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

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0144 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

Federico Niccolò Ricotta

Vulnerability disclosure e *penetration testing*: questioni da normare

L'Autore è assegnista di ricerca presso l'IGSG/CNR

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Nel progressivo impegno legislativo nel campo della sicurezza cibernetica il disegno di legge governativo C 1717 (XIX legislatura) è l'ulteriore tassello utile a blindare lo spazio nazionale e a conformare l'ordinamento interno alle direttive europee.

I profili di intervento sono molti, ma i più convergono sulle modifiche alla legislazione penale in materia di criminalità informatica, responsabilità delle persone giuridiche e competenza della Procura Nazionale Antimafia.

C'è tuttavia un aspetto speculare alle politiche di criminalizzazione ancora non compiutamente trattato ed essenzialmente legato alla dimensione lecita delle attività informatiche offensive realizzate per scopi di sicurezza cibernetica.

Il contesto di riferimento è quello dell'adozione di politiche c.d. di *coordinated vulnerability disclosure* (CVD), espressione con la quale si indica la complessiva regolazione delle pratiche di rilevare, segnalare e gestire le vulnerabilità dei sistemi informatici da parte di sviluppatori, ricercatori e autorità pubbliche.

Tra i vari profili che compongono queste politiche spicca quello della responsabilità di chi controlla la sicurezza dei sistemi: far emergere una vulnerabilità richiede che vengano svolti i c.d. *penetration test*, azioni di sicurezza informatica che possono implicare il ricorso ad attività offensive per saggiare la resistenza di un sistema: per esempio, simulando un attacco come un accesso forzoso ad una rete o un apparato.

Questi stessi test, sebbene siano determinanti nelle prassi di sicurezza, possono essere considerati illeciti ed esporre gli operatori a ripercussioni sul piano penale e civile (per esempio, laddove siano svolti senza il consenso del proprietario del sistema verificato) con potenziali effetti paralizzanti sul piano dello sviluppo e dell'ordinata gestione del fenomeno: da qui, la necessità dell'intervento regolatorio.

2. La fonte del dovere di adottare una politica di CVD è l'art. 12 della direttiva NIS 2.

La direttiva considera le pratiche di *vulnerability disclosure* cruciali per la sicurezza cibernetica e, come tali, da incentivare e regolare (v. i considerando nn. 58 e 60). Sono tracciate allo scopo due

indicazioni alle quali adeguarsi: assicurare ampia e libera partecipazione della comunità di riferimento ma nel contesto di una gestione ordinata della sicurezza cibernetica.

Il richiamo alla partecipazione è piuttosto ricorrente e suggerisce di prediligere politiche nazionali che assicurino il coinvolgimento diffuso e trasparente di tutti i possibili soggetti interessati (sviluppatori, aziende, ricercatori, autorità), soprattutto volgendo un occhio di riguardo alla posizione della comunità tecnico-scientifica che è da porre al riparo dalle conseguenze penali e civili della propria attività. Testimone dell'importanza attribuita alla comunità scientifica e all'indipendenza degli operatori della *cybersecurity* è anche l'invito della medesima NIS 2 (v. considerando 52) a dotarsi di strumenti e applicazioni c.d. *open source*, per dotarsi di processi di sviluppo e verifica più trasparenti e soprattutto "processi di individuazione delle vulnerabilità guidati dalla comunità", quali fattori determinanti per conseguire livelli più elevati di sicurezza.

Sul piano della gestione complessiva del fenomeno, la direttiva imprime comunque una preferenza per un processo accentrato e affidato al coordinamento delle autorità nazionali di settore, affinché le vulnerabilità non siano scoperte e comunicate in modo indiscriminato e potenzialmente dannoso.

Da qui, la prescrizione dell'art. 12 della direttiva di adottare a livello nazionale politiche che consentano alle persone fisiche o giuridiche di rilevare e segnalare in forma anonima le vulnerabilità e adottare le necessarie azioni susseguenti.

Per il vero, lo statuto giuridico di queste politiche è già stato in parte eretto: l'art. 2 del disegno di legge 1717 irrobustisce il dovere di conformarsi alle prescrizioni di sicurezza impartite dall'Agenzia Cyber, che si aggiunge ai doveri di segnalazione di rischi e incidenti già previsti nella normativa primaria.

Restano scoperti, s'anticipava, i profili di responsabilità degli operatori della sicurezza e i relativi meccanismi di tutela.

3. Nella loro dimensione massimalista le politiche di CVD si riassumono nella triade emersione, comunicazione e correzione di una vulnerabilità.

La vulnerabilità è anzitutto un insieme di condizioni che consente la violazione della sicurezza o della riservatezza di un sistema: si sostanzia in una falla nella sicurezza 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, 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.*, per quelle dei sistemi che rientrano nel perimetro di sicurezza cibernetica e che, come tali, sono sottoposti alla vigilanza dell'Agenzia per la cybersicurezza nazionale. Questa comunicazione circa l'esistenza della vulnerabilità è l'attività di *disclosure*: in Italia, per esempio, è il CSIRT ad essere destinatario delle informative sui rischi dei sistemi e delle infrastrutture digitali.

4. La *vulnerability disclosure* è così un processo tramite il quale vengono segnalate le vulnerabilità a chi può risolverle, tendenzialmente prima che esse siano rese note al pubblico generale. Questo processo, quindi, consente a venditori, sviluppatori, gestori e ricercatori IT di cooperare per trovare soluzioni che riducano il rischio associato alle vulnerabilità: un ricercatore, colui che trova che scopre un difetto in un sistema, informa lo sviluppatore (venditori, fornitori) del sistema riguardo al difetto e alle possibili correzioni, affinché quest'ultimo possa assumere misure di mitigazione (patch, monitoraggio del traffico, blocco) per eliminare o ridurre il rischio associato alla vulnerabilità.

5. Le falle nella sicurezza informatica emergono perché vengono condotti i c.d. *penetration test*, pratiche che simulano un attacco ad un sistema per identificarne le debolezze. I test possono essere svolti da soggetti interni alla società che sviluppa il sistema, oppure da esterni, soggetti pubblici o privati (come enti di ricerca o organizzazioni no profit), che operano con o senza la consapevolezza ed il consenso delle entità proprietarie dei sistemi.

Per questo tali attività, così come gli strumenti utilizzati per i test, possono costituire una condotta illecita penalmente o civilmente rilevante. 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 (o le amministrazioni) a non far emergere pubblicamente i difetti dei propri

prodotti e, quindi, a non consentire che siano i terzi a condurre i *penetration test*.

6. I profili di rilevanza penale, comuni alla persona fisica e a quella giuridica (quest'ultima ne risponde nei limiti della responsabilità *ex* d.lgs. n. 231/2001), riguardano l'attività di emersione e, in misura minore, quella successiva della comunicazione.

Quanto all'emersione, tanto la materiale esecuzione del test quanto talune delle attività preparatorie possono avere conseguenze penali: il test può integrare una delle condotte che puniscono l'accesso, lo svolgimento di operazioni abusive ai sistemi informatici o la manipolazione dei dati senza autorizzazione (così agli artt. 615-*ter* c.p., 617-*bis* c.p., 635-*bis* – art. 635-*quinquies* c.p.); del pari, anche l'approvvigionamento delle apparecchiature necessarie a condurre il test può integrare uno dei reati che puniscono procacciamento, detenzione e uso di certi *software* che la legge ritiene pericolosi (come i programmi c.d. *dual use*, così all'art. 461 c.p., artt. 625-*quater* e *quinquies* c.p, art. 617-*quinquies* c.p., ma anche artt. 171-*bis* e *ter* della l. 22 aprile 1941, n. 633, c.d. Legge sulla protezione del diritto di autore).

In tutte queste fattispecie assume rilevanza la violazione della volontà del titolare del sistema informatico che, in forza del proprio *ius excludendi alios*, potrebbe non autorizzare l'accesso ai propri sistemi o risorse da parte di soggetti diversi dai propri. Da qui, il fondamento di una responsabilità che prescinde dai motivi del soggetto agente e/o dalla natura dei programmi, dei dati o delle informazioni archiviate o trattate nel sistema informatico, ovvero dai "risultati" o dalle "conseguenze" del fatto.

Ulteriormente, sul piano della comunicazione, una *disclosure* della vulnerabilità potrebbe integrare il reato di diffamazione se le informazioni sulle possibili criticità del sistema giungono incontrollate al pubblico.

Va da sé che, per entrambi i profili, la responsabilità penale è accompagnata dalle possibili pretese di natura risarcitoria nutrite dai titolari dei sistemi violati.

7. Dati i termini della problematica, può essere utile guardare alle soluzioni già sperimentate altrove. Ad oggi sono quattro gli Stati membri dell'Unione europea, Francia, Olanda, Lituania e Belgio, che hanno proceduto a introdurre policy di CVD e a regolamentare la responsabilità penale, prevedendo forme di *safe harbour* per i tester.

Tra questi, è interessante dare atto dell'equilibrio raggiunto dalla Repubblica Francese, dove una modifica introdotta all'art. 40 del codice di procedura penale consente al pubblico ministero di non esercitare l'azione penale nei confronti del *penetration tester*.

Le condizioni dell'inazione sono poste dagli art. 47 della Legge per una Repubblica Digitale (LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique) e dall'art. L 2321-4 *Code de la defense*: i ricercatori che segnalano una vulnerabilità devono agire in buona fede, nella consapevolezza di star procedendo legalmente e secondo i regolamenti di settore; la vulnerabilità deve essere segnalata tempestivamente ed esclusivamente all'ANSSI (*Agence nationale de la sécurité des systèmes d'information*) l'autorità nazionale francese per la cybersicurezza, che a sua volta garantisce l'anonimato del segnalante e la riservatezza delle condizioni di scoperta del vulnerabilità (così da tutelare le aspettative di tutti i soggetti coinvolti).

Così, soddisfatto l'onere di comunicazione all'autorità di settore, il pubblico ministero può valutare autonomamente la meritevolezza dell'attività del *pen tester* e, se del caso, non promuovere l'azione penale nei suoi confronti.

8. In sé per sé considerata, la soluzione francese è una scelta incentivante perché l'esenzione da responsabilità è essenzialmente processuale, e dipende dalla scelta discrezionale del PM di non procedere se ritiene l'attività del tester conforme a buona fede. A sua volta, in questo giudizio che la Procura conduce sulla meritevolezza dell'azione del tester confluisce anche quello sulla diligenza nell'attenersi alle indicazioni dell'autorità governativa di settore: tanto in termini di aderenza ai regolamenti adottati, tanto nell'esauriente trasmissione dei dati relativi alla propria attività di test. Così, l'esenzione di responsabilità opera in sinergia tra il piano penale e quello regolatorio.

Va da sé che in Francia l'azione penale è discrezionale: è per questo che la loro soluzione può contemplare una valutazione dell'agito del tester condotta secondo criteri così elastici.

9. *De iure condendo*, raggiungere un equilibrio analogo in Italia è un'operazione decisamente più difficoltosa. Una politica normativa CVD che contempli l'area del penalmente rilevante deve infatti

conformarsi ai principi di stretta legalità e dell'obbligatorietà dell'esercizio dell'azione penale (che ne è conseguenza).

Ipotizzando quindi un'area di esenzione da responsabilità satisfattiva delle aspettative della NIS 2 ma coerente con il sistema italiano, una soluzione papabile potrebbe essere quella di coniare una scriminante o una condizione di non punibilità per determinante attività del *penetrator tester*. Così procedendo, la conseguenza sul piano processuale sarebbe quella di promuovere l'archiviazione del procedimento penale o il proscioglimento dell'imputato con riflessi, laddove si operasse sull'antigiuridicità, anche sull'eventuale responsabilità civile.

Ai fini di una qualsiasi esimente, discernere le attività illecite da quelle lecite, e di conseguenza valutare la meritevolezza dell'attività del tester per esentarlo da responsabilità, richiede parametri oggettivi e condizioni poste dalla legge: *i.e.* individuando le condotte rilevanti e in quale proporzione l'offesa arrecata dal test può dirsi giustificata per perseguire obiettivi di sicurezza cibernetica, conferendo eventualmente rilevanza al grado di conformità della condotta dell'agente alle linee guida di settore e, più in generale, ai doveri nei confronti dell'Agenzia nazionale di settore.

Dal punto di vista soggettivo, andrebbe inoltre considerata la diversa situazione di chi svolge attività istituzionali di sicurezza da quella dei privati.

Per il personale in ruolo all'ACN o delle forze di polizia risulta decisamente più semplice disegnare una scriminante speciale in ragione della rilevanza delle proprie funzioni di sicurezza che, sebbene in situazioni diverse, sono già assistite da esimenti penali (si pensi, *i.e.*, alla disciplina dell'agente sotto copertura ex art. 9 legge 16 marzo 2006, n. 146 o quella delle c.d. garanzie funzionali).

Diversamente, per i privati, siano essi persone fisiche o giuridiche, si deve soddisfare l'esigenza di promuovere l'indipendenza della ricerca e l'anonimato della segnalazione (art. 12 NIS 2) senza tuttavia giungere ad una liberalizzazione incontrollata di condotte pur sempre potenzialmente decettive, che potrebbero ben prestarsi ad usi strumentali o obliqui (incentivati da uno scudo penale troppo ampio).

Da qui, la necessità di considerare, anche ai fini dell'esenzione da responsabilità, il rispetto di obblighi regolamentari e amministrativi che consentono un'ordinata e consapevole gestione della sicurezza cibernetica da parte dell'Agenzia, l'organo così deputato a fornire le indicazioni guida e a verificare le circostanze delle attività di sicurezza potenzialmente offensive.

10. Come si è visto, nel disegno di legge governativo C 1717 la questione della *vulnerability disclosure* non è stata ancora compiutamente regolata.

Tuttavia, l'assenza di normazione degli ulteriori profili, soprattutto quelli che insistono sulla responsabilità penale, non deve sorprendere: le politiche di CVD sono una problematica piuttosto complessa da risolvere, in parte per questo dualismo tra la dimensione lecita e illecita ma soprattutto per le numerose implicazioni che esso comporta sul piano dei diritti privati e su quello della sicurezza pubblica.