Razzante R, 'L'attribuzione degli attacchi informatici' (2022) 2 EJPLT, 215-241.
DOI : https://doi.org/10.57230/EJPLT222RR

EJPLT
ISSN 2704-8012



L'attribuzione degli attacchi informatici

The attribution of cyberattacks

RANIERI RAZZANTE
Contract Professor of Techniques for Anti-Money Laundering Risk Management at Alma Mater Studiorum Università di Bologna,
Contract Professor of Techniques and Rules of Cybersecurity, at Università degli Studi Suor Orsola Benincasa

Abstract

Il presente approfondimento si pone l'obiettivo di evidenziare gli attuali limiti del diritto nell'individuazione, e quindi della possibilità di sanzionare, gli attacchi informatici. Infatti, l'evoluzione tecnologica e le nuove frontiere della comunicazione hanno portato alla proliferazione di nuove condotte penalmente rilevanti, nonché ad una significativa espansione delle attività illecite, anche nel Metaverso, difficilmente controllabili. della materia.

The purpose of this paper is to highlight the current legal limitations in the identification and the possibility of sanctioning cyber-attacks. In fact, technological evolution and new frontiers of communication have resulted in the proliferation of new criminally relevant conducts, as well as a significant increase in illicit activities. This increase is affecting also the Metaverse, and today it appears to be hardly controllable.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: attribuzione; attacco informatico; cybersicurezza; cybersecurity; metaverso; cyberlaundering.

Summary: Introduzione: Il Metaverso: un locus commissi delicti atipico. – 1. Gli attacchi informatici: le minacce del nuovo millennio. – 2. Le tre fasi dell'attribuzione. La fase tecnica. – 3. (Segue) La fase politica. – 4. (Segue) La fase giuridica. – 5. La normativa europea: il Regolamento 2019/796/UE. – 6. Il nuovo volto del riciclaggio nell'era digitale: il cyberlaundering. – 7. Il fenomeno del cyberterrorismo. – 8. (Segue) La cybersicurezza in Italia: sviluppi del 2022. – 9. Direttiva NIS (Network and Information Security). – 10. (Segue) Direttiva NIS 2: i cambiamenti. – Conclusioni: Attacchi informatici ed attuale panorama sanzionatorio italiano: prospettive de iure condendo.

Introduction: Il Metaverso: un locus commissi delicti atipico.

Il Metaverso è una realtà digitale, risultante dall'insieme di dimensioni virtuali e reali interconnesse, in cui gli utenti vengono rappresentati da propri *alter ego*, definiti avatar [1].

Questo nuovo mondo fa sorgere molti interrogativi in merito alla possibilità di applicarvi le tradizionali categorie del diritto, ponendo l'interprete davanti a questioni quali la perseguibilità di azioni ivi poste in essere, la relativa qualificazione e la possibilità di effettiva comminazione della pena.

La prima ambiguità che si pone è la plausibilità o meno del ritenere che il Metaverso[2] possa rappresentare un vero e proprio *locus commissi delicti*, ed è ormai pacifico che una realtà diversa da quella fattuale sia idonea alla commissione di reati. È legittimo chiedersi come sciogliere il nodo dell'individuazione della competenza per territorio e, a tal fine, giova richiamare le considerazioni della Corte di Cassazione in merito alle ipotesi di diffamazione[3] a mezzo Internet, a detta della quale, ai fini «dell'individuazione della competenza, sono inutilizzabili, in quanto di difficilissima, se non impossibile individuazione, criteri oggettivi unici (…) Ne consegue che non possono trovare applicazione né la regola stabilita dall'art. 8 c.p.p., né quella fissata dall'art. 9 c.p.p., comma 1. (…) In tale articolato contesto è, quindi, imprescindibile fare ricorso ai criteri suppletivi fissati dal predetto art. 9 c.p.p., comma 2, ossia al luogo di domicilio dell'imputato»[4].

Inoltre, le condotte realizzate sul web si estrinsecano nell'emanazione o nella captazione di una serie di impulsi elettronici, interconnessi tra loro, indifferentemente dalla concreta ubicazione del soggetto agente. Per questa ragione il reato assume una connaturata ed inevitabile dimensione transnazionale.

---

[1] Termine che sta ad indicare la rappresentazione grafica e virtuale di un visitatore di sito web.

[2] F. SARZANA DI SANT'IPPOLITO, I.O. EPICOCO, M. PIERRO, *Il diritto del metaverso*, Torino, 2022 e D. DELFINO, *La corsa al metaverso e le criticità giuridiche*, in *Filodiritto*, 18 novembre 2022. Consultabile al sito: https://www.filodiritto.com/la-corsa-al-metaverso-e-le-criticita-giuridiche.

[3] Sul tema si veda anche P. ZARRA, *L'evoluzione applicativa della diffamazione via e-mail nell'era dello smart-working, commento a Cass. Pen., Sez. V, 8 aprile 2021, n. 13252*, in *Diritto di Internet*, 2021, IV, 733-735.

[4] Cass. Pen., sez. I, sent. 21.12.2010, n. 2739, in *Guida al diritto*, 2011, 23, 92.

In secondo luogo, sarebbe possibile rispondere positivamente alla possibilità di qualificare le condotte poste in essere sulla base delle ordinarie figure di reato, come dimostra l'ampia gamma dei crimini informatici già tipizzati. Ad esempio, la giurisprudenza ha ricondotto al concetto di luogo aperto al pubblico, rilevante ai fini dell'integrazione dell'art. 660 c.p., una pagina Facebook, equiparandola ad una pubblica agorà virtuale. Ad ulteriore dimostrazione dell'esaustività del catalogo di fattispecie, si possono riportare le ipotesi di abuso sessuale, di istigazione al suicidio, di revenge porn, di minaccia, ecc.

Un ulteriore quesito interessa il rispetto del principio di materialità e, in merito, si è ipotizzato che, nel Metaverso, non potesse mai concretizzarsi un'azione in senso stretto e che, dunque, l'inquadramento del fatto dovesse sempre avvenire in termini di mera intenzionalità. Tuttavia, come già sottolineato, c'è una connessione tra la realtà reale e quella virtuale; difatti, per accedervi sono necessari appositi strumenti (visori, caschetti e occhiali), una valuta virtuale e connessioni idonee a supportare l'esperienza immersiva.

Alla luce di queste considerazioni è opportuno interrogarsi, altresì, sulla possibilità concreta che un'azione estrinsecata nel Metaverso, laddove lesiva di un bene giuridicamente protetto attraverso norme penalistiche, possa dar vita a responsabilità.

Da ultimo, è opportuno sottolineare[5] come, in taluni casi, sono stati ritenuti integrati reati, quale la violenza sessuale, pur a fronte dell'assenza di contatto fisico; in merito, si richiama una pronuncia della Corte di Cassazione la quale, condividendo le considerazioni del Tribunale del Riesame, concludeva per l'applicazione dell'art 609-*bis* c.p., atteso che: «La violenza sessuale risultava pienamente integrata, pur in assenza di contatto fisico con la vittima, quando gli atti sessuali coinvolgessero la corporeità sessuale della persona offesa e fossero finalizzati e idonei a compromettere il bene primario della libertà individuale nella prospettiva di soddisfare o eccitare il proprio istinto sessuale»[6]. C'è chi riconosce in questa impostazione una continuità rispetto ai casi di illecito perpetrati nel Metaverso, propendendo a favore di una punibilità di tali condotte. A sfavore di tale impostazione milita chi[7], al contrario, ritiene che le ipotesi in esame ricadrebbero nell'ambito dell'art. 49 c.p., cioè che si tratterebbe di reati impossibili[8].

Venendo alla possibilità di sovrapposizione della figura dell'avatar a quella del soggetto persona fisica, è da rilevare come, nel Metaverso, non operi concretamente e direttamente l'individuo, bensì una sua proiezione; la paternità delle azioni, dunque, dovrebbe essere ascrivibile al soggetto che,

---

[5] Si veda, A. CONTINIELLO, *Le nuove frontiere del diritto penale nel Metaverso. Elucubrazioni metagiuridiche o problematica reale?*, in *Giur. Pen.,* 2022, V; V. IMPROTA, *Metaverso e reati nell'ordinamento giuridico italiano*, in *Filodiritto*, 6 giugno 2022. Consultabile al sito: https://www.filodiritto.com/metaverso-e-reati-nellordinamento-giuridico-italiano; C. CRISCI, *Metaverso: brevi riflessioni sui profili di diritto penale*, in *Filodiritto*, 30 novembre 2022. Consultabile al sito: https://www.filodiritto.com/metaverso-brevi-riflessioni-sui-profili-di-diritto-penale.

[6] Cass. Pen., sez. III, sent. 08.09.2020, n. 25266 in *Foro It.,* 2020; si veda anche, L. PICOTTI, *La violenza sessuale via whatsapp, commento a Cass. Pen., Sez. III, 8 settembre 2020, n. 25266*, in *Diritto di Internet*, 2020, IV, 683-685.

[7] D. INGARRICA, *Metaverso criminale. Quali interazioni nel presente nazionale e quali sfide globali del prossimo futuro*, in *Giur. Pen.*, 2022, IX.

[8] G. FIANDACA, E. MUSCO, *Diritto Penale. Parte generale,* 8ª ed., Torino, 2019.

attraverso input informatici, determina l'avatar – rappresentazione di sé stesso – ad agire. La soluzione non pare essere così lineare, in ragione della evidente discrasia tra le due figure, dalla quale discende un verosimile contrasto con il principio di personalità della responsabilità penale. Tuttavia, il Legislatore ha contezza dei rischi derivanti dal mancato riconoscimento di una responsabilità personale per le ipotesi in cui si dovrebbe accettare una *fictio* iuris, come avvenuto per le società e per l'adozione del D. Lgs. 8 giugno 2001, n. 231. In ragione della similarità delle due situazioni, ben potrebbero essere superati i timori in merito al rispetto del principio di personalità della pena rispetto al fatto di reato.

In conclusione, sarebbe opportuno porsi a metà strada tra la rilevanza di condotte *contra legem* poste nel Metaverso e, al contrario, una loro assoluta irrilevanza. Una soluzione di compromesso potrebbe, eventualmente, essere il rafforzamento di una responsabilità di natura civile.

1. Gli attacchi informatici: le minacce del nuovo millennio.

Si definisce, con i limiti attuali del diritto, attacco informatico: «un'operazione informatica, di natura offensiva o difensiva, che sia ragionevolmente prevedibile e che cagioni lesioni o morte a persone o danni o distruzione a oggetti»[9]. Trattasi, dunque, di operazioni condotte attraverso l'impiego di strumenti informatici o telematici, che implicano atti di violenza.

Per valutare se un atto costituisca un attacco informatico, è necessario porre l'attenzione sul rapporto causale tra la condotta ed i danni cagionati, quindi porre l'attenzione sul piano delle conseguenze.

A venire in rilievo non sono esclusivamente le conseguenze dirette sul supporto informatico ma anche quelle indirette, consequenziali e ragionevolmente prevedibili, che insistano su persone o cose che, pertanto, costituiranno l'oggetto dell'attacco.

I cyberattacks, attualmente, rappresentano la modalità di attacco più funzionale nei confronti di uno Stato, grazie ad alcune peculiarità proprie degli strumenti informatici, tra cui l'anonimato, l'a-spazialità e l'a-temporalità[10].

Per questa ragione, è essenziale che gli Stati si dotino di sistemi di prevenzione e, in particolar modo, di rilevazione di tali minacce, con la finalità di individuare prontamente il soggetto a cui attribuire l'attacco.

In questa delicata fase si inserisce il problema dell'attribuzione, intesa quale procedimento volto a risalire al soggetto mittente dell'operazione[11]; a tal fine, risulta dirimente disporre di risorse tecnologiche congrue, sia fisiche che umane, e di potersi avvalere di strumenti di collaborazione internazionale che favoriscano lo scambio di informazioni rilevanti.

Si tratta, ora, di delineare le fasi del processo di attribuzione dell'atto informatico ostile.

---

[9] M. N. SCHMITT (a cura di), *Tallinn Manual 2.0 on the international law applicable to cyber operations,* Cambridge, 2017.

[10] R. RAZZANTE, A. CRISTALLINI, *Cybercrime*, Pisa, 2021, 15. Per ulteriori approfondimenti, si veda L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, Bologna, 2018, I, 69.

[11] T. RID, B. BUCHANAN, *Attributing Cyber Attacks*, in *The Journal of Strategic Studies*, 2015, 5 – 37.

2. Le tre fasi dell'attribuzione. La fase tecnica.

Si può tentare di declinare il processo dell'attribuzione in tre macro-fasi: tecnica, politica-pubblica e giuridica.

La prima fase ha come obiettivo l'individuazione della strumentazione utilizzata per condurre l'attacco, tramite elaboratori in grado di analizzare, quantificare e manipolare dati informatici. All'esito di questo procedimento, si giungerà a circoscrivere la fonte responsabile.

In questo stadio, ci si avvale dei cc.dd. indicatori di compromissione (indicators of compromise, IoC), quali malware, virus, signature, domain name ed indirizzi IP.

Nella maggior parte delle ipotesi, la ricostruzione *sic et simpliciter* delle modalità tecniche della violazione può non condurre a risultati esaustivi, dunque si ricorre ad un'analisi incrociata con le *TTP* (tattiche, tecniche e procedure) che più di frequente trovano impiego nel cyberspazio.

Di recente, si è assistito ad una maggior frequenza nell'impiego di tool standardizzati e non personalizzati, che aggravano ulteriormente la fase di individuazione del soggetto responsabile. Pertanto, entra in gioco un'analisi di natura empirica per il tramite di modelli comportamentali a supporto degli strumenti ordinari.

La fase tecnica, certamente la più delicata, dovrebbe poter contare su risorse che permettano, quanto più possibile, una riduzione dei tempi di rilevamento, per evitare una dispersione di elementi e di dati rilevanti.

3. (Segue) La fase politica.

La fase politica consiste nella raccolta di informazioni attraverso canali interstatali – ufficiali e non – per giungere all'individuazione delle potenziali ragioni (spesso, geopolitiche) sottese all'attacco e al soggetto, ovvero all'organizzazione da cui esso proviene.

Questo secondo step ha una connotazione fortemente pubblica[12]; spesso, difatti, si mira ad individuare il soggetto colpevole, diffondendo la notizia attraverso i mass media, per disincentivare l'eventuale reiterazione degli attacchi[13], con finalità, dunque, eminentemente deterrente.

Da ultimo, la diffusione della notizia, tramite canali di comunicazione ufficiale, costituisce una forte presa di posizione, nel panorama internazionale, nei casi in cui l'attribuzione di un attacco avvenga congiuntamente da parte di più Stati.

[12] Per approfondimenti, F. J. EGLOFF, M. SMEETS, *Publicly attributing cyber-attacks: a framework*, in *Journal of Strategic Studies*, 2021.

[13] A. BENDIEK, M. SCHULZE, *Attribution: A Major Challenge for EU Cyber Sanctions, German institute for International and Security Affairs*, in *SWP Research Paper*, 2021.

4. (Segue) La fase giuridica.

Nell'ultima fase, prettamente giuridica, l'attacco è imputato ad un soggetto, ad un'organizzazione o ad uno Stato.

Nei casi in cui viene individuata come responsabile una persona fisica o un'organizzazione, ne deriverà l'imputazione sulla base della fattispecie penale prevista all'interno del singolo Stato.

Nelle ipotesi in cui l'attacco sia riconducibile ad uno Stato, tuttavia, si rilevano difficoltà nell'attribuzione, derivanti dall'assenza di una normativa internazionale, dovendosi risolvere la questione in via interpretativa.

Da una minaccia informatica, in queste ipotesi, potrebbe derivare una responsabilità internazionale dello Stato a cui essa si attribuisce, come prevista dal Progetto di articoli sulla responsabilità degli Stati del 2001[14].

Affinché si possa ritenere sussistente un illecito internazionale, è necessaria l'integrazione del relativo elemento oggettivo, il cui fondamento risiede nella violazione di un obbligo parimenti internazionale facente capo allo Stato.

A tal fine, potrebbe addursi come referente giuridico l'art. 2, par 4, della Carta delle Nazioni Unite, che dispone: «I Membri devono astenersi, nelle loro relazioni internazionali, dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite».

È possibile inquadrare i casi in esame, dunque, nel concetto di uso della forza, riconducendovi le ipotesi di attacchi cyber, con conseguente applicabilità della legittima difesa di cui all'art 51 della Carta. Ammettendo tale soluzione, si riterrebbe integrato l'elemento oggettivo di un illecito internazionale, consistente nella violazione dell'obbligo giuridico avente ad oggetto il generale dovere di astensione dall'uso della forza[15]. Inoltre, la Rule 11 del Manuale di Tallinn delinea i requisiti affinché un attacco cyber possa essere ascrivibile all'ipotesi di uso della forza, stabilendo che: «A cyber operation consitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force».

Si esige, dunque, che dall'attacco derivino conseguenze analoghe e qualitativamente equivalenti a quelle che si verificherebbero a seguito di un attacco tradizionalmente inteso, focalizzando l'attenzione dalla convenzionale fenomenologia dell'uso della forza al piano dei concreti effetti pregiudizievoli che ne possono derivare, pur a fronte di modalità di azione atipiche e nuove.

Tuttavia, non manca chi milita a favore di un'impostazione più rigorosa e meno soggetta ad una fluidità interpretativa, sulla base di argomentazioni che ruotano attorno alla risalente posizione espressa a suo tempo – nel 1927 – dalla Corte permanente di giustizia internazionale, secondo la quale: «The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement

[14] M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, 35.

[15] A tal proposito, è utile il richiamo alla Rule 10 del Manuale di Tallin, secondo cui: «A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of a State, or that is in any other manner inconsistent with the purposes of the United Nation, is unlawful».

of common aims. Restrictions upon the independence of States cannot therefore be presumed»[16].

Da tale prospettiva, la responsabilità di uno Stato potrebbe sorgere solo a fronte della violazione di un obbligo esplicito, da cui *a contrario* si ricaverebbe la legittimità di ogni condotta non vietata. Tale seconda impostazione, a ben vedere, rispetto alla prima, restringerebbe ulteriormente le ipotesi di attribuzione, azzerandole del tutto, visto che, a livello internazionale, tale obbligo esplicito non sussiste in tema di attacchi informatici.

Pertanto, l'interprete constaterà l'assenza, come anticipato, di una normativa puntuale volta a disciplinare il fenomeno in esame e, salvo ammettere un *vulnus* di tutela a fronte di attacchi che sovente si dirigono verso infrastrutture critiche[17] statali, la prima soluzione interpretativa parrà essere preferibile.

A supporto di tale conclusione, infatti, si ricorda che, all'interno del Progetto di articoli sulla responsabilità degli Stati del 2001, l'art. 14 stabilisce che una violazione si può verificare tramite: «an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character».

Concludendo, dunque, che un attacco informatico costituisca uso della forza, si apre la possibilità di agire in legittima difesa, ai sensi dell'art. 51 della Carta delle Nazioni Unite, che dispone: «Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale».

5. La normativa europea: il Regolamento 2019/796/UE.

Con il Regolamento 2019/796/UE del 17 maggio 2019, concernente Misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, l'Unione europea ha inteso predisporre un sistema volto a limitare l'ingresso ed il transito sul territorio unico europeo, unitamente a misure di congelamento di fondi e di risorse economiche, nei confronti di soggetti «quali identificati dal Consiglio a norma dell'art. 5, par. 1, della Decisione (PESC)

[16] Corte Permanente di Giustizia Internazionale, 07.09.1927, *France vs Turkey, The Case of the S.S. "Lotus"*.

[17] Definizione calzante di infrastruttura critica la si può rintracciare nella Direttiva 114/08/CE del Consiglio dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, che definisce « "Infrastruttura Critica" un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

2019/797: a) persone fisiche o giuridiche, entità o organismi che sono responsabili di attacchi informatici o tentati attacchi informatici; b) persone fisiche o giuridiche, entità o organismi che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, o agevolandoli per azione o omissione; c) persone fisiche o giuridiche, entità o organismi associati alle persone fisiche o giuridiche, alle entità o agli organismi di cui alle lettere a) e b) del presente paragrafo».

In particolare, all'art. 1 vengono individuate le azioni che integrano un cyberattacco, quali l'accesso o l'interferenza a sistemi informatici e l'intercettazione di dati; tali attacchi sono sferrati dall'esterno dell'Unione o impiegano infrastrutture esterne alla stessa. Per quanto riguarda i soggetti agenti, rilevano quali attacchi informatici quelli compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti oppure operanti al di fuori dell'Unione o commessi con il sostegno, sotto la direzione o sotto il controllo di tali soggetti.

Nel successivo par. 4 dell'art. 1, si circoscrivono quali attacchi implicanti una minaccia per l'Unione quelli che insistono sulle infrastrutture critiche essenziali per il mantenimento delle funzioni vitali della società, della salute, dell'incolumità, della sicurezza e del benessere economico o sociale della popolazione. Inoltre, vi si ricomprendono quelli che attaccano i servizi necessari, quali l'energia, i trasporti, il settore sanitario, la distribuzione di acqua potabile.

La rilevanza delle azioni che presentino i requisiti dell'art. 1 sono stabilite sulla base degli effetti che da esse derivano; in particolare, l'art. 2 dispone che, al fine di determinare se l'attacco abbia avuto un effetto significativo, bisogna aver riguardo a: «a) portata, entità, impatto o gravità delle turbative causate, anche per quanto riguarda le attività economiche e sociali, i servizi essenziali, le funzioni statali essenziali, l'ordine pubblico o la sicurezza pubblica; b) numero di persone fisiche o giuridiche, entità o organismi interessati; c) numero di Stati membri interessati; d) importo della perdita economica causata per esempio mediante furti su larga scala di fondi, risorse economiche o proprietà intellettuale; e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi; f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati; o g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso».

Nell'ambito della politica estera e della sicurezza comune dell'Unione europea, possono essere, altresì, impiegati strumenti alternativi, modulabili sulla base dell'intensità dell'attacco. Fermo restando che le sanzioni entrano in gioco a fronte di un evento connotato da un alto grado di gravità, in ipotesi ordinarie si può, anzitutto, ricorrere all'adozione di misure preventive, spesso in accordo con Paesi terzi, grazie ad interlocuzioni politiche che consolidino, ad esempio, una posizione comune o che giungano a misure di cooperazione. È possibile, inoltre, che la presa di posizione avvenga già in seno al Consiglio (in tali casi, tuttavia, si esigerebbero maggioranze qualificate) e, in ipotesi di particolare gravità, come le operazioni militari e di difesa.

6. Il nuovo volto del riciclaggio nell'era digitale: il cyberlaundering.

L'evoluzione tecnologica e le nuove frontiere della comunicazione hanno portato, come anticipato, alla proliferazione di nuove condotte penalmente rilevanti, nonché ad una significativa espansione delle attività illecite[18].

Difatti, la rete è diventata terreno fertile per la realizzazione dei propositi criminosi delle organizzazioni nel più breve tempo possibile. Queste ultime, per sopravvivere ed operare, necessitano di ingenti risorse finanziarie che, tramite il *web*, possono essere facilmente reperite, per poi essere reinvestite: Internet ha consentito la diffusione e la perpetrazione di frodi informatiche, favorendo il reperimento di importanti somme e, di conseguenza, il riciclaggio di denaro "sporco"[19].

Il cyberlaundering rappresenta la trasformazione digitale di un fenomeno già esistente, che ha quale obiettivo primario quello di: «allontanare il denaro dalle relative origini illecite, ostacolando la tracciabilità dell'origine dei proventi. E alcuni delitti, quali estorsioni informatiche, furti di identità, phishing e spamming, vengono, a loro volta, adoperati per concretizzare e agevolare il riciclaggio online»[20].

Il phishing, ad esempio, è l'attività illecita in base alla quale, attraverso vari artifici, - si pensi allo spamming di messaggi o all'utilizzo di malware -, un soggetto riesce ad impossessarsi, fraudolentemente, dei codici elettronici di un dato utente, allo scopo di utilizzarli, successivamente, per frodi informatiche considerevoli, quali, ad esempio, l'accesso ai conti correnti bancari o postali al fine di trarne profitto.

Nello specifico, l'autore del phishing invia un messaggio piuttosto credibile, nel cui testo si rappresentano urgenti ragioni di sicurezza per le quali sarebbe assolutamente necessario che il destinatario clicchi sul link indicato, allo scopo di inserire o modificare le proprie credenziali di accesso ai conti online. Il link, in realtà, rimanda ad una pagina web contraffatta ma identica, almeno graficamente, a quella originale dell'istituto di credito[21].

Ebbene, il phisher si impossesserà dei dati immessi dall'utente raggirato, e li utilizzerà per accedere al conto corrente della vittima, al fine di sottrarne denaro.

Si segnala, altresì, la presenza di un altro soggetto, il financial manager, sul cui conto verranno accreditate le somme di cui il phisher si sia impossessato abusivamente, al fine poi di trasferirle all'estero con operazioni di money transfert.

---

[18] Sul punto si confronti R. RAZZANTE, A. CRISTALLINI, *op. cit.*, 5 ss.

[19] Per approfondire si veda R. RAZZANTE, *Le insidie di blockchain e bitcoin*, in *Formiche*, 2019, 153, 20-22 e R. RAZZANTE, L. CUOMO, *La nuova disciplina dei reati informatici*, Torino, 2009.

[20] In merito, per approfondire, si veda, R. RAZZANTE, *Manuale di legislazione e prassi dell'antiriciclaggio*, 2ª ed., Torino, 2023.

[21] In questo senso, S. BATTAGLIA, *Criminalità informatica al tempo di internet: rapporti tra* phishing *e riciclaggio*, in *Altalex,* 18 settembre 2014. Consultabile al sito: https://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio; E. BASSOLI (a cura di), *I crimini informatici, il dark web e le web room*, Pisa, 2021 e, da ultimo, F. CORONA (a cura di), *Reati informatici e investigazioni digitali*, Pisa, 2021. Alcune interessanti ricerche in tal senso sono state pubblicate sui siti di Mandiant e di Visa; L. PICOTTI, *"Nuovi" crimini cibernetici e possibile rilevanza dell'intelligenza artificiale*, in *Stati Generali del Diritto di Internet*, Atti del Convegno Luiss, Roma, 16, 17, 18.12.2022, I.

La posizione giuridica del financial manager ha sollevato un importante interrogativo: invero, il dibattito dottrinale e giurisprudenziale verte sulla configurabilità o meno, in capo allo stesso, del delitto di riciclaggio.

La giurisprudenza di legittimità[22] ha chiarito che questi risponde a titolo di concorso nei medesimi delitti realizzati dal phisher solo se abbia agito con la consapevolezza del disegno criminoso posto in essere.

Al contrario, il financial manager risponderà di ricettazione o di riciclaggio, a seconda che si sia limitato a ricevere le somme di denaro, consapevole della loro provenienza illecita, ovvero le abbia anche trasferite all'estero con modalità idonee ad ostacolare l'identificazione di tale provenienza[23].

Questo orientamento è stato autorevolmente sancito con la sentenza 1° luglio 2011, n. 25960, ove la Suprema Corte ha richiamato l'orientamento delle Sezioni Unite in tema di compatibilità del dolo eventuale con il delitto di ricettazione[24].

Quanto appena segnalato è soltanto un esempio di utilizzo abusivo delle nuove tecnologie informatiche per la realizzazione di propositi criminosi: l'origine del cyberspace, dimensione sconfinata e multiforme, pertanto difficilmente controllabile, ha comportato uno spostamento online delle attività delle organizzazioni criminali. Nascono, così, nuove forme di ipotesi delittuose, minacce concrete della sicurezza economica e sociale, nazionale ed internazionale.

I criminali che operano sul web sfruttano anche l'anonimato (sostanzialmente) garantito dalle monete virtuali, le quali consentono trasferimenti rapidi e di cui è difficile rintracciare gli autori. Difatti, il Bitcoin viene ampiamente utilizzato, così come le nuove tipologie di virtual assets[25] che si avvalgono della blockchain, proprio per riciclare denaro. La blockchain si presta infatti a soddisfare le principali esigenze dei riciclatori, quindi «globalizzazione, dematerializzazione ed anonimizzazione delle transazioni»[26], e allo stesso tempo garantisce anche l'occultamento del valore del trasferimento. Queste caratteristiche sono corollario della struttura delle transazioni, non supervisionate da un intermediario ma gestite tra utenti (peer to peer)[27].

È stato osservato che più che di anonimato sarebbe corretto parlare di "pseudoanonimato", dal momento che le transazioni sono registrate in un

---

[22] *Cass. Pen., sez. II, sent. 17.06.2011, n. 25960, in Guida al diritto*, 2011, 44, 76.

[23] Si veda, A. SCIRÈ, *In tema di riciclaggio informatico, dolo eventuale e frode informatica mediante 'phishing', nota a Cass. Pen., Sez. II, 17.06.2011 (dep. 01.07.2011), n.* 25960, in *Dir. Pen. Cont.*, 2011 e R. RAZZANTE, *Riciclaggio e reati connessi. Applicazioni giurisprudenziali e di vigilanza,* Milano, 2023.

[24] Cfr. Cass. Pen., SS.UU., sent. 26.11.2009, n. 12433, in *Guida al diritto*, 2010, 20, 80.

[25] Per approfondire, R. RAZZANTE, *Tracciabilità e riciclaggio: binomio indissolubile tra gli artt. 648 bis e ter c.p. e la recente entrata in vigore del delitto di autoriciclaggio, nota a Cass. Pen., Sez. II, 22 ottobre 2014, n. 43881*, in *Arch.Pen.*, 2014; S. BONFANTE, *Quella incerta linea di confine tra il phishing ed il riciclaggio*, in *Il Penalista*, 28 aprile 2017 e, da ultimo, R. RAZZANTE, *Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari*, Santarcangelo di Romagna, 2018. In giurisprudenza, si veda Cass. Pen., sez. II, sent. 09.02.2017, n. 10060, in *Diritto & Giustizia*, 2017.

[26] Così A. LAUDATI, *Cybercrime e cryptovalut*e, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo,* Roma, 2022, 211-230; R. RAZZANTE, A. CRISTALLINI, *op.cit.*, 5 ss.

[27] Per ulteriori approfondimenti sul tema si veda R. RAZZANTE., *Bitcoin tra diritto e legislazione,* in *Notariato*, 2018, IV.

distributed ledger pubblico [28] ; tuttavia, l'esistenza di un registro delle operazioni, sebbene utile per la tracciabilità, non garantisce la rintracciabilità delle persone fisiche o giuridiche celate dietro i wallet[29].

Anche a livello giurisprudenziale [30] è aumentata la sensibilità rispetto ai potenziali impieghi delle valute virtuali per porre in essere reati di riciclaggio e autoriciclaggio.

A tal proposito è stato osservato, infatti, che concettualmente la dimensione "virtuale" dei reati compiuti con criptovalute non incide sulla formazione della fattispecie criminosa: il fatto che le condotte di occultamento di proventi illeciti abbiano luogo nel cyberspace non esclude il reato di autoriciclaggio, così come se il reato presupposto avviene online e il riciclaggio è offline si avrà comunque l'imputazione per riciclaggio.

La Suprema Corte ha esplicitato come anche la moneta virtuale, se impiegata per investire profitti di origine delittuosa in operazioni finanziarie speculative [31], possa essere ricondotta alla fattispecie di autoriciclaggio [32]: «Anche la moneta virtuale (cosiddetto bitcoin) può rientrare tra gli strumenti finanziari e speculativi presi in considerazione dalla norma incriminatrice dell'autoriciclaggio, in quando l'indicazione normativa di cui all'articolo 648 ter.1 del Cp delle attività (economiche, finanziarie, imprenditoriali e speculative) in cui il denaro, profitto del reato presupposto, può essere impiegato o trasferito individua delle macro aree tutte accomunate dalla caratteristica dell'impiego finalizzato al conseguimento di un utile e, in questa prospettiva, le valute virtuali ben possono essere ricondotte nell'ambito della dizione di "attività speculativa" in quanto possono essere utilizzate per scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento. Del resto, il sistema di acquisto di bitcoin si presta ad agevolare condotte illecite, in quanto è possibile garantire un alto grado di anonimato, senza tra l'altro alcun controllo sulla provenienza del denaro convertito» (cfr. Cass. Pen., Sez. II, 13 luglio 2022, n. 27023).

Si può osservare, da ultimo, che la giurisprudenza si è trovata a dover svolgere una funzione definitoria a proposito dell'impiego delle criptovalute, per scopi leciti o illeciti, anche al di fuori dell'ambito del riciclaggio e dell'autoriciclaggio. Si sta verificando un progressivo avvicinamento della moneta virtuale al denaro; tuttavia, ancora ci sono degli aspetti in via di definizione.

---

[28] In tal senso, L. STURZO, *Bitcoin e riciclaggio*, in *Dir. Pen. Cont.*,2018, V, 21 e R. RAZZANTE, *Autoriciclaggio con bitcoin: nuove impostazioni criminali e giurisprudenziali*, in *Il Penalista*, 28 febbraio 2022.

[29] A tal proposito L. LA ROCCA, *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi Giuridica dell'Economia,* 2015, I, 201 -222.

[30] La tematica delle criptovalute è stata affrontata per la prima volta nel 2017 dalla giurisprudenza nazionale, vedi Trib. Verona, sent. 26.01.2017, n. 195, in *Foro It.*, 2017.

[31] Cfr. F. COLAZZO, *Investire i profitti della truffa per acquistare criptovalute integra il reato di autoriciclaggio*, *nota a Cass. Pen., Sez. II, 13 luglio 2022, n. 27023*, in *Antiriciclaggio & Compliance,* 2022.

[32] Si raccomanda G. J. SICIGNANO, *La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*, Pisa, 2021.

7. Il fenomeno del cyberterrorismo.

Il cyberterrorismo, come il terrorismo tradizionale, presenta un notevole problema definitorio. Questa lacuna deriva, a monte, dall'incertezza nell'inquadrare il fenomeno già da un punto di vista fattuale e reale.

Il dibattito in merito alla questione terminologica si amplia se si tiene conto dei pareri degli esperti: alcuni di essi negano azioni di cyberterrorismo, mentre altri ritengono che alcuni gruppi ricorrano sistematicamente alla rete [33]. È indubbio come la stessa società dell'era digitale, impiegando la tecnologia informatica e telematica in settori sempre più ampi, abbia consentito ai gruppi terroristici di poter accedere con maggiore facilità alle informazioni circa le cc.dd. infrastrutture critiche, quali sistemi di difesa nazionali, sistemi di controllo e di trasporto di persone e merci, sistemi di controllo di fonti energetiche, sistemi sanitari e circuiti economico-finanziari. Di fatto, dunque, il livello di progresso tecnologico che una società riesce a raggiungere si affianca, parallelamente e proporzionalmente, ad una maggiore vulnerabilità rispetto ai potenziali rischi cyber.

È così che due dei più rilevanti rischi che gli Stati sono chiamati a prevenire e ad affrontare sono il pericolo cyber ed il terrorismo; quest'ultimo, in particolare, rappresenta un fattore di destabilizzazione degli assetti internazionali, soprattutto sul versante della sicurezza interstatale, anche alla luce delle sue nuove modalità di manifestazione, che si sono adeguate senza fatica alla rivoluzione digitale.

I singoli Stati e, più in generale, l'intera compagine mondiale, si trovano, infatti, a fronteggiare un fenomeno *sui generis*, che presenta caratteri e modalità di manifestazione indeterminati, volatili e ubiquitari, in grado di penetrare le strutture delle moderne società occidentali, anche tramite canali informatici. Per queste ragioni è sentita l'esigenza di approntare strumenti di cooperazione sinergica sia da un punto di vista esterno (tra Stati, federazioni e organizzazioni internazionali), sia interno (tramite la predisposizione di un sistema sanzionatorio nazionale idoneo a contrastare queste minacce).

Proprio grazie allo sviluppo della rete si è affermato il c.d. cyberterrorismo, una particolare declinazione del terrorismo tradizionale, che ha cambiato la natura e le modalità delle minacce alla sicurezza internazionale, rendendole più dinamiche e fluide rispetto al passato. È il caso del terrorismo c.d. globalizzato di matrice islamica, la cui prima manifestazione risale agli attentati dell'11 settembre 2001, destinato a divenire un modello più efficiente e incisivo delle forme ordinarie di criminalità terroristica.

É noto come le organizzazioni terroristiche fondamentaliste, tipo Daesh o Al Quaeda, utilizzino strumenti informatici e di comunicazione per finalità non solo propagandistiche ma anche operative, come ad esempio il controllo o il comando dei cc.dd. 'lupi solitari' e delle cc.dd. 'cellule dormienti'; inoltre, nello

[33] Si vedano sul punto, F. SPIEZIA, S. ORLANDI, *Misure antiterrorismo del Consiglio d'Europa,* in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 479-506, i quali osservano che: «L'uso della rete è il mezzo principale attraverso cui i terroristi perseguono i propri fini. Esso ingloba sia la fattispecie dei reati di cybercrime indirettamente collegati alle finalità di terrorismo (e per questo difficili da etichettare con il termine di cyberterrorismo in senso stretto), sia quelli direttamente finalizzati al terrorismo. Per tale motivo, cybercrime e cyberterrorismo necessitano di pari attenzione, essendo due fenomeni molte volte potenzialmente correlati tra loro».

stesso modo, si trasmettono le guide e le informazioni utili per la radicalizzazione e l'addestramento dei cc.dd. foreign fighters[34].

La rete, dunque, figura in ogni aspetto dell'organizzazione stessa e diviene essenziale per attività quali il reclutamento, il finanziamento e la propaganda.

In questo scenario, può osservarsi come gli attentati dell'11 settembre 2001[35] abbiano dato vita ad un nuovo paradigma di guerra, che si basa su una forma di conflittualità poco prevedibile nelle sue manifestazioni, nelle sue modalità, nei suoi tempi. Tale paradigma riflette la nuova strategia terroristica che, da nazionale a transazionale, è diventata di tipo globalizzato. Questa transizione è stata in larga parte agevolata dall'impiego di strumenti informatici, grazie ai quali le organizzazioni terroristiche hanno potuto raggiungere un'audience mondiale. La rete accresce la forza e la propagazione del terrorismo perché riesce a trasformare un evento geograficamente delimitato in un evento aspaziale e atemporale di risonanza globale.

Da ultimo, la rete consente una diffusione della propaganda ad un bacino di utenti sempre più ampio – soprattutto giovani. È divenuto, infatti, imprescindibile ricorrere a siti Internet, anche all'interno del c.d. dark web, per garantire stabilità a tutte le attività strumentali all'organizzazione stessa, quali l'affiliazione, il finanziamento, la promozione di iniziative criminose, le raccolte di fondi attraverso collegamenti tra le singole organizzazioni.

Per quanto concerne il reclutamento, anch'esso avviene tramite l'impiego di strumenti informatici, in particolare delle piattaforme quali Facebook, Twitter, Instagram, ma anche blog e siti di dating online; successivamente, la fase della radicalizzazione si consuma in un ambiente virtuale privato, terreno fertile per familiarizzare con l'organizzazione. Inoltre, il web consente l'estrazione di dati – c.d. data mining – che permettono di reperire non solo informazioni su infrastrutture critiche, quali trasporti, edifici pubblici, aeroporti e porti, ma anche informazioni sulla predisposizione di armi chimiche ed esplosivi. Per concretizzare una minaccia sarebbero necessari degli attacchi simultanei a differenti obiettivi strategici e una loro protrazione nel tempo; successivamente, si dovrebbe generare un riverbero mediatico tale da destabilizzare l'opinione pubblica e la società tutta.

L'impiego abituale di strumenti tecnologici nello scambio di informazioni[36], nella raccolta dati e nel reclutamento da parte delle organizzazioni criminali è confermato da alcune investigazioni svolte in seguito agli attentati dell'11 settembre 2001. È necessario, però, sottolineare come non sempre queste azioni siano sic et simpliciter di natura terroristica, potendo rientrare anche nell'uso ordinario della rete. A tal proposito, in dottrina si sono delineati due orientamenti definitori del cyberterrorismo; nel primo, target oriented, la rete è intesa come obiettivo e come arma, e ne sono un esempio i casi di danneggiamento, di distruzione o di compromissione di sistemi informatici e di strutture critiche di un Paese; nel secondo, tool oriented, la rete è considerata uno strumento e un supporto, come nelle operazioni di gestione, propaganda,

[34] *Ibidem*, 481 ss.

[35] P. ANGELOSANTO, *Unità antiterrorismo*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 605 ss.

[36] Si rinvia a R. INCUTTI, *Il contrasto al terrorismo attraverso la cooperazione giudiziaria internazionale*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022, 155 ss.

reclutamento e raccolta fondi. A fronte di questa distinzione, è opportuno rilevare come ancora non si verifichino attacchi ascrivibili al primo orientamento; mentre l'impiego del cyberspazio come strumento per perseguire gli scopi delle associazioni terroristiche è ormai un *modus operandi* ineludibile.

Dorothy Denning, nel qualificare il terrorismo informatico, lo definisce come «[…] la convergenza del concetto di cyberspazio e di terrorismo; generalmente è inteso come l'attacco illegale e/o minaccia di attacco contro i computer, le reti, e le informazioni in essi memorizzate, eseguito per intimidire o costringere un governo o la sua gente ad assoggettarsi a obiettivi politici o sociali. Inoltre, per qualificarsi come cyberterrorismo, un attacco dovrebbe essere caratterizzato da violenza contro persone o cose, o essere in grado di causare danni talmente ingenti, tali da generare paura. Sono da considerarsi esempi di attacchi gravi quelli che portano morte o lesioni, nonché esplosioni, incidenti aerei, contaminazione delle acque, o grave perdita economica. Analogamente, possono essere considerati gli attacchi contro le infrastrutture critiche, a seconda del loro impatto»[37].

Occorre, dunque, tracciare un confine tra i casi in cui, come riportato, si verificano attacchi che si risolvono in una lesione di beni giuridici primari della vita o in un danneggiamento di infrastrutture critiche, e i casi, di maggior tenuità, in cui si verificano danni economici meno rilevanti.

In conclusione, la rete svolge un ruolo primario nel mantenimento e nell'operatività delle organizzazioni criminali: dalla commistione tra il terrorismo e gli strumenti informatici nasce un nuovo pericolo, smaterializzato, delocalizzato e, spesso, imprevedibile.

A fronte della natura peculiare del fenomeno *de quo*, è utile analizzare gli strumenti approntati dal legislatore, nazionale e sovranazionale. La mancanza di efficaci misure di natura extra-penale rende possibile il ritorno ad una disciplina penalistica che ricalca la teoria del c.d. diritto penale del nemico[38] per contrastare le organizzazioni terroristiche islamiche.

In un ambito in cui è necessario attuare una tutela preventivo-repressiva, si concretizza il rischio di una risposta legislativa, sostanziale e processuale, non conforme ai principi costituzionali di riserva di legge, offensività e giusto processo, ex artt. 25 co. 2, 111 Cost. e artt. 6 e 7 CEDU, per un duplice ordine di ragioni. La prima si risolve nell'inadeguatezza dei sistemi di difesa informatici statali che, a monte, dovrebbero fungere da protezione[39]. La seconda è legata alla natura ibrida del fenomeno terroristico e cyberterroristico, che rende necessario trovare una sintesi tra discipline giuridiche ed extragiuridiche, come l'informatica.

Lo spazio virtuale, infatti, non presenta un substrato giuridico di riferimento che ne disciplini il funzionamento e i limiti; il legislatore, dunque, dovendosi

---

[37] D. E. DENNING, *Cyberterrorism*, Georgetown, 2000. Consultabile al sito: www.cs.georgetown.edu.

[38] Sul tema, U. NAZZARO, *Il diritto penale del nemico tra delitto di associazione politica e misure di contrasto al terrorismo internazionale*, Napoli, 2016; E. KALICA, *La pena di morte viva: Ergastolo, 41 bis e diritto penale del nemico*, Sesto San Giovanni, 2019; P. BRUNETTI, *Diritto penale del nemico: una lettura critica dei presupposti filosofici*, in *Penaledp*, 29 maggio 2020; R. PUCA, *La teoria del diritto penale del nemico di Günther Jakobs tra funzionalismo luhmanniano e populismo penale*, in D. RONCO, A. SBRACCIA, V. VERDOLINI (a cura di), *La violenza penale: conflitti, abusi e resistenze nello spazio penitenziario*, in *Riv. Antigone,* 2020, II.

[39] Ancora, P. ANGELOSANTO, *op. cit.*, 524.

interfacciare con una dimensione non retta da uno Stato di diritto, opta, talvolta, per un arretramento della soglia di rilevanza penale, mediante la previsione, quali reati consumati, di condotte meramente preparatorie rispetto ad eventuali successivi delitti od effettive lesioni dei beni giuridici protetti, come nei casi di detenzione o in cui l'illiceità dipende soltanto dal fine specifico dell'agente. Questa anticipazione, se ben si concilia con le citate esigenze preventivo-repressive, potrebbe confliggere con il principio di offensività.

Alla luce di queste considerazioni, il bilanciamento tra interessi rilevanti e meritevoli di tutela è lo strumento primario di cui il legislatore si deve servire, per evitare, da un lato, che le finalità repressive eclissino i diritti costituzionali degli individui e, dall'altro, che le esigenze di tutela contro i fenomeni terroristici non trovino realizzazione.

In particolare, ponendo l'attenzione sulla predisposizione delle singole fattispecie incriminatrici, il rischio da paventare è quello che la risposta sanzionatoria sia parametrata non già sul fatto di reato, quanto piuttosto sull'autore e, nella maggior parte dei casi, su alcune manifestazioni di pensiero o di religione.

Sul piano del diritto penale sostanziale ancora non è stata prevista una fattispecie unitaria che tipizzi il terrorismo cibernetico, fenomeno che presenta denominatori comuni alla criminalità informatica e al terrorismo tradizionale. Questa convergenza è evidente negli attacchi informatici a motivazione politica, attuati con la finalità di cagionare gravi e, spesso irreversibili, danni all'istituzioni, all'economia, alla vita e all'integrità fisica.

Si tratta ora di delineare, se pur brevemente, l'*excursus* normativo e gli interventi del Legislatore dell'UE sulla tematica che si sta trattando.

La Convenzione di Budapest sul Cybercrime del 2001 è stata ratificata con la legge 18 marzo 2008, n. 48, e ha introdotto nuove fattispecie, in alcuni casi apportando modifiche alle preesistenti. In particolare, si ricordano l'art. 635-*bis* c.p., recante Danneggiamento di informazioni, dati e programmi informatici, l'art. 635-*ter* c.p., recante Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stati e da altro ente pubblico o comunque di pubblica utilità; l'art. 635-*quater* c.p., recante Danneggiamento di sistemi informatici e telematici e l'art 635-*quinquies* c.p., recante Danneggiamento di sistemi informatici o telematici di pubblica utilità.

In seno all'Unione europea, il fenomeno terroristico viene in considerazione già all'interno del Trattato sul funzionamento dell'Unione Europea, che al suo art. 222 inserisce una clausola di solidarietà, prevedendo che l'Unione e i singoli Stati agiscano congiuntamente laddove «uno Stato membro sia oggetto di un attacco terroristico». Pacificamente, si possono far rientrare nella disposizione i casi in cui l'effetto dell'attacco si sostanzi nell'impiego di strumenti informatici.

Per quanto concerne la ripartizione delle competenze tra legislatore nazionale e sovranazionale, nell'art 83, par. 1, del Trattato di Lisbona del 2009, la criminalità informatica e il terrorismo figurano tra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione europea ha competenza penale.

Con la Direttiva 2013/40/UE del 12 agosto 2013[40], relativa agli attacchi contro i sistemi di informazione, che ha imposto un irrigidimento sanzionatorio ed una cooperazione di polizia e giudiziaria tra gli Stati membri, l'Unione ha posto l'attenzione anche sulla salvaguardia delle cc.dd. infrastrutture critiche, vulnerabile punto di apertura per le organizzazioni criminali.

La successiva Direttiva 2017/541/UE del 15 marzo 2017, sulla lotta conto il terrorismo, ha recepito il concetto di cyberterrorismo come crasi tra lo spazio cibernetico e il terrorismo. L'art 21 della Direttiva, recante Misure per contrastare i contenuti online riconducibili alla pubblica provocazione, imponeva agli Stati di predisporre strumenti per intervenire rapidamente nella rimozione di contenuti online che rappresentano, per l'appunto, una provocazione a commettere reati di terrorismo; tale disposizione è sintomatica della ormai consolidata consapevolezza che le organizzazioni terroristiche si avvalgono di Internet per attività di inneggiamento e di reclutamento.

Nella disposizione in esame si ha riguardo anche delle richiamate esigenze di bilanciamento, prevedendo, al par. 3, che tali misure debbano in ogni caso essere stabilite secondo procedure trasparenti e fornire idonee garanzie, in particolare al fine di assicurare che tali misure siano limitate allo stretto necessario e proporzionate e che gli utenti siano informati del motivo di tali misure.

Nel contesto descritto, deve aggiungersi l'utilizzo delle valute virtuali per scopi illeciti che, progressivamente, ha assunto una dimensione sempre più vasta, come testimonia ad esempio l'operazione condotta dal Dipartimento di Giustizia americano (DoJ) nel 2020. In quella sede, si rilevava come Al-Quaeda e Al-Quassam invitassero, tramite social network - tra cui, apertamente, Facebook – ad effettuare donazioni in Bitcoin per il finanziamento di attività quali l'acquisto di armi; l'esito delle indagini ha visto sequestrati 3 milioni di dollari, 300 account di criptovalute, 4 siti web e 4 pagine Facebook.

Il legislatore interno, per far fronte al fenomeno de quo, ha introdotto, con la Legge 17 aprile 2015, n. 43, l'art. 470-*quinquies* 1, c.p., rubricato Finanziamento di condotte con finalità di terrorismo; la disposizione, rappresentativa della tendenza all'anticipazione della soglia di rilevanza penale per comportamenti apparentemente solo prodromici al compimento di atti terroristici, prevede che «Chiunque, al di fuori dei casi di cui agli articoli 270-bis e 270-quater 1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-*sexies*, è punito con la reclusione da sette a quindici anni, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte».

[40] La Direttiva 2013/40/UE del Parlamento e del Consiglio del 12 agosto 2013 è consultabile su www.eur-lex.europa.eu. Si rinvia, altresì, a F. SPIEZIA, A. CONTINISIO, *Misure antiterrorismo del Consiglio d'Europa*, in R. RAZZANTE (a cura di), *Dizionario dell'antiterrorismo*, Roma, 2022,., 458, a detta dei quali: «Il Consiglio d'Europa apporta un particolare valore aggiunto agli sforzi regionali e globali per prevenire e reprimere il terrorismo attraverso le sue attività di definizione di standard, che mirano a fornire quadri giuridici efficaci, e compatibili con i diritti umani e lo stato di diritto, per la cooperazione tra gli Stati membri, ma anche attraverso le altre attività volte a prevenire la radicalizzazione che porta al terrorismo e, più in generale, a consolidare la democrazia. Il Consiglio d'Europa è determinato a proseguire gli sforzi per promuovere i suoi standard, sia a livello regionale che globale, in stretta cooperazione e coordinamento con gli Stati membri e con altre organizzazioni regionali e globali, comprese le Nazioni Unite».

Nella predisposizione della fattispecie è stata inserita una clausola di apertura rispetto al quomodo della realizzazione del bene o denaro, che consente di farvi rientrare anche le criptovalute, attesa ormai la loro pacifica natura di bene virtuale[41].

Successivamente, il Consiglio d'Europa, su impulso del Comitato per la lotta al Terrorismo (CDCT), ha adottato, sempre nel 2018, una Strategia quinquennale contro il terrorismo; questa si declina in tre punti principali: la prevenzione del fenomeno, il perseguimento dei reati ad esso connessi e la protezione degli Stati membri. In particolare, si auspicava l'adozione sia di misure di law enforcement per rilevare ed impedire attacchi terroristici, sia di un sistema in grado di prevenire fenomeni di radicalizzazione. Inoltre, si individuava, tra gli obiettivi prioritari, quello di approntare un sistema di cooperazione giudiziaria ed internazionale al fine di assicurare non soltanto l'effettività della pena per i responsabili, ma anche la sicurezza degli Stati membri.

Il Legislatore sovranazionale, conscio di come l'attività di addestramento sia ormai agevolata – e quindi, amplificata - dalla rete, nell'undicesimo considerando della Direttiva 2017/541/UE[42], precisava che: «La qualificazione come reato dell'atto di ricevere un addestramento a fini terroristici integra il reato esistente consistente nell'impartire addestramento […] L'atto di ricevere addestramento a fini terroristici comprende l'acquisizione di conoscenze, documentazione o abilità pratiche. L'autoapprendimento, anche attraverso Internet o la consultazione di altro materiale didattico, dovrebbe altresì essere considerata ricevere addestramento a fini terroristici qualora derivi da una condotta attiva e sia effettuato con l'intento di commettere o di contribuire a commettere un reato di terrorismo».

Con la seguente Risoluzione del 13 giugno 2018 sulla cyberdifesa[43], il Parlamento europeo constatava come il cyberspazio sia uno strumento «a basso costo», in grado di flettersi ad ogni esigenza delle reti transnazionali criminali, dando vita ad una minaccia senza precedenti. Occorreva ribadire l'opportunità di predisporre una cooperazione più intensa e strutturata con le forze di Polizia, in una prospettiva di prevenzione rispetto a minacce connesse alla jihad informatica, il terrorismo informatico, la radicalizzazione online e il finanziamento di organizzazioni estremiste o radicali.

Un ulteriore apporto è rappresentato dalla Direttiva 2018/1808/UE del 14 novembre 2018, con la quale si prescriveva agli Stati di approntare un sistema di vigilanza sui contenuti audiovisivi volto ad impedire che siano veicolati contenuti che inneggino alla commissione di reati di terrorismo tramite strumenti di comunicazione di massa. Sebbene non si tratti di un intervento afferente al versante degli strumenti informatici strictu sensu, è comunque sintomatico della consapevolezza da parte dell'Unione della necessità di adottare un approccio onnicomprensivo nei confronti delle minacce terroristiche.

---

[41] In proposito si veda A. LAUDATI, *Cybercrime e criptovalute*, *op. cit.*, 212 ss.

[42] Direttiva 2017/541/UE sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la Decisione 2005/671/GAI del Consiglio.

[43] Si veda, Risoluzione del Parlamento europeo sulla ciberdifesa (2018/2004(INI)). Consultabile al sito: www.eur-lex.europa.eu, 13 giugno 2018.

Inoltre, l'11 dicembre 2018, la Commissione europea ha presentato una proposta di Regolamento, COM/2018/845, in cui si propone di inserire nell'alveo dei contenuti terroristici online una serie di condotte, quali «(a) istigazione, anche mediante l'apologia del terrorismo, alla commissione di reati di terrorismo, generando in tal modo il pericolo che tali reati siano effettivamente commessi; (b) incitamento a contribuire a reati di terrorismo; (c) promozione delle attività di un gruppo terroristico, in particolare incoraggiando la partecipazione o il sostegno a un gruppo terroristico […] (d) istruzioni su metodi o tecniche allo scopo di commettere reati di terrorismo».

La Commissione europea, il 14 aprile 2021, ha presentato la Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025[44], in cui particolare riguardo è riservato ai crimini informatici; a tal proposito, infatti, si sottolinea come: «Oltre l'80 % dei reati ha oggi una componente digitale» e, a seguire, che «Le autorità di contrasto e giudiziarie devono stare al passo con le tecnologie in rapido sviluppo utilizzate dai criminali e con le loro attività transfrontaliere. Ciò richiede un coordinamento nello sviluppo di strumenti e formazioni tra gli Stati membri». Ciò che emerge è l'ambizione di rafforzare la cooperazione comunitaria, varando anche un Codice unico europeo nell'ambito della lotta al riciclaggio al fine di espungere dal circuito economico gli utili generati alla criminalità organizzata e prevenirne l'infiltrazione nell'economia digitale e nella società.

La Commissione si mostra sensibile rispetto alla problematica del finanziamento delle associazioni criminali attraverso le moderne valute virtuali. Infatti, il punto di convergenza tra la dimensione terroristica e quella del cyberspazio è, oggi, emblematicamente rappresentato dalle criptovalute. Questo strumento vanta, tra i suoi punti di forza, l'anonimato e l'immediatezza nell'effettuare transazioni, peculiarità che ne rendono l'impiego particolarmente appetibile nelle attività di finanziamento delle organizzazioni criminali.

Due settimane dopo la presentazione della strategia della Commissione, il 29 aprile 2021 è stato approvato il Regolamento 2021/784/UE, recante disposizioni di Contrasto della diffusione di contenuti terroristici online. In particolare, in capo ai prestatori di servizi di hosting sono prescritti, all'art. 6, degli obblighi volti a prevenire la diffusione di contenuti terroristici all'interno delle relative piattaforme; eventuali contenuti illeciti dovranno essere conservati presso gli stessi per sei mesi dalla rimozione o dalla disabilitazione, per consentirne il vaglio da parte delle Autorità competenti. Laddove i prestatori non dovessero procedere alla rimozione, l'art. 3 riconosce alle autorità competenti del singolo Stato il potere di emettere un ordine di rimozione del contenuto, che dovrà essere adempiuto prontamente, entro un'ora dal suo ricevimento[45].

Sempre in ottica sovranazionale, è doveroso porre l'attenzione sull'attualità della problematica del cyberterrorismo, alla luce del conflitto tra Russia e Ucraina che si sta consumando in Occidente. In particolare, già il 13 gennaio

[44] Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025. Consultabile al sito: www.eur-lex.europa.eu

[45] Si veda sul tema, F. SPIEZIA, S. ORLANDI, *Misure antiterrorismo dell'Unione Europea*, *op.cit.*, 493 ss.

2022 era stato rilevato un malware – WhisperGate[46] – che aveva coinvolto alcune istituzioni governative ucraine. Successivamente, alcuni ricercatori di sicurezza rilevavano un'operazione di attacco da parte del collettivo russo Gamaredon – anche noto come Armageddon o Shuckworm[47]. Dall'inizio della guerra, il 20 febbraio 2022 l'attività di hackeraggio da parte della Federazione russa nei confronti delle infrastrutture rilevanti dell'Ucraina pare non essersi mai arrestata, ed anzi secondo il Servizio delle Comunicazioni Speciali e della Protezione dell'Informazione dello Stato Ucraino (SSSCIP), gli attacchi rilevati si aggirano intorno ai 1123, a danno dei siti governativi, del Ministero delle Infrastrutture, degli Esteri, degli Affari e dell'Educazione e della Banca Nazionale ucraina. La cyber-war si consuma attraverso attacchi DDoS, campagne di disinformazione e attività distruttive di sabotaggio con malware. L'Ucraina, tramite l'Ukraine Cyber Troops, una divisione del Ministero della Difesa, ha portato a compimento numerose operazioni informatiche offensive contro gli obiettivi governativi russi[48].

L'ACN – Agenzia per la Cybersicurezza Nazionale italiana – si è attivata tramite lo CSIRT che, già nel 24 febbraio 2022, aveva segnalato un significativo rischio cyber derivante da possibili impatti collaterali a carico di infrastrutture ITC interconnesse con il cyberspazio ucraino. Altri paesi, quali Lituania, Croazia, Polonia, Estoni, Romania e Paesi Bassi, hanno attivato un Cyber Rapid Response Team, in risposta alla richiesta di sostegno ucraina.

8. (Segue) La cybersicurezza in Italia: sviluppi del 2022.

Da ultimo, è utile segnalare le ultime novità del 2022 in tema di sicurezza cibernetica in Italia, compresa tra i progetti finanziati dal Piano nazionale di ripresa e resilienza (PNRR), in attuazione del quale è stato adottato il decreto - legge n. 82 del 2021, che ha definito la governance del sistema nazionale di sicurezza cibernetica.

Il sistema ha, al suo vertice, il Presidente del Consiglio dei ministri cui è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza e a cui spetta l'adozione della relativa strategia nazionale e la nomina dei vertici della nuova Agenzia per la cybersicurezza nazionale. Il Presidente del Consiglio dei ministri può delegare alla Autorità delegata per il sistema di informazione per la sicurezza della Repubblica le funzioni che non sono a lui attribuite in via esclusiva. Presso la Presidenza del Consiglio dei ministri, è istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. L'Agenzia per la cybersicurezza nazionale (ACN) è istituita a tutela degli interessi nazionali nel campo della cybersicurezza.

---

[46] P. TAVARES, *WhisperGate: A destructive malware to destroy Ukraine computer systems*, in *Infosec*, 25 maggio 2022. Consultabile al sito: www.resources.infosecinstitute.com.

[47] *Shuckworm: Russia-Linked Group Maintains Ukraine Focus*, in *Symantec*, 15 agosto 2022. Consultabile al sito: www.symantec-enterprise-blogs.security.com.

[48] Si rinvia a *Russia's war on Ukraine: Timeline of cyber-attacks*, in *ThinkTank European Parliament*, 21 giugno 2022. Consultabile al sito: www.europarl.europa.eu.

Su questa specifica materia è intervenuto il decreto - legge 9 agosto 2022, n. 115 (c.d. DL Aiuti-bis), recante Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali (c.d. Aiuti-*bis*), in particolare per il tramite dell'art. 37 e dell'art. 37-*quater.*

L'art. 37 prevede che il Presidente del Consiglio dei ministri possa autorizzare l'adozione di misure di intelligence di contrasto in ambito cibernetico, in caso di crisi o emergenza, anche con la cooperazione del Ministero della difesa.

L'autorizzazione è basata sulla valutazione che escluda, alla luce delle più aggiornate cognizioni informatiche e fatti salvi i fattori imprevisti e imprevedibili, che possa essere messa in pericolo o lesa la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone.

Nell'adottare le misure di intelligence, si prevede: la cooperazione del Ministero della difesa; il ricorso alle garanzie funzionali, di cui all'art. 17 della Legge 124/2007 (si tratta di una speciale causa di giustificazione che prevede la non punibilità del personale dei servizi che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizi, nel rispetto di limiti tassativi previsti dal medesimo articolo).

Le misure sono attuate dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI), con il coordinamento del Dipartimento delle informazioni per la sicurezza (DIS), ossia gli organismi operativi dei servizi di intelligence.

Il Presidente del Consiglio dei ministri informa il Comitato parlamentare per la sicurezza della Repubblica (Copasir) delle misure adottate con le modalità di cui all'art. 33, comma 4, della Legge 124/2007. Il richiamato art. 33 stabilisce che il Presidente del Consiglio dei ministri informa il Copasir circa le operazioni condotte dai servizi di informazione per la sicurezza nelle quali siano state poste in essere condotte normalmente previste dalla legge come reato, ma autorizzate da disposizioni di legge, quali l'art. 18 della Legge 124/2007 e l'art. 4 del D. L. n. 144/2005. In particolare, si prevede che le informazioni devono essere inviate al Copasir entro 30 giorni dalla data di conclusione delle operazioni.

A sua volta il Copasir, dopo ventiquattro mesi, trasmette alle Camere una relazione sull'efficacia delle suddette disposizioni.

Restano ferme le competenze del Ministero della difesa ai sensi dell'art. 88 del Codice dell'ordinamento militare e del Ministero dell'interno di cui all'art. 7-*bis* del decreto-legge n. 144/2005, recante Misure urgenti per il contrasto del terrorismo internazionale.

A ben vedere, si tratta di una nuova arma contro gli hacker e questa innovazione non può che considerarsi positiva e rivolta al futuro: i sistemi di difesa devono azionarsi per preservare e proteggere anche lo spazio virtuale, e non solo quello fisico, aereo e terrestre, come già suggerito da tempo, e sotto il coordinamento dell'intelligence e della difesa.

Degno di nota è anche l'art. 37-*quater* del c.d. DL Aiuti-*bis*, posto che estende gli obblighi di notifica attualmente previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale

cibernetica (beni ICT), anche agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), ma che sono di pertinenza di soggetti inclusi nel Perimetro *de quo*. Viene fatta salva la disciplina vigente per gli incidenti a reti del Ministero della difesa.

A ben vedere, l'art. 37-*quater* interviene in particolare sull'articolo 1 del decreto legge n. 105 del 2019 (c.d. decreto Perimetro), inserendo un nuovo comma 3-*bis* che, nel dettaglio, prevede che i soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica (P.A., enti e operatori pubblici e privati che svolgono funzioni istituzionali o essenziali per gli interessi dello Stato, individuati con apposito atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC) notifichino anche gli incidenti, che hanno un impatto su reti, sistemi informativi e servizi informatici di propria pertinenza, pur non riguardando direttamente beni ICT.

Le novità sono di particolare importanza e si inseriscono nel solco già tracciato dal decreto-legge 17 maggio 2022, n. 50 (c.d. DL Aiuti), che aveva recentemente modificato l'art. 88 del Codice dell'ordinamento militare, al fine di inserire tra gli ambiti tutelati dalla difesa nazionale, quale funzione propria e principale dello strumento militare, oltre ai domini tradizionali (terrestre, marittimo ed aereo), anche i domini cibernetico e aero-spaziale. Come precisato dal Governo, la disposizione relativa alla difesa dello spazio cibernetico opera nel pieno rispetto delle competenze di tutte le altre amministrazioni coinvolte nello specifico settore: cyber resilience, in capo all'Agenzia per la Cybersicurezza Nazionale, cyber intelligence, di competenza del Dipartimento Informazioni per la Sicurezza e le collegate Agenzie, cyber crime & investigation, attestata al Ministero degli Interni. Allo stesso modo, afferendo esclusivamente ai profili di tutela militare delle infrastrutture spaziali (antenne, satelliti, strutture per la comunicazione satellitare, ecc.) strettamente connessi alla funzione di difesa nazionale, anche l'inclusione del dominio aero-spaziale non implica contrasti o sovrapposizioni di competenze, ma solo l'adeguamento dell'ambito di interesse della difesa nazionale.

9. Direttiva NIS (Network and Information Security).

La Direttiva NIS (Network and Information Security) è stata recepita dallo Stato italiano con il D. Lgs. 18 maggio 2018, n. 65, perseguendo l'obiettivo di proteggere le reti e i sistemi informatici sul territorio. L'esigenza di introdurre una Direttiva espressamente dedicata all'istituzione di un sistema uniforme sul piano europeo si è consolidata a seguito dell'aumento dell'incidenza degli attacchi cibernetici, in grado di paralizzare sistemi profondamente connessi, come le banche dati digitali o i dati raccolti su cloud.

Con la Direttiva NIS è stata messa in piedi una struttura preventiva e riparativa, per potenziare il livello globale di cybersicurezza nei Paesi membri, ampliando le tutele degli operatori dei servizi essenziali tramite strumenti normativi di garanzia e di prevenzione delle minacce cyber.

Invero, la NIS ha il merito di aver dotato gli Stati membri di una cornice legislativa, lasciando a ciascun Paese l'onere di specificare come gestire

l'attuazione degli obblighi previsti in sede UE[49]. In Italia è emersa, in occasione dell'attuazione della Direttiva, la necessità di prestare attenzione soprattutto alle risorse digitali della Pubblica Amministrazione, ai target di attacchi informatici così come agli enti e agli operatori nazionali pubblici e privati che forniscono servizi imprescindibili per il funzionamento della macchina statale.

Inoltre, è necessario ricordare che, a livello nazionale, gli interventi recenti in materia di cybersicurezza, sulla scia delle indicazioni del legislatore comunitario, sono stati in realtà molteplici; si pensi al decreto - legge 14 giugno 2021, n. 82, con cui è stata determinata l'architettura nazionale di cybersicurezza [50] ed è stata completata l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN)[51]. Ancora, è stata valorizzata l'importanza di misure di cybersicurezza nel Piano nazionale di ripresa e resilienza (PNRR)[52].

10. (Segue) Direttiva NIS 2: i cambiamenti.

A rendere ancora più efficace la protezione di questi settori chiave hanno contribuito ulteriori disposizioni della Direttiva NIS2, approvata [53] dal Parlamento Europeo e, in via definitiva, dal Consiglio il 27 dicembre 2022, e, da ultimo, entrata in vigore il 17 gennaio 2023. Attraverso tale Direttiva si prevede una collaborazione potenziata tra Stati dell'Unione europea, al fine di prevenire e neutralizzare gli attacchi cyber.

La Direttiva NIS 2[54] si è resa indispensabile per fornire alle imprese strumenti in grado di fronteggiare le sfide di un futuro interconnesso e tecnologicamente complesso. Pertanto, da un lato, attraverso il coordinamento delle azioni messe in campo con l'istituzione di organismi di governo del meccanismo di protezione, di raccolta di segnalazioni di incidenti e di indirizzo della reazione; dall'altro lato, incentivando un'adesione delle aziende su base volontaria, rendendole così consapevoli del rischio cibernetico

Si prevede, quindi, anche il supporto fornito dalla rete CyCLONe (Cyber Crisis Liaison Organisation Network), nata nel 2020 per attuare una risposta

[49] A partire dal 2018 la Direttiva NIS (Network and Information System Security) ha rappresentato una pietra miliare per la costruzione di un sistema comune di difesa digitale. Si veda, E. PEZZUTO, *NIS2: l'evoluzione del quadro normativo UE per un livello comune di cybersicurezza*, in *Intelligence e Sicurezza*, 2022, IV.

[50] Il provvedimento prevede l'istituzione del Comitato interministeriale per la cybersicurezza (CIC) presso la Presidenza del Consiglio dei ministri e del Nucleo per la cybersicurezza presso l'ACN.

[51] L'Agenzia è l'autorità nazionale che si occupa di sicurezza cibernetica, sia in attuazione delle misure introdotte dalla Direttiva NIS che per svolgere le funzioni ispettive e irrogare per le sanzioni previste nel D. Lgs. 18 maggio 2018, n. 65 che ha recepito la normativa comunitaria.

[52] L'ultima versione del PNRR è stata trasmessa dal Governo alla Commissione europea il 30 aprile 2021, e definitivamente approvata il 13 luglio 2021.

[53] A. CANDINI, *Il Parlamento europeo approva la Direttiva NIS2 - Nuove e più stringenti misure per la Cybersecurity nell'Unione,* in *Il Sole 24 Ore*, 28 novembre 2022. Consultabile al sito: https://ntplusdiritto.ilsole24ore.com/art/il-parlamento-europeo-approva-direttiva-nis2-nuove-e-piu-stringenti-misure-la-cybersecurity-unione-AETUJnKC?refresh_ce=1.

[54] E. PEZZUTO, *op. cit.,* 2022; G. MARINO, *Cybersecurity comune nell'UE: ecco le ragioni di una NIS 2*, in *Agenda Digitale*, 24 novembre 2022. Consultabile al sito: https://www.agendadigitale.eu/sicurezza/cybersecurity-comune-nellue-ecco-le-ragioni-di-una-nis2/; F. CERCIELLO, *Direttiva NIS 2: ecco come prepararsi a recepire i nuovi obiettivi di cyber security,* in *Cybersecurity360*, 9 gennaio 2023. Consultabile al sito: https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-ecco-come-prepararsi-a-recepire-i-nuovi-obiettivi-di-cyber-security/.

collettiva a livello europeo in caso di crisi informatiche ed assicurare uno scambio celere di informazioni in caso di necessità.

La Direttiva mira ad introdurre anche meccanismi per favorire la cooperazione tra le autorità competenti di ciascun Paese dell'UE, ampliando l'elenco formulato nella Direttiva NIS dei settori tenuti al rispetto di obblighi di cybersicurezza.

Ad ogni modo, a livello nazionale, nell'ambito della Direttiva NIS sono gli Stati membri a dover incoraggiare e vigilare sull'adozione, da parte dei soggetti pubblici e privati a capo delle infrastrutture critiche, di misure in grado di recuperare la funzionalità in breve tempo in caso di attacchi, e di strumenti di prevenzione e tutela di dette strutture[55].

La prevenzione nelle infrastrutture strategiche è stata ripesa anche nella Direttiva NIS2[56], secondo la quale è imprescindibile il perfezionamento delle tecniche di prevenzione e di esistenza ai fenomeni cyber all'interno dell'UE[57]; si propone, infatti, di integrare e di aggiornare le misure per la cybersicurezza al fine di ostacolare opportunamente le minacce informatiche.

Inoltre, la nuova Direttiva NIS2 rende obbligatoria la segnalazione degli incidenti di rilievo aventi ad oggetto strutture strategiche; le segnalazioni dovranno avere luogo entro 24 ore all'Autorità nazionale competente, dando modo di comprendere la gravità dell'attacco e informando anche gli utenti del servizio.

È previsto, inoltre, un obbligo di attivazione immediata, e un report più approfondito all'Autorità pubblica competente da consegnare entro 72 ore dall'incidente. Sulla base delle segnalazioni ricevute, l'Agenzia UE per la cybersicurezza (ENISA) dovrà realizzare delle raccolte di dati per individuare le maggiori criticità, al fine di poterle risolvere.

Ebbene, gli Stati membri hanno tempo fino all'ottobre 2024 per recepire le disposizioni della Direttiva in esame.

Si introducono più stringenti misure di controllo, vigilanza e sanzioni armoniche per tutta l'Unione Europea, a fronte anche di una semplificazione degli obblighi di comunicazione. Inoltre, la Direttiva in esame necessita di una reinterpretazione delle disposizioni al fine di attuare un'opera di adeguamento ai flussi digitali, a fronte di un aumento di traffico in rete a seguito anche della pandemia.

Attraverso i nuovi provvedimenti si mira, inoltre, ad ampliare i settori di attività, coinvolgendo un variegato numero di organizzazioni. Tale ampliamento contribuisce ad incrementare il livello di sicurezza informatica in tutto lo spazio europeo.

Rilevante è il perfezionamento del situational awareness e delle capacità di risposta attraverso misure che aumentino la collaborazione e la fiducia tra le

---

[55] Così D. MAISTO, *Infrastrutture critiche, l'UE ha il Piano d'azione*, in *Qui finanza*, 2 novembre 2022. Consultabile al sito: https://quifinanza.it/innovazione/infrastrutture-critiche-lue-ha-il-piano-dazione/673923/.

[56] Sul punto F. BORDONE, *Cybersicurezza, l'Ue accelera: norme, obiettivi e prossimi step*, in *Agenda digitale,* luglio 2022. Consultabile al sito: https://www.agendadigitale.eu/sicurezza/cybersicurezza-lue-accelera-norme-obiettivi-e-prossimi-step/.

[57] La NIS2 introduce adempimenti ulteriori per i destinatari una serie di prescrizioni, in particolar modo in tema di sicurezza della catena di approvvigionamento, reazione agli incidenti e certificazione di prodotti per la cybersecurity.

autorità, mediante la condivisione del maggior numero di informazioni e prevedendo regole in caso di crisi estese a livello europeo.

Uno dei più rilevanti aspetti della NIS 2 è l'ampliamento dei settori di mercato ad "elevata criticità" e di quelli cc.dd. "importanti". Vi rientrano pertanto, oltre ai settori compresi nella precedente Direttiva, anche la gestione dei servizi ICT, la Pubblica Amministrazione, le Acque Reflue e l'ambito Spazio.

Critici sono ritenuti anche i gestori di rifiuti, le aree di fabbricazione, di distribuzione e produzione di prodotti chimici, l'area manifatturiera, i corrieri e le organizzazioni di ricerca[58].

In riferimento a quelli che vengono chiamati enti "importanti" viene operata una distinzione da quelli qualificati, invece, come "essenziali"[59]. La differenza risiede nei diversi regimi di vigilanza e di applicazione.

A differenza della precedente Direttiva NIS, viene qui introdotto la Size-cap, cioè la regola del massimale dimensionale, quale parametro per l'identificazione delle entità regolamentate. Ad essere esclusi sono, invece, tutti quegli enti svolgenti attività di difesa e sicurezza nazionale, oltre che le banche centrali, i parlamenti e la magistratura.

Viene istituita, in via formale, la rete europea di organizzazioni di collegamento per le crisi informatiche, come strumento di supporto della gestione connessa degli incidenti di sicurezza informatica. Ciò al fine di raggiungere un elevato livello comune di cybersicurezza.

Da ultimo, occorre considerare che tale nuova Direttiva si è posta necessariamente in coordinamento con altre e specifiche norme di settore, tra tutte DORA e la CER[60].

Conclusions: Attacchi informatici ed attuale panorama sanzionatorio italiano: prospettive de iure condendo.

Alla luce di quanto emerge dal rapporto relativo al primo semestre del 2022 dell'Associazione Italiana per la Sicurezza Informatica[61], gli attacchi informatici rivolti in via diretta ad infrastrutture critiche, operatori di servizi essenziali ed aziende si attestano, nel solo mese di maggio, a quota 1380. Se si ha considerazione, in aggiunta, degli effetti indiretti che ne discendono, quali, tra tutti, il possibile riverbero dei danni economici nella catena di produzione, una quantificazione effettiva risulta impossibile. Da questi rilievi si denota la natura endemica del fenomeno in esame e diviene doveroso procedere ad una disamina del perimetro di tutela che l'ordinamento italiano ha approntato nei confronti degli attacchi cyber, al fine di vagliarne l'adeguatezza e l'esaustività.

---

[58] Sul punto e per un più esaustivo elenco, si veda A. VALENTINI, *Dentro la NIS 2, più obblighi e regole per la cybersecurity europea*, in *Cybersecurity 360*, 20 dicembre 2022. Consultabile al sito: https://www.cybersecurity360.it/outlook/dentro-la-nis-2-piu-obblighi-e-regole-per-la-cybersecurity-europea/.

[59] Quelle aziende che, secondo la definizione dell'Anssi, «forniscono un servizio essenziale la cui interruzione avrebbe un impatto significativo sull'andamento dell'economia o della società».

[60] D. DELL'ARIA, M. ROSSI, *Direttive NIS 2 e CER: così l'Europa metterà in sicurezza le sue infrastrutture critiche*, in *Cybersecurity 360*, 20 gennaio 2023. Consultabile al sito: https://www.cybersecurity360.it/cybersecurity-nazionale/direttive-nis-2-e-cer-cosi-leuropa-mettera-in-sicurezza-le-sue-infrastrutture-critiche/.

[61] *Rapporto Clusit sulla sicurezza ICT in Italia 2022.* Consultabile al sito: www.clusit.it.

Anzitutto, con la Legge 23 novembre 1993, n. 547, il Legislatore ha introdotto tre fattispecie – gli artt. 615-*ter,* 615-*quater* e 615-*quinquies* – a presidio dell'inviolabilità del domicilio, ivi inteso quello informatico; in particolare, in merito al reato di accesso abusivo a sistema informatico di cui all'art. 615-*ter* c.p.[62], la Corte di Cassazione, in un orientamento ormai risalente del 1999, ha affermato che esso non mira a tutelare esclusivamente i dati personalissimi contenuti nei sistemi informatici, anzi «si concreta nello *ius excludendi alios* […] e la tutela della legge si estende anche i profili economico-patrimoniali dei dati»[63]. Occorre puntualizzare che, benché quella del 1999 non sia una pronuncia delle Sezioni Unite, tale orientamento è rimasto costante ed inalterato, atteso che le successive pronunce appaiono conformi.

I successivi artt. 615-*quater* e 615-*quinquies* c.p. [64] , con l'obiettivo di perseguire il *possesso* di strumenti quali apparecchiature, codici ed altri mezzi idonei a consentire l'accesso, la distruzione o l'interruzione di sistemi informatici, svolgono una funzione incriminatrice imprescindibile[65]; difatti, uno dei canali privilegiati per la realizzazione di attacchi è rappresentato dal malware – un software deleterio, inserito in un computer al fine di danneggiarne un secondo collegato alla stessa rete – e si stima che ad esso si ricorra nel 38% dei casi[66]. In prima battuta troverà certamente applicazione l'art. 615-*quinquies* c.p.*,* che opera a prescindere dalla verificazione di un danno; laddove questo dovesse concretizzarsi, entreranno in gioco gli artt. 635-*bis* ss. c.p.

Successivamente, all'art. 617-*bis* c.p., è disposta la punibilità dell'installazione di apparecchiature atte a captare o ad impedire comunicazioni telefoniche o telegrafiche altrui. Nel panorama del cybercrime, anche queste condotte trovano frequente impiego, spesso in funzione prodromica e strumentale rispetto ad un disegno criminoso più ampio. È il caso della tecnica BEG (Business E-mail Compromised), attraverso la quale si realizzano frodi a danno delle aziende: dapprima si accede abusivamente ad una casella di posta elettronica, successivamente si carpiscono informazioni in merito alle richieste di pagamento, sino a dirottare transazioni o comunicare nuove coordinate bancarie.

Tra delitti contro il patrimonio si annoverano le fattispecie di cui agli artt. 635 *bis* [67] e seguenti, i quali presentano quale denominatore comune la

---

[62] M. BORGOBELLO, *Il reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. alla luce della giurisprudenza più recente*, in *Giur. Pen. Web*, 2021, II. Consultabile al sito: https://www.giurisprudenzapenale.com/2021/02/21/il-reato-di-accesso-abusivo-a-sistema-informatico-di-cui-allart-615-ter-c-p-alla-luce-della-giurisprudenza-piu-recente/ e, da ultimo, V. IORIO, *I reati informatici ex d.lgs. 231/2001,* in F. CORONA (a cura di), *Reati informatici e investigazioni digitali*, *op.cit*, 187-236.

[63] Cass. Pen., sez. VI, sent. 04.10.1999, n. 3067, in *CED Cassazione Penale*, 2000.

[64] Rubricati rispettivamente Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici e Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

[65] Per approfondimenti, C. PARODI, *Reati patrimoniali*, in C. PARODI, V. SELLAROLI, *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, 103-178.

[66] *Rapporto Clusit sulla sicurezza ICT in Italia*, 2022. Consultabile al sito: https://www.saccani.net/wp-content/uploads/2022/03/Rapporto-Clusit-marzo-2022_b_web.pdf.

[67] Introdotto con la Legge 23 novembre 1993, n. 547, successivamente modificato ad opera della Legge 14 marzo 2008, n. 48.

condotta di danneggiamento [68], che si sostanzia nella distruzione, deterioramento, cancellazione, alterazione e soppressione di informazioni, dati o programmi informatici. Queste disposizioni operano, ad esempio, in ipotesi particolari di attacchi attuati nell'ambito della c.d. information warfare[69], per il tramite delle CNOs (Computer Network Operations), con cui si procede alla distruzione delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi a presidio della difesa nazionale.

È opportuno, altresì, attenzionare le fattispecie in cui il danneggiamento abbia come oggetto materiale sistemi informatici o telematici di pubblica utilità – quale l'art 635-*quinquies* c.p. – oppure informazioni, dati e programmi utilizzati da Stato, enti pubblici o comunque di pubblica utilità, *ex* art. 635-*ter* c.p.

Ai fini dell'integrazione del requisito di "pubblica utilità" non si esige una formale titolarità da parte dello Stato o dell'ente pubblico, essendo sufficiente che i dati, programmi e sistemi siano soltanto impiegati o, eventualmente, nella semplice disponibilità di questi.

Le disposizioni in esame dimostrano la presa di coscienza da parte del Legislatore della particolare appetibilità, da parte dei criminali informatici, delle infrastrutture statali.

Dal 19 maggio 2022, l'Italia – unitamente ad altri Paesi con posizioni di sostegno all'Ucraina – ha subito numerosi attacchi (e tentativi), perpetrati da gruppi di dichiarata appartenenza russa, diretti verso le infrastrutture critiche di numerosi Paesi occidentali. In Italia, tali attacchi si sono tradotti, tra l'altro, nella minaccia di danneggiamenti significativi a pubbliche amministrazioni, ivi compresi i sistemi informatici del Governo, del Ministero dell'Interno e della Difesa.

Dall'analisi della normativa penale italiana in tema di attacchi informatici, può dedursi che le problematiche circa l'attribuzione dei reati non attengano al piano legislativo, bensì interpretativo.

Benché sarebbe utile un riordino della normativa attualmente in vigore, non si ritiene di dover sostenere uno stravolgimento delle fattispecie previste nel Codice penale. Resta, tuttavia, il problema dell'attribuzione, non ancora risolto a livello europeo o nazionale. In questo senso, come anticipato, si tratta di spostarsi sul piano interpretativo, poiché è rimessa al Giudice l'attribuzione concreta del reato all'autore.

È imprescindibile una considerazione in merito al legame di interdipendenza che intercorre tra il diritto alla prova e l'effettività della tutela penale. Nell'ambito dei reati informatici, infatti, pur disponendo di un corpus sanzionatorio esaustivo, questo dovrà necessariamente essere sorretto dall'impiego di conoscenze tecniche specializzate. Pertanto, occorre ampliare il

[68] Come affermato dalla Corte di Cassazione, il danneggiamento risulta integrato anche laddove l'operazione sia reversibile «È ravvisabile il reato di cui all'art. 635-*bis* c.p., in caso di cancellazione di file da un sistema informatico sia quando la cancellazione sia stata provvisoria, mediante lo spostamento dei files nel cestino, sia quando la cancellazione sia stata definitiva», cfr. Cass. Pen., sez. V, sent. 18.11.2011, n.8555, in *Guida al diritto*, 2012, 13, 76.

[69] Per approfondimenti, U. Gori, L. S. Germani, *Information Warfare. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, Milano, 2011; M. Iaselli, G. B. Caria, *Cybesecurity & Cyberwarfare*, Roma, 2023.

ruolo rivestito dai consulenti tecnici. Non sarebbe inopportuno, allora, ipotizzare la presenza di un consulente stabile presso le aule giudiziarie, che coadiuvi le parti ed il giudice.

In questo senso, potrebbe pensarsi anche ad un albo professionale apposito: ancora una volta la realtà ed il mondo propongono sfide che il diritto deve riuscire ad accogliere ed affrontare.