabilità, lasciando ancora da definire i profili relativi alla responsabilità e all'anonimato del segnalante.

2. Vulnerabilità e *penetration testing*

Nella loro dimensione massimalista le politiche di CVD si riassumono nelle tre fasi della emersione, comunicazione e correzione di una vulnerabilità.

La vulnerabilità è un insieme di condizioni che consente la violazione della sicurezza o della riservatezza di un sistema. È sostanzialmente una falla nella sicurezza informatica che, in quanto tale, si presta ad essere sfruttata per scopi malevoli. In quanto rischio strutturale per la sicurezza, se la vulnerabilità viene scoperta, dovrebbe essere comunicata tempestivamente: anzitutto allo sviluppatore del sistema informatico, affinché venga corretta; in secondo luogo, se la legge lo prevede, anche all'autorità pubblica di settore, se la vulnerabilità ha l'attitudine a compromettere interessi ultra-individuali rilevanti sul piano pubblicistico. Questo può accadere, i.e., in relazione ai sistemi che rientrano nel perimetro di sicurezza cibernetica e che, come tali, sono sottoposti alla vigilanza dell'Agenzia per la cybersicurezza nazionale. Nella comunicazione circa l'esistenza della vulnerabilità è l'attività di disclosure: in Italia, per esempio, è il CSIRT (acronimo di *Computer Security Incident Response Team*) ad essere destinatario delle informative sui rischi dei sistemi e delle infrastrutture digitali.

Le vulnerabilità emergono solitamente attraverso l'esecuzione dei cd. penetration test, quali pratiche comuni nella sicurezza informatica che, simulando un atto hacker, hanno lo scopo di identificare le debolezze nei sistemi informatici. I test possono essere condotti da soggetti interni alla società che sviluppa il sistema, oppure da soggetti esterni, pubblici o privati, che operano con o senza la consapevolezza ed il consenso delle entità proprietarie dei sistemi, per esempio nel corso dei cd. Bug Bounty Programs, vale a dire quando un'organizzazione offre ricompense (spesso economiche)

a chi riesce a scoprire e segnalare vulnerabilità nei loro sistemi, applicazioni o servizi[1].

Per questo, come si vedrà, queste attività, così come gli strumenti utilizzati per i test, possono costituire la condotta materiale di un reato o rilevare in sede civile. Del resto, e qui risiede l'ulteriore profilo di interesse per la regolazione pubblica, ragioni economiche, reputazionali o legate a segreti industriali possono disincentivare i privati, ma anche le amministrazioni, a non far emergere pubblicamente le vulnerabilità dei propri prodotti e, quindi, a non consentire che siano i terzi a condurre i *penetration test*.

3. I modelli di *vulnerability disclosure*

La prassi cibernetica conosce tre modelli di vulnerability disclosure[2], che differiscono tra loro in ragione del diverso grado di intervento e coordinamento tra chi con la propria attività fa emergere le vulnerabilità e le segnala, chi sviluppa o è proprietario dei sistemi vulnerabili e l'eventuale autorità pubblica deputata all'esercizio di una funzione di cybersicurezza[3].

Il tratto comune delle vulnerability disclosure è l'essere un processo tramite il quale vengono rivelate le vulnerabilità di sicurezza in software o sistemi a chi può risolverle, tendenzialmente prima che queste informazioni diventino note al pubblico generale. Questo processo, quindi, consente a venditori, sviluppatori, gestori e ricercatori IT che rilevano una vulnerabilità di cooperare per trovare soluzioni che riducano il rischio associato alle vulnerabilità pubbliche; cioè, un ricercatore (chi trova) che scopre un difetto in un sistema, informa lo sviluppatore (venditori, fornitori) del sistema riguardo al difetto e alle possibili correzioni. Questo consente allo sviluppatore di prendere misure di mitigazione (patch, monitoraggio del traffico, blocco) per eliminare o ridurre il rischio che la vulnerabilità sia utilizzata da un attaccante.

A partire da questa matrice comune le soluzioni, come anticipato, si dividono tra divulgazione pubblica o full disclosure, divulgazione responsabile o responsible disclosure e divulgazione coordinata o coordinated disclosure.

Nella full disclosure le informazioni sulla vulnerabilità vengono pubblicate apertamente e in modo che chiunque possa accedervi; nella responsible disclosure le informazioni sulla vulnerabilità vengono condivise privatamente con il fornitore del software o hardware interessato, dando loro il tempo di risolvere il problema prima che la vulnerabilità sia resa pubblica, anche attraverso una timeline concordata tra chi ha scoperto la vulnerabilità e il fornitore per la correzione e la successiva divulgazione pubblica; infine la coordinated disclosure, che consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico[4]. Secondo questo modello, quello prescelto dalla stessa direttiva NIS 2, la divulgazione delle informazioni sulla vulnerabilità viene gestita in collaborazione tra ricercatori, fornitori e talvolta anche organizzazioni di terze parti, come i CERT (Computer Emergency Response Team) o i CSIRT.

4. CSIRT e politiche di *coordinated vulnerability disclosure*

Il primo pilastro delle politiche di CVD riguarda certamente la gestione delle segnalazioni e tutto ciò che ne consegue in termini di comunicazioni e correzioni.

Appare evidente che la stessa NIS 2 prediliga il modello di gestione coordinata della disclosure e lo affidi alle competenze del CSIRT nazionale e, per quanto non espressamente conferito, all'Agenzia per la cybersicurezza nazionale dal quale il CSIRT dipende.

Il legislatore nazionale si è quindi mosso conformemente al modello indicato dalla NIS 2 e, all'art. 16 del Decreto Legislativo 4 settembre 2024 n.138 di recepimento della direttiva europea, ha designato il

1. V. Fiorinelli–Zucca 2024.
2. *Ivi*, p. 5 ss. e NIS Cooperation Group 2023 e Enisa 2016.
3. V. in generale Rossa 2023; Ursi 2023, p. 7 ss.; Pupillo–Ferreira–Varisco 2018; Householder–Wassermann–Manion–King 2017.
4. Cfr. Considerando n. 58 della direttiva NIS 2.

CSIRT Italia quale coordinatore della divulgazione coordinata delle vulnerabilità e intermediario tra il soggetto segnalante e quello produttore o fornitore del servizio ICT potenzialmente vulnerabile.

Si è quindi scelto di impostare l'implementazione delle politiche assecondando un criterio di accentramento delle diverse funzioni connesse alle CVD in un unico polo operativo deputato, da un lato, a gestire le segnalazioni in via riservata, assicurando l'anonimato del segnalante, dall'altro, a procedere agli adempimenti necessari per comunicare e avviare la correzione della vulnerabilità tra i vari soggetti interessati dalla procedura.

La scelta del modello non è casuale ma coerente con la necessità di soddisfare i diversi interessi sottesi al modello di gestione coordinata: in primo luogo, assicurare la tutela dello sviluppatore e della pubblica sicurezza cibernetica, affinché l'esistenza di una potenziale falla nella sicurezza dei sistemi non venga resa indiscriminatamente nota al pubblico, con il rischio di essere malevolmente sfruttata nelle more che venga risolta, ma che essa venga corretta in linea con le prescrizioni tecnico-operative impartite dall'Agenzia stessa; inoltre, garantire la tutela del soggetto segnalante sotto il duplice profilo dell'esenzione da responsabilità e della garanzia dell'anonimato.

5. Esenzione di responsabilità dell'attività di *penetration testing*

Il secondo pilastro delle politiche interne di *coordinated vulnerability disclosure* è quello che insiste sui profili di responsabilità penale e civile di chi effettua i *penetration test*.

La tutela di chi opera legittimamente nel campo della sicurezza cibernetica risulta ancora uno dei profili da normare, probabilmente il più rilevante, per un'implementazione conforme alle indicazioni della NIS 2 che, a mente del considerando n. 60, richiede agli Stati membri di adottare misure atte a proteggere i ricercatori dalla loro potenziale esposizione alla responsabilità penale e civile per le attività svolte.

Il rapporto tra crimini informatici e le vulnerability disclosure si presenta piuttosto complesso e non nuovo, soprattutto se si guarda alle esperienze pilota avvenute oltreoceano[5].

Dal punto di vista del diritto nazionale italiano, la variabilità dell'esposizione a responsabilità penale è essenzialmente legata all'effettiva offensività della condotta di penetration test che, conseguentemente, traccia il limite oltre al quale l'hacking per finalità di ricerca e di sicurezza può causare danni ai sistemi considerati accettabili per l'ordinamento.

Nel diritto penale italiano la criminalizzazione delle condotte riconducibili all'attività di penetration testing opera essenzialmente su tre livelli: quello delle attività prodromiche, che riguardano essenzialmente l'uso di software cd. dual use, vale a dire programmi che consentono la violazione dei sistemi[6]; quello dell'esecuzione vera e propria dei test attraverso attacchi simulati potenzialmente riconducibili all'accesso abusivo a sistema

5. Il problema è stato affrontato negli USA. A livello federale la principale legge è il *Computer Fraud and Abuse Act* (CFAA) del 1986 (il cd. statuto federale "anti-hacking"), che ha configurato l'accesso non autorizzato a un sistema informatico, in particolare a un sistema governativo o commerciale quale l'atto di «accedere consapevolmente a un computer senza autorizzazione o eccedere le condizioni dell'accesso autorizzato». Il problema si è conseguentemente concentrato sulla vaghezza del significato "eccedere le condizioni dell'accesso autorizzato", con il rischio di criminalizzare un ampio novero di condotte, ulteriori a quelle di penetration testing, laddove si pongano in contrasto con i termini di licenza o delle condizioni di uso del software. È intervenuta sul punto la Corte suprema degli USA, stabilendo e.g. in *Van Buren v. United States* che in materia di accesso abusivo e condizioni di autorizzazione non rilevano le regole EULA (*End User License Agreement*)).
6. Le principali fattispecie sono quelle considerate all'art. 615-*quater* c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; all'art. 615-*quinquies* c.p. Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico; all'art. 617-*quinquies* c.p., Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; all'art. 171-*bis*, co. 1, legge diritto di autore; all'art. 171-*ter*, co. 1, lett f), legge diritto di autore; all'art. 171-*ter*, co. 1, lett. f-*bis*), legge diritto di autore; v. per un approfondimento Cadoppi–Canestrati–Manna–Papa 2023 ed in particolare Salvadori 2017.

informativo, all'intercettazione di sistema informatico o al danneggiamento dei sistemi[7].

La criminalizzazione si fonda essenzialmente sulla rilevanza della natura abusiva della condotta di chi opera su sistemi informatici o ricorre a determinati strumenti, ricomprendendo tutte quelle attività intenzionalmente nocive e soprattutto condotte in assenza del consenso dell'avente diritto[8]. Per altro, sul piano strettamente penalistico, con l'art. 615 ter c.p. il legislatore ha inteso sanzionare l'accesso abusivo ad un sistema informatico o telematico, o la permanenza non autorizzata in esso, in quanto tali. Non assume infatti alcuna rilevanza, ai fini della consumazione dell'illecito, né l'effettiva presa di conoscenza di dati o informazioni, né la natura di questi ultimi né, soprattutto, le motivazioni che hanno mosso il soggetto agente[9].

6. La politica di CVD adottata nella Repubblica Francese

Come anticipato, adottare una politica di CVD che sia in linea con le aspettative della direttiva NIS 2 richiede la previsione di un'area di esenzione da responsabilità del *penetration tester* per tutte quelle attività che, sebbene siano necessarie a far emergere una vulnerabilità, possono in condotte materiali di rilevanza penale.

Una soluzione interessante, ma come si vedrà inattuabile nel nostro ordinamento, è quella adottata nel 2016 in Francia, dove un tester può far emergere una sospetta vulnerabilità all'*Agence nationale de la sécurité des systèmes d'information* (ANSSI) e giovarsi della disciplina dell'Art. 47 della Loi per une République Numérique che esenta da responsabilità penale il ricercatore che ha effettuato in buona fede le operazioni di penetration testing. Effettuata la comunicazione, è compito dell'ANSSI proteggere l'anonimato del segnalante e delle informazioni relative alla scoperta della vulnerabilità.

Il funzionamento dell'esimente francese si caratterizza per una spiccata interconnessione tra le attività giudiziarie e quelle amministrative dell'ANSSI, che invero assume un ruolo di primissimo piano.

Anzitutto, il meccanismo di tutela opera attraverso la facoltà di non esercitare l'azione penale: il menzionato Art. 47, attraverso la modifica dell'art. L 2321-4 Code de la defense[10], consente al pubblico ministero di non perseguire penalmente[11] il tester laddove ricorrano congiuntamente due condizioni: il tester che segnala una vulnerabilità deve aver agito in buona fede e la vulnerabilità deve essere segnalata esclusivamente all'ANSSI che, s'è detto, si occupa anche di garantire le condizioni di anonimato.

A sua volta, la valutazione di buona fede effettuata dal Pubblico Ministero, quindi sulla meritevolezza dell'inazione penale a fronte di condotte potenzialmente criminose ma utili per la sicurezza

7. Le principali fattispecie sono art. 615-*ter* c.p., Accesso abusivo a Sistema informatico; art. 617-*bis* c.p., Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche; artt. 635-*ter* e 635-*quinquies* c.p., Danneggiamento di dati e sistemi pubblici; artt. 635-*bis* e 635-*quater*, Danneggiamento di dati e sistemi privati; v. nota precedente per i riferimenti bibliografici.
8. Vedi per tutti Fiorinelli–Zucca 2024, p. 8 ss. e Flor 2020-a, p. 165 ss. e Flor 2020.
9. Cfr. Flor 2020-a, p. 165 ss.
10. Tradotta, la disposizione stabilisce che ai fini della sicurezza dei sistemi informatici, non si applica l'obbligo previsto dall'articolo 40 del codice di procedura penale nei confronti di chi trasmette in buona fede all'autorità unica nazionale per la sicurezza dei sistemi informativi informazioni sull'esistenza di una vulnerabilità riguardante la sicurezza di un sistema di trattamento automatizzato dei dati. L'autorità preserva la riservatezza dell'identità della persona all'origine della trasmissione nonché delle condizioni in cui questa è stata effettuata. L'autorità può compiere le operazioni tecniche strettamente necessarie per caratterizzare il rischio o la minaccia di cui al primo comma del presente articolo, al fine di allertare l'host, l'operatore o il responsabile del sistema informativo.
11. La deroga contenuta nell'art. 2321-4 *Code de la defense* agisce sull'art. 40 del Codice di procedura penale francese in materia di esercizio dell'azione penale e obbligo di denuncia del pubblico ufficiale: il pubblico ministero riceve le denunce e valuta il seguito da dare loro conformemente alle disposizioni dell'articolo 40-1 (codice di procedura penale).

cibernetica, poggia sulle regolamentazioni fornite dall'ANSSI: il grado della buona fede richiesto per beneficiare dell'esenzione penale è essenzialmente il grado di aderenza del tester alle stesse regole, migliori pratiche, protocolli individuati dall'Agenzia cyber francese nella sua veste di supervisore e regolatore.

La soluzione è del resto ragionevole perché codifica sostanzialmente un controllo pubblicistico.

Poiché tornerà utile nei successivi paragrafi, bisogna qui osservare come la tutela dell'anonimato è sì affidata all'ANSSI ma essenzialmente dipende dalla scelta di non avviare un procedimento penale a carico del tester.

Anonimato, responsabilità e azione penale sono infatti un trinomio interdipendente: infatti, non v'è vero anonimato se c'è un processo penale da celebrare, e c'è un processo penale solo in presenza di una notizia di reato effettivamente da perseguire.

7. Una scriminante procedurale come possibile porto sicuro per i *penetration tester*?

La soluzione francese è interessante ma così com'è inapplicabile nel nostro ordinamento, non foss'altro perché nella Repubblica Francese l'azione penale è pur sempre discrezionale ed è per questo che lì la condotta del tester può essere valutata secondo un criterio tanto elastico come quello della buona fede (seppur integrata nella sua tipicità dalle disposizioni dell'ANSSI), che invece sarebbe incompatibile con la struttura delle nostrane esimenti penali.

Immaginare nel nostro ordinamento un'area di esenzione della responsabilità richiede anzitutto una impalcatura coerente con il principio di legalità, fondata quindi sulla tipicità delle condotte rilevanti e delle condizioni esimenti sulla scorta delle quali valutare la meritevolezza dell'attività del tester: devono sussistere elementi oggettivi e predeterminati che stabiliscano se e soprattutto in quale proporzione l'offesa arrecata dal test può dirsi giustificata per ragioni di sicurezza cibernetica.

Bisogna anche considerare il ruolo dei soggetti che svolgono i test e la salvaguardia delle ulteriori manifestazioni degli interessi ordinamentali alla sicurezza e all'ordine pubblico.

Per esempio, è più agile immaginare una esimente per chi svolge istituzionalmente attività di sicurezza, quali il personale in ruolo all'Agenzia per la cybersicurezza nazionale o delle forze di polizia data la rilevanza pubblicistica delle relative funzioni e l'esistenza di una disciplina omologa (si pensi, i.e., alla disciplina dell'agente sotto copertura o quella delle cd. garanzie funzionali).

Più complesso risulta invece disciplinare l'attività dei privati, siano essi persone fisiche o giuridiche: per quest'ultimi, si deve contemperare l'esigenza di promuovere l'indipendenza della ricerca e l'anonimato della segnalazione (art. 82 NIS) senza tuttavia giungere ad una liberalizzazione incontrollata di condotte, pur sempre potenzialmente offensive, che potrebbero prestarsi ad usi strumentali.

Emerge, quindi, la necessità di approntare specifici controlli pubblicistici: in questo caso, analogamente all'ANSSI, affidare all'autorità di settore, in sinergia con l'Autorità giudiziaria, il compito di garantire un'ordinata e consapevole gestione delle attività di sicurezza cibernetica attraverso l'adozione di best practices da seguire nell'esecuzione dei test, nella verifica dei relativi risultati e delle metodologie adottate attraverso l'introduzione di eventuali obblighi di comunicazione circa le azioni di penenetration testing intraprese.

Poiché la NIS 2 richiede un'esenzione che copra le responsabilità penali e civili, la soluzione maggiormente satisfattiva in punto di tutela potrebbe essere quella di introdurre una causa di giustificazione che elimini in radice l'antigiuridicità del fatto commesso, nelle forme della cd. scriminante procedurale, vale a dire quella scriminante che esclude l'antigiuridicità all'esito di una procedura di autorizzazione che si completa prima che il fatto di rilevanza penale venga commesso[12].

In termini generali, rispetto i.e. alle clausole di esclusione della punibilità, la scriminante è oggettiva e agisce sull'antigiuridicità del fatto e, come tale, apporta tutta una serie di benefici in termini di effettività della tutela del penetration testing: si estende a tutti i correi eventuali (i.e. all'intero team di hacking); eliminando l'antigiuridicità si escluderebbero anche le conseguenze extra penali

12. V. Consulich 2018, p. 38 ss. che in particolare osserva come il modello della scriminante procedurale possa estendersi anche oltre l'ambito delle questioni "eticamente sensibili" nelle quali la categoria si è principalmente sviluppata e Sessa 2023.

della condotta in punto di responsabilità civile e disciplinare[13].

Nello specifico contesto della sicurezza cibernetica, la predilezione per un modello procedurale di scriminante è data dal fatto che essa consente di meglio incorporare i controlli pubblicistici sulle attività e la garanzia di anonimato[14].

La dinamica procedurale è ben spiegata dalla applicazione della scriminante nel delicato settore dell'autodeterminazione terapeutica, il cd. il suicidio medicalmente assistito: qui le condotte legate a queste pratiche perdono rilevanza penale perché vengono compiute in forza, e in conformità, ad una specifica autorizzazione che è l'epilogo di una procedura volta a valutare in concreto la sussistenza dei presupposti.

In sostanza, con le scriminanti procedurali il soggetto agisce nel rispetto di una disciplina che prevede l'esperimento di controlli pubblicistici preventivi alla condotta, sulla base di parametri di liceità tassativamente predeterminate dalla legge.

Così, il meccanismo di controllo pubblicistico ex ante della scriminante procedurale ha il pregio di consentire un ordinato e vigilato svolgimento di pratiche potenzialmente decettive. Come s'è anticipato, proprio per i penetration test svolti da soggetti terzi ed estranei al produttore/sviluppatore o alle istituzioni, le stesse ragioni di ordine e sicurezza pubblica che giustificano il loro svolgimento impongono di evitare una indiscriminata "liberalizzazione" ma anzi di vagliare, e autorizzare, solo le condotte che risultano meritevoli di non subire conseguenze legali.

Sicché, si potrebbe dunque ipotizzare l'adozione di un decalogo delle pratiche di penetration testing ammissibili e una procedura di autorizzazione preliminare, o meccanismi di notifica e controllo concomitante, affidate all'organo pubblico affinché chi svolge attività di test di sicurezza cibernetica agisca all'interno di un perimetro regolato e tutelato dalla stessa Autorità di settore che, nel sistema italiano, è senz'altro l'Agenzia per la cybersicurezza nazionale.

Infine, come si vedrà nel paragrafo che segue, l'adozione di una scriminante procedurale ha risvolti diretti anche in relazione alla tutela dell'anonimato del segnalante, l'ultimo pilastro delle politiche di divulgazione coordinata delle vulnerabilità.

8. Anonimato delle segnalazioni e comunicazione della notizia di reato e controllo giudiziario sulle condotte autorizzate

Il terzo pilastro delle politiche di CVD è l'anonimato della segnalazione. Esso è espressamente previsto dalla NIS 2 e ribadito dal già menzionato all'art. 16 del Decreto Legislativo 4 settembre 2024 n.138, a mente del quale il CSIRT Italia ha il compito di assicurare (a richiesta dallo stesso segnalante) l'anonimato delle persone fisiche e giuridiche al momento della segnalazione e nel corso delle azioni successivamente intraprese a seguito della notifica di vulnerabilità.

L'anonimato è parte integrante del generale schema di tutela del tester segnalatore, perché lo mette al riparo dalle possibili conseguenze professionali o legali e quindi lo invoglia a fare test e a condividere nel modo più completo possibile le vulnerabilità identificate, promuovendo la collaborazione e nel complesso contribuendo ad una maggiore sicurezza dei sistemi.

Tuttavia, così congegnato, quest'anonimato risponde solo parzialmente al problema. L'anonimato deve essere infatti letto unitamente ai profili di responsabilità penale e del relativo controllo giudiziario: un segnalatore anonimo ma non scriminato, ad esempio perché non legalmente autorizzato, resta tale fino a quando non viene avviato un procedimento penale volto a verificare la legittimità della sua condotta.

S'è detto[15], infatti, che l'anonimato risulta irrimediabilmente legato alla responsabilità e al promovimento dell'azione penale: se c'è un processo penale da celebrare non c'è anonimato, e se c'è un processo penale significa che si è in presenza di una notizia di reato che è stata comunicata e che incardina il dovere della Procura di procedere conformemente.

La questione è complessa e si apprezza su almeno due livelli: il primo flusso informativo rilevante si attesta nel dovere di comunicare tutte le

13. Sul tema v. Fiorinelli–Zucca 2024, p. 9 ss.

14. Anche se bisogna osservare come il modello teorico della scriminante procedurale non sia ancora unanimemente accettato in dottrina v. *supra* Consulich 2018.

15. V. *supra* § 6.

informazioni relative ad una potenziale condotta di reato da parte del personale dell'Agenzia cyber alla Procura della Repubblica, secondo il dovere generale stabilito dall'art. 331 c.p.p. c.p.p. a carico dei Pubblici Ufficiali e rafforzato dai doveri di comunicazione introdotti nei decreti cybersicurezza adottati di recente[16]; in secondo luogo, vi sono i doveri di ostensione informativa che gravano sulla stessa Procura della Repubblica in sede di iscrizione della notizia di reato e successivo svolgimento delle indagini[17].

Anzitutto, l'ACN, se nel corso delle proprie funzioni ravvisa gli estremi di una condotta di reato, circostanza che in assenza di una specifica disciplina ad hoc per i penetration testing può virtualmente accadere sempre, non può non comunicare alla Procura della Repubblica anche il nome del soggetto segnalatore: il quantum comunicativo è quello della denuncia, la quale contiene, ai sensi dell'art. 332 c.p.p.[18], l'esposizione degli elementi essenziali del fatto e, quando possibile, il domicilio e quanto altro valga alla identificazione della persona alla quale il fatto è attribuito, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

A sua volta, la Procura ha il dovere dell'iscrizione nominativa della notizia di reato, atto che è il prodromo necessario all'avvio delle indagini preliminari e infine alla disclosure delle identità del segnalante-autore del test di sicurezza attraverso l'ostensione degli atti di indagine.

Quindi, la notizia di reato espone il segnalatore non solo all'azione investigativa ma soprattutto alla conoscenza della sua identità da parte del produttore/sviluppatore testato che, nella situazione appena descritta, assume senz'altro la posizione di potenziale persona offesa, con conseguente sterilizzazione della funzione di tutela stessa che l'anonimato dovrebbe invece approntare.

Quindi, l'identità del segnalante, prima o poi, è destinata ad emergere. Così accade anche nel whistleblowing[19], la cui dinamica è prossima a quella ora in commento: l'identità del segnalante è coperta dall'anonimato in relazione e nei limiti del segreto istruttorio dell'art. 329 c.p.p., istituto che è funzionale alla tutela delle indagini e non dei soggetti coinvolti. Per questo, l'anonimato del segnalante è destinato a perdersi senz'altro nel momento in cui le indagini preliminari terminano e, indipendentemente dalla scelta del pubblico ministero sull'esercizio della azione penale, gli atti di indagine vengono messi a disposizione delle parti.

Tuttavia, la situazione si prospetta qui diversa rispetto al whistleblowing: il whistleblower è tendenzialmente il soggetto che ha notizia di una condotta illecita commesso nella struttura dove opera, della quale ha avuto conoscenza in ragione del proprio rapporto di lavoro e che decide di comunicare ai responsabili deputati a ricevere tali segnalazioni che ne assicurano l'anonimato.

Il penetration tester segnalatore, invece, è solitamente colui il quale ha anche commesso le operazioni di test e, quindi, il potenziale fatto stesso di reato, e questo pone il suo anonimato in una posizione decisamente meno resistente di quella del segnalatore testimone.

Per risolvere i segnalati inconvenienti è possibile ipotizzare almeno due soluzioni. La prima si basa sulle ricadute processuali della scriminante procedurale considerata unitamente alle sue ricadute processuali: considerando tale scriminante, il segnalante riceverebbe una tutela decisamente più forte perché, in radice, non ci sarebbe una notizia di reato da comunicare. La seconda, invece, si trae dall'istituto delle garanzie funzionali.

9. L'anonimato attraverso l'assenza di comunicazione della notizia di reato

La prima soluzione è quella legata alle ricadute processuali della causa di giustificazione procedurale: poiché con la scriminante in discorso il fatto

16. In particolare, gli obblighi di trasmettere informazioni rilevanti al Procuratore nazionale antimafia e antiterrorismo relative ai gravi reati informatici inseriti dal comma 1 dell'art. 2-*bis* del d.l. n. 123/2023 che introduce il nuovo comma 4 dell'art. 17 d.l. n. 82/2021 «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». V. Nocerino 2023.
17. V. Aprati 2010. Per le novità apportate dalla riforma Cartabia v. Scarpino 2023 e Curtotti 2022.
18. V. Paulesu 2023, p. 1524 ss.
19. Secondo le disposizioni della l. 30 novembre 2017, n. 179 e normativa collegata. V. Evaristi 2021.

è sì tipico ma non antigiuridico già al momento in cui è commesso, in linea di principio non risulta notizia di reato alcuna da comunicare all'ufficio del pubblico ministero, e tanto basta a garantire l'anonimato del *tester*, che evidentemente ha superato positivamente lo scrutinio pubblicistico legato alla scriminante.

In altra prospettiva, questa soluzione lascia comunque spazi di tutela per la persona offesa, verosimilmente il soggetto il cui sistema è stato violato per ragioni di test, che dal canto suo potrebbe nutrire comunque l'interesse all'esercizio dell'azione penale.

Si tratterebbe quindi di prediligere una soluzione di cd. *prosecution by complaint*[20] incentrata sull'iniziativa del soggetto target delle operazioni di *penetration testing*: a fronte di una scriminante, è il testato che con la propria denuncia solleciterebbe un sostanziale riesame di quanto compiuto dal tester e, in particolare, del fatto che quest'ultimo abbia agito al di fuori dei limiti di legge.

Il modello di *prosecution by complaint* è di agevole applicazione perché può contare su quanto già disciplinato dal codice di procedura penale: anche a fronte di una condotta scriminata proceduralmente, la persona offesa può comunque trasmettere alla Procura la denuncia di aver subito un'attività di testing illegittima ivi allegando, in modo puntale, tutti gli elementi utili a rappresentare una notizia di reato quale fatto determinato e non inverosimile riconducibile ad una fattispecie incriminatrice secondo la definizione data dall'art. 335 c.p.p.[21].

A sua volta il pubblico ministero, ricevuta la denuncia del privato e acquisita la documentazione dell'autorità incaricata dell'autorizzazione, può verificare l'attività di penetration testing senza sacrificare l'anonimato del tester, valutando prima facie se si trova dinanzi ad una notizia di reato o meno.

Se la risposta è negativa, perché non risultano oltrepassati i limiti legali, allora il pubblico ministero può infine iscrivere il fatto non nel registro delle notizie di reato ma in quella dei fatti non costituenti reato (il cd. modello 45 delle pseudo-notizie[22]). Per le pseudo-notizia non vigono meccanismi di comunicazione a soggetti diversi dalla Procura che procede all'annotazione, circostanza quest'ultima che ben tutelerebbe gli scopi a cui la ratio dell'anonimato è preordinata: poiché la pseudo notizia riguarda fatti che non hanno rilevanza penale, non ci sono indagini da avviare e, quindi, identità da divulgare alle parti interessate.

Diversamente, se la risposta è positiva, e quindi risulta un'attività di test che eccede o viola le condizioni scriminanti, allora il pubblico ministero procederebbe iscrivendo la notizia di reato e dando avvio alle indagini nelle forme ordinarie.

Del resto, in quest'ultima situazione ci si troverebbe di fronte di un'attività di rilevanza penale da perseguire che, in quanto tale, farebbe venir meno la necessità di tutelare l'anonimato del soggetto che ha agito al di fuori dei limiti legali.

10. L'anonimato e le garanzie funzionali

La seconda possibile soluzione potrebbe essere tratta dalla disciplina delle cd. garanzie funzionali, il nomen con il quale è conosciuta la scriminante speciale disciplinata dagli artt. 17-19 della l. n. 124/2007 che serve ad abilitare gli operatori dei servizi di informazione e sicurezza al compimento di atti costituenti reato laddove quest'ultimi siano necessari per le attività di sicurezza nazionale[23].

Tralasciando i presupposti e le dinamiche applicative, qui rileva in particolare lo speciale regime

20. V. Fiorinelli–Zucca 2024, p. 9.
21. Così come recentemente puntualizzata dalla riforma Cartabia al codice di procedura penale. V. Curtotti 2022, p. 198 ss.
22. La disciplina delle pseudo notizie si ricava da quella dell'art. 335 c.p.p. per le notizie che costituiscono reato e dall'art. 109 disp. att. c.p.p., il cui combinato disposto abilita le Procure a tenere un registro dove vengono annotati atti e comunicazioni di fatti che non hanno rilevanza penale. La dinamica processuale attesta come nel registro delle pseudo-notizie vengano annotati fatti che, giunti alla procura come notizie solo nominalmente di reato, vengono successivamente accertati come privi di rilevanza penale V. Di Bitonto 2006, p. 113 ss. V. anche Sottani 2021; Valentini 2020.
23. V. Amato 2024; Ricotta 2024, p. 65 ss.; Montagnese–Neri 2016; Mosca 2008, p. 235 ss. e Marzaduri 2007, p. 735 ss.

di segretezza stabilito per le indagini penali eventualmente avviate su fatti commessi sotto lo scudo delle garanzie: l'art. 19 l. n. 124/2007 prescrive al pubblico ministero di iscrivere la notizia e conservare gli atti di indagine in un separato registro "segreto" allo scopo di preservare l'anonimato degli operatori dei servizi e la riservatezza delle relative attività fintanto che viene verificata la legittimità delle autorizzazioni a commettere reato.

La dinamica processuale dell'istituto è incentrata sulla risoluzione di un conflitto tra poteri che si consuma quando le attività dei servizi sono incise da quelle della magistratura: quando il pubblico ministero si imbatte in un reato commesso dai servizi, avvia una procedura di interpello con il DIS e con il Presidente del consiglio teso a verificare se l'autorizzazione è stata effettivamente rilasciata e il fatto sia stato compiuto entro i limiti di legge. In questo contesto, il segreto serve a tutelare l'integrità delle ragioni di sicurezza nazionale per tutto il corso dell'interpello tra potere esecutivo e giudiziario.

Se la risposta è affermativa, e quindi sussistono i presupposti delle garanzie, il procedimento penale si arresta e quanto documentato nel registro separato ex art. 19 l. n. 124/2007 viene mantenuto segreto ben oltre il corso del procedimento.

Diversamente, se l'autorizzazione manca o eccede i limiti di legge, il procedimento penale, e con esso il regime divulgazione degli atti di indagine, prosegue seguendo il corso ordinario.

Si tratterebbe quindi di mutuare un regime di segretezza ad hoc degli atti di indagine per tutelare l'anonimato dei penetration tester da quello disciplinato dalle garanzie funzionali, ma siffatta soluzione deve essere menzionata per essere esclusa: l'istituto in discorso, e con esso il particolare regime di segretezza del fascicolo preliminare che è parte integrante del complessivo equilibrio normativo, è assolutamente speciale perché giustificato da quelle supreme ragioni di sicurezza nazionale nelle quali si radicano le attività dei Servizi di informazione che le garanzie funzionali sono chiamati a proteggere.

Pertanto, l'istituto, confinato com'è in quello specifico ambito, non può essere spacchettato e fatto oggetto di applicazione estensiva.

11. Conclusioni

Si è ampiamente illustrato come l'assenza di una chiara esenzione legale espone i penetration tester a potenziali responsabilità penali e civili, creando un clima di incertezza che può disincentivare la collaborazione essenziale tra attori pubblici e privati nel campo della cybersicurezza.

La designazione del CSIRT Italia quale organo competente rappresenta un passo importante, ma restano aperte questioni fondamentali che riguardano proprio l'esenzione da responsabilità per i tester di sicurezza e la tutela dell'anonimato dei segnalanti quali pilastri delle politiche di vulnerability disclosure indicati dalla NIS 2.

In questo contesto, l'adozione di una scriminante procedurale emerge come la soluzione più efficace, capace di eliminare l'antigiuridicità delle condotte dei tester quando queste sono svolte in conformità a procedure autorizzate e sotto il controllo dell'autorità competente, in questo caso l'Agenzia per la Cybersicurezza Nazionale, e al tempo stesso tutelare l'anonimato del segnalante sulla scorta delle conseguenze che si verificherebbero nella dinamica processuale.

La tutela dell'anonimato è infatti una garanzia strutturale per la protezione dei tester da possibili ripercussioni legali o professionali e per incentivare la segnalazione tempestiva delle vulnerabilità e, come si è visto, è legato a doppio filo con la dinamica del processo penale che, a sua volta, si impernia sulla rilevanza penale delle condotte di testing.

In definitiva, il pilastro per una politica nazionale di vulnerability disclosure non può che essere un quadro normativo che elimini, o quantomeno minimizzi la rilevanza penale delle attività di testing condotte per finalità legittime, così da rimuovere a cascata gli ostacoli alla tutela della riservatezza da assicurare ai segnalanti, incentivando la cooperazione necessaria per affrontare efficacemente le minacce alla sicurezza cibernetica.

Riferimenti bibliografici

G. Amato (2024), *Le garanzie funzionali dell'operatore dei servizi di informazione*, in "Sistema penale", 7 novembre 2024

R. Aprati (2010), *La notizia di reato nella dinamica del procedimento penale*, Jovene, 2010

A. Cadoppi, S. Canestrati, A. Manna, M. Papa (a cura di) (2023), *Cybercrime*, Utet, 2023

F. Consulich (2018), *Lo statuto penale delle scriminanti. Principio di legalità e cause di giustificazione: necessità e limiti*, Giappichelli, 2018

D. Curtotti (2022), L'*iscrizione della notizia di reato e il controllo del giudice*, in G. Spangher (a cura di), "La riforma Cartabia", Pacini giuridica, 2022

M.L. Di Bitonto (2006), *L'avocazione facoltativa*, Giappichelli, 2006

Enisa (2016), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2016

G.M. Evaristi (2021), Whistleblowing*, tutela dell'anonimato e processo penale: tra limiti costituzionali e orizzonti convenzionali*, in "Diritto Penale e Processo", 2021, n. 7

G. Fiorinelli, M.V. Zucca (2024), *Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU*, in G. D'Angelo, F. Luccio, F. Palmieri (a cura di), "Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024)", paper 45, vol. 3731, CEUR, 2024

R. Flor (2020), *Ethical hacker, assolti ma non troppo: le "zone grigie" del diritto penale*, in "Agenda Digitale", 1 ottobre 2020

R. Flor (2020-a), *Il diritto penale alla prova dell'*hands-on *dell'*ethical hacking, in "Diritto di Internet", 2020, n. 1

A.D. Householder, G. Wassermann, A. Manion, C. King (2017), *The CERT Guide to Coordinated Vulnerability Disclosure*, Software Engineering Institute, Carnegie Mellon University, 2017

E. Marzaduri (2007), *Art. 19 - Opposizione della speciale causa di giustificazione all'autorità giudiziaria* (commento alla l. n. 3.8.2007 n. 124 - Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto di Stato), in "Legislazione penale", 2007, n. 3

A. Montagnese, C. Neri (2016), *L'evoluzione della sicurezza nazionale in Italia*, in "Sistema di informazione per la sicurezza della Repubblica", 2016

C. Mosca (2008), *Le garanzie funzionali*, in C. Mosca, S. Gambacurta, G. Scandone, M. Valentini (a cura di), "I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)", Giuffrè, 2008

NIS Cooperation Group (2023), *Guidelines on Implementing National Coordinate Vulnerability Disclosure Policies*, 2023

W. Nocerino (2023), *Le nuove norme di prevenzione e contrasto alla criminalità informatica*, in "Penale Diritto e Procedura", 9 novembre 2023

P.P. Paulesu (2023), *Sub Art. 332*, in A. Giarda, G. Spangher (a cura di), "Codice di procedura penale commentato", Wolters Kluwer, 2023

L. Pupillo, A. Ferreira, G. Varisco (2018), *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*, CEPS Task Force Reports, 2018

F.N. Ricotta (2024), *Arresto e garanzie funzionali nella legge n. 124 del 2007,* in "Rivista giuridica delle forze armate e di polizia", 2024, n. 1

S. Rossa (2023), *Cybersicurezza e pubblica amministrazione*, Edizioni Scientifiche Italiane, 2023

I. Salvadori (2017), *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in "Rivista italiana di diritto e procedura penale", 2017, n. 2

D. Scarpino (2023), *Le innovazioni apportate dalla Riforma Cartabia in tema di iscrizione della notitia criminis*, in "Penale Diritto e Procedura", 26 luglio 2023

A. Sessa (2023), *Le giustificazioni procedurali nella teoria del reato*, Edizioni Scientifiche Italiane, 2023

S. Sottani (2021), *Il controllo giudiziale sulle pseudo notizie di reato*, in "Archivio Penale", 2021, n. 3

R. Ursi (2023), *La sicurezza cibernetica come funzione pubblica*, in R. Ursi (a cura di), "La sicurezza nel cyberspazio", Franco Angeli, 2023

C. Valentini (2020), *Obbligatorietà dell'azione penale, patologie della prassi e mancanza di controlli*, in "Rivista di diritto processuale", 2020, n. 3