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

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0143 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

GAIA FIORINELLI

Il *ransomware* nel DDL Cybersicurezza: dalla fattispecie di estorsione "informatica" al coordinamento tra indagini e *incident response*

L'Autrice è ricercatrice in Diritto penale alla Scuola Superiore Sant'Anna di Pisa

La ricerca è stata svolta nell'ambito del Progetto PNRR "Partenariato Esteso" *SERICS - SEcurity and RIghts in the CyberSpace, Spoke 1 – Cyberights* (CUP J53C22003110001), finanziato dall'Unione europea - Next Generation EU

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. Tra gli interventi di maggiore interesse previsti dal Capo II del ddl Cybersicurezza si segnala la proposta di introdurre un'apposita fattispecie penale denominata «estorsione informatica» o «estorsione mediante reati informatici» (art. 15, co. 1, lett. m), mediante la quale s'intende reagire alla «gravità» e alla «frequenza» dei «ricatti realizzati attraverso la minaccia o l'attuazione di attacchi informatici» (ddl, p. 7).

Il ddl fa riferimento ai c.d. attacchi *ransomware*, che, secondo i dati del C.N.A.I.P.I.C., hanno costituito nel 2023 la tipologia più diffusa di "attacchi gravi" (34%), con un rilevante impatto a livello nazionale sulla PA e sull'erogazione di servizi (Clusit 2024). Come rilevato da ENISA e dal *Cybercrime Convention Committee* del Consiglio d'Europa, gli attacchi *ransomware* rappresentano una delle forme più gravi di cybercriminalità dell'ultimo decennio, ai danni di individui, imprese e pubbliche amministrazioni (ENISA 2022; T-CY 2022); nondimeno, si tratta di una fenomenologia criminosa che, in virtù della particolare complessità dell'*iter criminis*, risulta tuttora priva di una rilevanza penale unitaria, potendo un singolo attacco *ransomware* integrare molteplici (ma distinti) reati (informatici e non) nelle singole fasi della sua esecuzione (Cybercrime Convention Committee 2022), con un connesso rischio di parcellizzazione e dispersione delle attività di *law enforcement* (Wall 2021).

Prima di analizzare la soluzione ideata dal legislatore italiano, occorre rilevare come un attacco *ransomware* (dall'inglese *ransom*, «riscatto») si componga generalmente (e semplificando): (i) di una prima fase più propriamente "informatica", nella quale l'attaccante introduce in vario modo un *malware* nel computer *target*, per criptare file, altri contenuti o il sistema stesso e renderli così inaccessibili al titolare (più nel dettaglio: ENISA, 2022); e (ii) di una seconda fase invece "estorsiva", nella quale l'attaccante richiede al bersaglio il pagamento di un riscatto (solitamente in criptovalute), in cambio del ripristino della funzionalità o dell'accessibilità dei dati o del sistema (Cybercrime Convention

Committee 2022), ovvero (o anche) dietro la minaccia di segnalare il *data breach* alle autorità o di divulgare pubblicamente i dati o la loro violazione, o ancora di venderli sul *dark web* (c.d. doppia estorsione; Hyslip-Burruss 2023; ENISA 2022). Come rilevato da Europol (Europol 2023), inoltre, dietro gli attacchi *ransomware* si celano spesso gruppi strutturati secondo il *business model* del *crime-as-a-service* (o *ransomware-as-a-service*), incentrati su "programmi di affiliazione" aperti alla libera adesione da parte di utenti della rete, i quali possono contribuire dietro compenso a una delle molteplici fasi del "processo", secondo il paradigma definito dalla letteratura criminologica «crimine *(dis)organizzato*» (Wall 2015).

Per reagire a questa fenomenologia criminosa, fonte di un crescente allarme sociale – anche in quanto realizzata, sempre più spesso, ai danni di pubbliche amministrazioni –, il legislatore si propone d'intervenire sia sul piano del diritto penale *sostanziale*, sia mediante un migliore coordinamento *procedurale* tra le attività di indagine e le attività di c.d. *incident response*, sul presupposto che, nel caso di attacchi informatici, il perseguimento prioritario di un'esigenza (indagine, oppure ripristino tempestivo) rischi spesso di compromettere l'altra.

2. L'art. 15, co. 1, lett. m del ddl prevede, dunque, l'introduzione di un terzo comma nell'art. 629 c.p. (*Estorsione*), per punire chiunque «costring[a] taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno», mediante le «condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinquies*» ovvero la «minaccia di compierle». In buona sostanza, nella "estorsione informatica" la *violenza* e la *minaccia*, che costituiscono le condotte tipiche produttive della costrizione nella fattispecie di estorsione "comune" (Marini 1990), sono sostituite dal riferimento alle *condotte* di una serie di reati informatici (*Accesso abusivo, Intercettazione, impedimento, etc. […] o Falsificazione, alterazione, etc. […] di comunicazioni informatiche, Danneggiamento di informazioni, dati e programmi informatici, Danneggiamento di sistemi informatici,* anche *di pubblica utilità),* ovvero alla «*minaccia di compierle*».

In termini generali, si può accogliere con favore l'intento del legislatore di "aggiornare" le fattispecie penali relative al *cybercrime*, a fronte di fenomeni criminosi, come il *ransomware*, che si sono diffusi in epoca recente e che solo con difficoltà possono ricondursi alle incriminazioni già esistenti. Invero, sebbene non manchino disposizioni per qualificare penalmente i singoli segmenti del complessivo *iter criminis* (dalla programmazione del *malware*, al danneggiamento del sistema informatico, etc.: Cybercrime Convention Committee 2022), nessuno dei "reati informatici" esistenti intercetta il disvalore della componente "estorsiva" degli attacchi *ransomware* e la loro conseguente natura pluri-offensiva (che unisce alla violazione della sicurezza informatica l'eventuale lesione patrimoniale e la lesione della libertà di autodeterminazione della vittima).

Del resto, anche l'applicazione della fattispecie di estorsione "comune" a questa tipologia di attacchi solleva alcune questioni interpretative. Nonostante, ad esempio, l'Agenzia delle Entrate, nella risposta n. 149/2023, si sia espressa per la generale riconducibilità dei casi di *ransomware* all'art. 629 c.p., non risulta affatto scontata la possibilità di qualificare le condotte di "aggressione informatica" realizzate dai *cyber*-attaccanti, pur potenzialmente produttive di una *costrizione*, alla stregua delle nozioni di *violenza* o *minaccia* di cui all'art. 629, co. 1, c.p. Con riguardo alla *violenza*, potrebbe invero farsi riferimento all'art. 392, co. 3, c.p., che configura la *violenza sulle cose* anche allorché sia danneggiato un programma informatico o sia turbato il funzionamento di un sistema informatico (senza nessun riferimento, tuttavia, al "sequestro" dei dati). Con riferimento alla *minaccia*, invece, nella maggior parte degli attacchi, più che la prospettazione di un male ingiusto, si riscontra una "aggressione informatica" già compiuta, antecedente rispetto alla richiesta di "riscatto" (sul punto, tuttavia, la giurisprudenza riconduce alla nozione di *minaccia estorsiva* anche la richiesta di denaro accompagnata dalla prospettazione della mancata restituzione del bene sottratto: Cass. pen., sez. II, n. 25213/2019).

3. Poste tali premesse di ordine generale, s'intende anche sottolineare come la fattispecie descritta nel disegno di legge presti il fianco ad alcune censure.

In primo luogo, la realtà degli attacchi *ransomware* avrebbe reso forse preferibile, in luogo del ricorso *tout court* alla fattispecie di estorsione, il "recupero" del modello del "reato commesso *a scopo di estorsione*" (il quale già nel codice Zanardelli era punito a titolo di "ricatto", quale fattispecie

distinta dall'estorsione, e che tuttora, secondo giurisprudenza costante, presenta una struttura diversa rispetto all'art. 629 c.p., come affermato ad es. da Cass. pen., Sez. Unite, n. 962/2003). Tale diversa struttura della fattispecie parrebbe preferibile non foss'altro perché, ad esempio, nel caso del delitto commesso *a scopo di estorsione* il reato sarebbe integrato a prescindere dall'avvenuto versamento del "prezzo della liberazione" dei sistemi informatici o dei dati (posto che il profitto costituirebbe soltanto l'oggetto del dolo specifico), mentre nell'estorsione il conseguimento del profitto ingiusto rappresenta un elemento costitutivo del reato, in assenza del quale può ritenersi tutt'al più integrata la fattispecie tentata (per un esempio dell'uso del requisito dell'*intent to extort* per la costruzione del reato di "*ransomware*" nel § 523 *California Penal Code*: Lubin 2022).

Anche in una prospettiva sistematica, peraltro, non va trascurato come in casi analoghi (es. sequestri di persona), alla riforma del delitto di estorsione (mediante una specificazione dei mezzi con funzione aggravante), sia stata preferita la creazione di varianti "a dolo specifico" (punite più gravemente) di fattispecie a "fine generico", per realizzare una «specializzazione della tutela» (Padovani 2023) funzionale a enucleare il diverso «significato offensivo» del perseguimento di una specifica e ulteriore *finalità* (ad es. estorsiva), nella commissione di un determinato reato (es. sequestro di persona).

Tale questione strutturale si riverbera, del resto, sulla stessa definizione del trattamento sanzionatorio. Per la fattispecie di "estorsione informatica", infatti, l'art. 15, co. 1, lett. m del ddl prevede limiti edittali molto elevati (reclusione da sei a dodici anni e multa da euro 5.000 a euro 10.000 per la fattispecie "base") e, soprattutto, più elevati rispetto a quelli dell'estorsione "comune" di cui al co. 1. Se, tuttavia, la finalità offensiva *ulteriore* generalmente giustifica la comminatoria di pene più elevate nei delitti a dolo specifico (rispetto alle ipotesi a "fine generico"), non è invece scontato che il ricorso a un "mezzo informatico" sia in ogni caso più grave, rispetto alla *violenza* o alla *minaccia*, nella commissione del delitto di estorsione. Il nuovo co. 3 dell'art. 629 c.p., dunque, parrebbe creare una disparità di trattamento potenzialmente irragionevole (in termini suscettibili di censura d'illegittimità costituzionale; Frigo 2013). Può dubitarsi, infatti, che l'estorsione *informatica* sia di per sé e in ogni caso *più grave* rispetto all'estorsione "comune", nella quale la violenza o la minaccia possono attingere anche l'integrità fisica della persona offesa; soprattutto, la potenziale irragionevolezza emerge nei casi virtualmente già rientranti nell'art. 629, co. 1, c.p. (ad es., la «*minaccia di compier[e]*» reati informatici, prevista dal nuovo co. 3, sarebbe già rilevante alla stregua di ordinaria *minaccia* ai sensi del co. 1, ma risulterebbe tuttavia punita più gravemente di ogni altra minaccia estorsiva).

Venendo, poi, alle ipotesi aggravate – punite con la pena (anch'essa molto elevata) della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000 – la riforma si espone a una censura in punto di tecnica legislativa. Per l'individuazione delle aggravanti, infatti, la disposizione rinvia alle "circostanze indicate nell'ultimo capoverso" dell'art. 628 c.p., riprendendo la stessa formulazione dell'art. 629, co. 2, c.p.: tale disposizione, tuttavia, già scontava un difetto di coordinamento con lo stesso art. 628 c.p., a seguito dell'introduzione, in tale ultima disposizione, di due ulteriori commi (dopo il co. 3 che elenca le aggravanti) nel 2009 e nel 2017. Se, dunque, già l'art. 629, co. 2, c.p. necessiterebbe di aggiornamento, è criticabile che la disposizione di nuova introduzione ne riproduca persino il mancato coordinamento con le modifiche dell'art. 628 c.p. (correttamente la proposta emendativa 11.24 tentava di ovviare a tale inconveniente, ma non è stata approvata). Del resto, la disciplina risultante dal rinvio si appalesa doppiamente insoddisfacente. Per un verso, infatti, si rinvia "in blocco" alle aggravanti previste per il delitto di rapina, senza considerare che la maggior parte di esse risulterà assolutamente inapplicabile agli attacchi *ransomware*, in virtù della differente dinamica esecutiva (ad es. la commissione con uso di armi, o da parte di persona travisata, o in luoghi di privata dimora, o di pubblico trasporto, o nei confronti di persona che si trovi nell'atto di fruire dei servizi di istituti di credito, uffici postali o sportelli automatici, per citarne soltanto alcune). Per altro verso, la disposizione risulta disallineata rispetto alle aggravanti speciali previste per gli altri reati informatici, anche sulla base del medesimo ddl (si fa riferimento all'elenco di aggravanti tipizzate dall'art. 615-*ter*, co. 2 e 3, c.p., ove ad es. si sottopone a pena più elevata l'attacco realizzato ai danni di un sistema informatico di interesse pubblico, alle quali, all'esito del riordino proposto

nel ddl, rinvierebbero gli artt. 615-*quater*, 617-*bis*, 617-*quater*, 635-*quater*.1 c.p.).

4. Completano la disciplina penale della nuova «estorsione informatica» alcune ulteriori disposizioni "di contorno".

Anzitutto, risulteranno applicabili anche ai casi previsti dall'art. 629, co. 3, c.p. le nuove circostanze attenuanti del "fatto di lieve entità" (attenuante a effetto comune) e del "ravvedimento"/"collaborazione" *post delictum* (attenuante a effetto speciale), previste dal nuovo art. 639-*ter* c.p. (art. 15, co. 1, lett. s). La disposizione riproduce un modello frequentemente adottato dal legislatore, specie in abbinamento con un generale inasprimento delle pene (secondo un approccio "*stick and carrot*" esplicitato nella stessa relazione al ddl): se il riferimento alla «lieve entità» risulta coerente (almeno rispetto alla fattispecie di estorsione) con la sentenza della Corte costituzionale n. 120/2023, e postulerà una valutazione di natura, specie, mezzi, modalità o circostanze dell'azione, nonché del danno o pericolo, la riduzione di pena per la collaborazione *post delictum* corrisponde a un modello concepito inizialmente per i reati di criminalità organizzata e progressivamente esteso dal legislatore a diversi settori di criminalità "plurisoggettiva" (tuttavia, a differenza di quanto si prevede, ad es., in materia di reati contro la PA, non si richiede in questo caso che la collaborazione sia *efficace*).

Piuttosto inconferente con la realtà criminologica degli attacchi *ransomware* può risultare invece la previsione dell'art. 19 del ddl, nella parte in cui modifica l'art. 24-*bis* del d.lgs. 8 giugno 2001, n. 231, inserendo l'art. 629, co. 3, c.p. tra i reati presupposto della responsabilità amministrativa da reato dell'ente: come si anticipava, risulta difficile ipotizzare che gli attacchi *ransomware* possano promanare dagli enti economici che costituiscono i principali destinatari del d.lgs. 231/2001, trattandosi nella maggior parte di attività riconducibili a veri e propri gruppi criminali.

Sempre con riferimento alla disciplina collaterale, si segnala ancora l'omesso rinvio all'art. 629, co. 3, c.p. nelle disposizioni processuali modificate dall'art. 16 (che non estende all'estorsione informatica né la specifica competenza della Procura distrettuale, né il regime derogatorio in tema di durata delle indagini preliminari e proroga dei termini), con una conseguente asimmetria che, almeno a prima lettura, risulta ingiustificata.

5. Ancora, si vuole segnalare come, proprio per la gestione di attacchi di questo tipo – specialmente se realizzati ai danni di sistemi di pubblico interesse (in commissione il Sottosegretario Mantovano ha richiamato, quale caso paradigmatico, il «blocco della sala operatoria», rispetto al quale ci si domanda se sia «meglio ripristinarla subito», anche a costo di «altera[re] la scena del crimine», oppure se debbano privilegiarsi le esigenze di indagine, a costo di «lascia[re] bloccata la sala operatoria») –, il ddl Cybersicurezza disciplini anche, all'art. 21, il coordinamento tra attività d'indagine e *incident response*. In tale direzione, oltre ai reciproci obblighi di informazione tra il Procuratore Nazionale Antimafia e antiterrorismo e ACN, in relazione ai casi di comune competenza (es. art. 371-*bis*, co. 4-*bis*, c.p.p. e altri elencati), il nuovo co. 4-bis.3 dell'art. 17 d.l. 14 giugno 2021, n. 82 (conv. l. 109/2021), per come riformulato dall'art. 21, co. 1, lett. b del ddl non soltanto prevede che spetti al Pubblico Ministero impartire le disposizioni necessarie, in fase di indagine, per assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall'ACN ai fini di resilienza, ma soprattutto gli attribuisce la facoltà di disporre il differimento (motivato) di una di tali attività, qualora ciò sia necessario per evitare un grave pregiudizio per il corso delle indagini. Nel testo del ddl è, dunque esplicita la "poziorità" delle attività investigative sulle operazioni di *cyber*-resilienza, contenimento e ripristino: se la scelta è coerente con l'impostazione marcatamente "punitiva" del provvedimento, nel contesto internazionale la soluzione è invece la progressiva integrazione operativa tra *digital forensics* e *incident management* (Kent et al. 2006).

6. In conclusione, deve rilevarsi come l'intervento legislativo proposto con il ddl, nonostante l'apparente (quanto simbolica) "severità" nel ricorso allo strumento punitivo, risulti destinato a una scarsa efficacia quanto al contrasto degli attacchi *ransomware*. Invero, il ddl si limita all'introduzione della fattispecie di "estorsione informatica" senza contestualmente affrontare i principali nodi critici che tuttora ostacolano il perseguimento dei c.d. *computer crime* (ad es. la difficile identificazione degli autori e attribuzione degli attacchi; la proiezione extra-territoriale della giurisdizione nazionale), non valorizza la realtà empirico-criminologica dei *ransomware* (nella misura in cui, ad es., non

attribuisce rilevanza alle dinamiche di affiliazione in programmi di *crime-as-a-service*; non prevede alcuno strumento *patrimoniale*, sebbene si tratti di attacchi imperniati sulla richiesta di un "riscatto"; non disciplina il pagamento del *ransom*, nemmeno con un obbligo di notifica; non interviene sul "mercato nero" dei dati (Hyslip-Burruss 2023), né valorizza possibili strumenti innovativi (ad es. *blockchain analytics*, per tracciare le transazioni in *bitcoin*).

Riferimenti bibliografici

Clusit (2024), *Rapporto 2024 sulla sicurezza ICT in Italia*, 2024

Cybercrime Convention Committee (2022), *T-CY Guidance Note #12. Aspects of ransomware covered by the Budapest Convention*, 2022

ENISA (2022), *Threat Landscape for Ransomware Attacks*, 2022

Europol (2023), *Cyber-attacks: the apex of crime-as-a-service*, 2023

G. Frigo (2013), *I principi di proporzionalità e ragionevolezza nella giurisprudenza costituzionale italiana in materia penale*, 2013

T.S. Hyslip, G.W. Burruss (2023), *Ransomware*, in D. Hummer, J. Byrne (eds.), "Handbook on Crime and Technology", Edward Elgar Publishing, 2023

K. Kent, S. Chavalier, T. Grance, H. Dang (2006), *Guide to Integrating Forensic Techniques into Incident Response*, 2006

A. Lubin (2022), *The Law and Politics of Ransomware*, in "Vanderbilt Journal of Transnational Law", vol. 55, 2022

G. Marini (1990), voce *Estorsione*, in "Digesto delle Discipline Penalistiche", Utet, vol. IV, p. 377 ss., 1990

T. Padovani (2023), *Diritto penale,* XII ed., Giuffrè, 2023

D.S. Wall (2021), *The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending*, in "European Law Enforcement Research Bulletin", 2021

D.S. Wall (2015), *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in "The European Review of Organised Crime", vol. 2, 2015, n. 2