

GIUSEPPE CORASANITI

STRATEGIE DI CONTRASTO AL RANSOMWARE E NUOVE FRONTIERE DELLA CRIMINALITÀ INFORMATICA

SOMMARIO: 1. Ransomware e dintorni: alla ricerca di una comprensione e di una strategia comune. — 2. Le peculiarità dell'associazione a delinquere cyber nella giurisprudenza italiana. — 3. Le strategie possibili e le problematiche effettive. — 4. Politiche drastiche come per i sequestri di persona? — 5. Le problematiche evidenziate in tema di riciclaggio informatico mediante criptovalute. — 6. L'esigenza di un approccio più integrato ed efficace alle condotte estorsive e fraudolente cyber.

I. RANSOMWARE E DINTORNI: ALLA RICERCA DI UNA COMPrensIONE E DI UNA STRATEGIA COMUNE.

Si è registrato in questi anni un aumento significativo del *cybercrime*, con le criptovalute che rappresentano un elemento ormai costante e chiave in queste attività. Nel primo semestre del 2024, il cybercrime ha rappresentato l'88% degli attacchi a livello globale e il 71% in Italia, segnalando un incremento rispetto al 2023. E tali dati vanno letti insieme al radicale aumento delle truffe *online*, in particolare il falso trading online, che sono altrettanto in crescita. Il falso trading online ha causato perdite per quasi 80 milioni di euro, con un aumento del 68% rispetto allo stesso periodo del 2023. Gli attacchi cyber sono aumentati del 23% a livello mondiale rispetto al semestre precedente, con una media di 9 attacchi importanti al giorno. In Italia, il 7,6% degli incidenti globali si è verificato nel primo semestre del 2024, con un totale di 124 incidenti noti di particolare gravità che hanno coinvolto vittime italiane (*Fonti Clusit*)¹. Gli attacchi *ransomware* possono colpire indiscriminatamente privati, aziende e

¹ Il settore manifatturiero è il più colpito in Italia, mentre a livello globale il settore sanitario è il più bersagliato. In Italia, il settore sanitario ha visto un aumento degli attacchi dell'83% rispetto al primo semestre del 2023. Il malware è la principale tecnica di violazione, causando il

51% degli incidenti in Italia. Crescono anche gli incidenti basati sull'*identity theft*. Nel primo semestre del 2024, lo *smishing* è il metodo più utilizzato per il furto di identità digitale. La Polizia Postale ha registrato 9.690 casi di truffe online nel primo

soggetti pubblici causando la perdita di dati sensibili o informazioni critiche.

Negli ultimi anni, l'Italia ha registrato un considerevole aumento degli attacchi *ransomware*, con gravi ripercussioni su aziende e istituzioni. Questi attacchi comportano l'infiltrazione nei sistemi informatici, la crittografia dei dati e la richiesta di un riscatto per ripristinare l'accesso. Secondo dati comparati del 2024, l'Italia si collocherebbe ai primi posti tra i paesi più colpiti da attacchi ransomware, con un incremento del 38% rispetto al semestre precedente. I settori più bersagliati includono l'industria, la consulenza e i servizi ².

Le strategie in genere utilizzate per diffondere l'infezione compromettono a vario titolo le funzioni in relazione ad obiettivi specifici sul sistema, tutti peraltro caratterizzati da una "risposta" dell'utente in termini adesivi alla proposta di pagamento estorsivo. Essi avvengono in tre fasi principali la prima è quella della Infezione del dispositivo, perché ogni ransomware si introduce nel computer tramite allegati o link dannosi contenuti nelle e-mail di phishing, siti web infetti, annunci fittizi ma anche con interventi malevoli su *browser* o *download drive*, cioè configurando appositamente sistemi che si ricollegano alle stesse applicazioni di fondo in modo automatico mediante possibili vulnerabilità. Una volta infettato il computer, il *ransomware* non fa altro che "bloccare" il computer compromesso cioè cripta i dati, rendendoli inaccessibili. In pratica il malware utilizzato contatta il server dell'hacker e genera una coppia di chiavi: una pubblica per crittografare i file e una privata per decrittografarli.

A questo punto scatta la vera e propria richiesta di riscatto, spesso con un link diretto ad un servizio di messagistica. Dopo il blocco crittografico cioè o contestualmente viene immediatamente visualizzata una richiesta personalizzata con l'importo da pagare e le modalità di pagamento, sempre attraverso un link diretto per accredito in criptovaluta, in modo da ostacolare il tracciamento dell'operazione poi sottoposta ad ulteriori triangolazioni in criprovalute internazionali. Esistono vari generi di ransomware noti, tra cui il *cryptomalware*, che cripta i file e richiede un riscatto per decriptarli, il *locker*, che blocca letteralmente l'accesso al sistema operativo, impedendo così l'uso del computer o di un intero server, lo *scareware* cioè software contraffatto che una volta installato richiede il pagamento per risolvere problemi inesistenti (ad esempio antivirus), il *doxware* che poi consiste nella minaccia di pubblicare online le informazioni riservate sottratte. Si diffondono sistemi di *ransomware as a Service* (RaaS) cioè

semestre del 2024, con un ammontare totale di 98.555.935 euro sottratti.

² Non esistono ancora dati statistici

precisi a livello globale ma molti elementi possono essere tratti da <https://www.ransomware.live/stats>.

Malware gestito su commissione da un hacker che si occupa capillarmente della distribuzione e della riscossione dei pagamenti e molte tecniche altrettanto invasive, talora gestite da strumenti di intelligenza artificiale che operano sia una selezione delle potenziali vittime che nella gestione dei rapporti in modo virtuale per adattare le richieste estorsive in modo automatico.

La crescente frequenza e sofisticazione degli attacchi evidenzia infatti anche l'importanza di adottare efficaci misure proattive per proteggere i sistemi informatici e i dati sensibili. La documentazione in *chat* spesso acquisita nel corso di investigazioni indirettamente conferma sempre di più l'esistenza di modelli "*as-a-service*", un quadro cioè nel quale la criminalità informatica svolge e programma attività illecite per conto terzi, oppure in cui anche i criminali meno esperti possono lanciare attacchi utilizzando strumenti e infrastrutture fornite da altri. Questo modello rende così tale tecnica pienamente fruibile ed accessibile a una vasta gamma di associazioni a delinquere che tuttavia sembrano solitamente ricalcare l'assetto di una gang di strada nelle logiche e nella documentazione circa le loro azioni criminose ³.

Le informazioni disponibili a livello internazionale documentano come vi sia una costante evoluzione delle tattiche dei cybercriminali, con l'uso sempre più frequente di tecniche di social engineering, phishing e altre forme di attacco. Si tratta di criminalità organizzata transnazionale, non priva di sviluppi in ambito terroristico ⁴ ma sicuramente radicata anche in Italia che opera in un ecosistema digitale complesso, in continua evoluzione e con una notevole capacità di adattamento, che sarà sempre di più caratterizzato da tecniche di intelligenza artificiale tanto nell'individuazione delle vittime che nella gestione delle negoziazioni con esse. Tali aggressioni sono spesso condotte da gruppi organizzati. Si tratta di un elemento significativo e tale da incentivare una analisi specifica sui collegamenti criminali che richiede una inter-

³ Le chat spesso rivelano i nomi dei gruppi di ransomware coinvolti, come Akira, Avaddon, BlackBasta, Conti, DarkSide, DragonForce, Hive, Hunters International, Lockbit 3.0, Mallox, Mount Locker, NoEscape, Qilin, Ransomhub, Ranzy, Revil e Trinity, mostrando che le operazioni di ransomware sono spesso condotte da gruppi organizzati. Si tratta di un elemento significativo e tale da incentivare una analisi specifica sui collegamenti criminali che richiede una interrelazione continua tra acquisizioni tecnologiche ed esigenze di indagine. Alcuni gruppi, come Hunters International, sembrano essere evoluzioni o derivazioni di gruppi precedenti, indicando una continua adattabilità delle reti cybercrimi-

nali. In sintesi, le chat delle gang di ransomware mostrano un quadro di attività criminale altamente organizzata, in cui le negoziazioni a volte sono fondamentali, le criptovalute sono il mezzo di scambio preferito e le tattiche di estorsione sono raffinate. In sintesi, le chat delle gang di ransomware mostrano un quadro di attività criminale altamente organizzata, in cui le negoziazioni a volte sono fondamentali, le criptovalute sono il mezzo di scambio preferito e le tattiche di estorsione sono sempre più raffinate.

⁴ Cfr. CISTERNA A., *Il contrasto al terrorismo online e la tutela delle infrastrutture informatiche*, in *Diritto penale e processo*, 2023, p. 1431.

relazione continua tra acquisizioni tecnologiche ed esigenze di indagine. Alcuni gruppi, peraltro sembrano essere pure evoluzioni o derivazioni di gruppi precedenti, indicando una continua adattabilità e mutevolezza delle reti cybercriminali. In sintesi, le chat delle gang di ransomware mostrano un quadro di attività criminale altamente organizzata, in cui le negoziazioni a volte sono fondamentali, le criptovalute sono così costantemente il mezzo di scambio preferito e le tattiche di estorsione sono raffinate. In sintesi, le chat delle gang mostrano così un quadro di attività criminale altamente organizzata, in cui le negoziazioni a volte sono fondamentali, le criptovalute sono il mezzo di scambio preferito e le tattiche di estorsione sono sempre più raffinate.

Per un contrasto efficace occorre un approccio pragmatico e soprattutto di coordinamento informativo, una specializzazione costante, una osservazione consapevole e di altissima professionalità e soprattutto una gestione “partecipata” delle informazioni raccolte in termini di analisi e di interlocuzione istituzionale a più livelli. E tutto ciò anche a vantaggio degli utenti e dei consumatori. Si registra, infatti, un aumento dei furti di criptovalute dagli *e-wallet* degli utenti e dalle piattaforme di investimento. La mancanza di regolamentazione uniforme e chiara nel settore delle valute virtuali facilita sempre di più il loro utilizzo per attività illecite. Così proprio la natura efficacemente definita “*proteiforme*” tipica delle criptovalute⁵ sembra ridisegnare e comunque adattare in qualche caso le stesse strategie investigative e le possibili valutazioni processuali, tanto sul piano civile in senso documentale sul piano di potenziali azioni risarcitorie, che più intensamente sul piano penale, sfumandosi così la definizione di regole di condotta generali e internazionali e tentativo costante e giustificato di assimilazione alla valuta tradizionale, nella preminente esigenza di ricostruire efficacemente ogni utilizzazione illecita di criptovalute in ambito penale e civile nel quadro di meccanismi di garanzia e di tutela dei danneggiati. Ed inoltre a tale indubbia natura corrisponde una azione criminale spesso ambivalente, atipica nelle forme e nelle formule organizzative, caratterizzata dall’uso sistematico di tecnologie in evoluzione rispetto alle quali il sistema pubblico di governance e la stessa esperienza giudiziaria fatica ad adattarsi, sviluppando idonee capacità di contrasto e di ricostruzione così come a comprenderne tanto le sue effettive connotazioni e dimensioni quanto gli effetti economici e sociali.

⁵ Così QUATTROCCHI A., *La natura proteiforme delle criptovalute al crocevia della*

tutela penale del mercato finanziario, in *Giurisprudenza italiana*, 2022, p. 1214.

2. LE PECULIARITÀ DELL'ASSOCIAZIONE A DELINQUERE CYBER NELLA GIURISPRUDENZA ITALIANA.

La configurabilità del reato di associazione a delinquere in ambito *cyber* è oggi pienamente ammessa dalla giurisprudenza, sempre che però vi sia documentazione di una pluralità di ruoli, di una ripartizione di proventi, di una connotazione della organizzazione con specifiche caratteristiche o tecniche di ammissione e di cooperazione⁶. Risulta così pienamente configurabile ogni ipotesi di associazione a delinquere finalizzata alla realizzazione di accessi abusivi a sistemi informatici *da parte di un sodalizio criminoso operante esclusivamente in rete, anche quando non risulti individuabile l'esistenza di una vera e propria struttura di vertice del gruppo*⁷. La giurisprudenza in materia ha sottolineato comunque come la esplicita manifestazione di una volontà associativa non è necessaria per la costituzione del sodalizio, potendo la consapevolezza dell'associato essere provata attraverso comportamenti significativi che si concretino in una attiva e stabile partecipazione⁸. Emergono invece specifiche problematiche sulla competenza territoriale⁹ posto che trattandosi di reato permanente, la competenza territoriale andrebbe sempre individuata *ex art. 8, comma terzo, del codice di procedura penale con la conseguenza che essa spetterebbe al giudice del luogo in cui ha avuto inizio la consumazione del reato*. Tuttavia, qualora — come avviene spessissimo — gli atti del processo non offrano elementi certi per l'individuazione di tale luogo, deve farsi ricorso ai criteri sussidiari previsti dall'art. 9 del codice di procedura penale. Alla luce di tale disposizione, ove non siano comunque percepibili neppure elementi presuntivi che valgano a radicare la competenza territoriale nel luogo in cui il sodalizio criminoso si manifesti per la prima volta all'esterno, possono utilizzarsi criteri desumibili dai reati fine, con particolare riferimento a quello della

⁶ Cfr. PICARELLA L., *Il "cybercrime" come nuova sfida definitoria al concetto di criminalità organizzata*, in *Studi sulla questione criminale*, 2024, p. 105; SPIEZIA F., *Cooperazione internazionale e tutela delle vittime nel "cyberspazio"*, in *Diritto penale e processo*, 2022, p. 1137; ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in *Amministrativ@mente*, 2021, p. 545.

⁷ Cass. Sez. F, Sentenza n. 46156 del 29/8/2013 e Sentenza n. 50620 del 12/09/2013.

⁸ Così Sez. 2 -, Sentenza n. 28868 del 02/07/2020 con riferimento ad una fattispecie di associazione a delinquere finalizzata

alla realizzazione di plurime condotte di frode informatica *ex art. 640-ter cod. pen.*, commesse mediante captazione di codici identificativi di carte di credito, clonazione delle stesse e conseguente svolgimento di una pluralità di operazioni bancarie caratterizzate dall'uso del pos collegato all'attività commerciale dell'imputato.

⁹ Sez. 6, Sentenza n. 3067 del 04/10/1999. Nella specie, nella quale l'associazione aveva ad oggetto i reati di accesso abusivo a sistema informatico e frode informatica, mediante ingresso in rete telefonica, attraverso un'utenza dalla quale venivano abusivamente raggiunte, in modo fraudolento e reiterato, utenze estere, si è ritenuto territorialmente competente il giudice del luogo dell'ultima telefonata.

consumazione dell'ultimo reato fine, specialmente nel caso in cui detti reati siano stati tutti commessi nello stesso luogo e siano poi tutti dello stesso tipo e rientranti nel medesimo schema criminoso.

3. LE STRATEGIE POSSIBILI E LE PROBLEMATICHE EFFETTIVE.

Si pone il problema di una azione di contrasto più concreta ed efficace, basata sulla elaborazione sistematica di informazioni puntuali ed in grado di incidere sui movimenti delle criptovalute durante le trattative, specialmente in contesti di indagini sulle attività illecite. È appena il caso di ribadire che si tratta di indagini che vanno condotte in modo sollecito già dalle primissime fasi dell'emersione dei messaggi estorsivi e che l'emergere di profili problematici o di tipo tecnico o di tipo giuridico (per esempio la frequente contestazione circa la competenza territoriale a seconda del mezzo fraudolento utilizzato) rischia ogni giorno di frenare, rendendo pressoché impossibile, una reazione istituzionale adeguata, tanto che spesso si ritiene opportuno concentrarsi su altre figure criminosi, come l'accesso illecito spesso considerate, a torto, il paradigma della totalità dei reati informatici e delle correlative condotte, che peraltro spesso si presentano in forma di concorso di reati.

Una delle modalità principali per bloccare le criptovalute è attraverso il sequestro delle chiavi private — ove disponibili — che consentono l'accesso ai *wallet*, cioè al vero e proprio “portafoglio” virtuale inteso ovviamente come strumento esclusivo e personalizzato di accesso e di disponibilità patrimoniale oltre che di abilitazione ai relativi movimenti. Il possesso della chiave privata è essenziale per controllare e movimentare le criptovalute; senza di essa, le valute virtuali diventano sostanzialmente inaccessibili. Ed ogni intervento del genere non può concepirsi senza un intervento presso i fornitori di servizi relativi alle criptovalute o tramite il sequestro del computer di un soggetto privato. E si tratta di uno strumento che può già essere utilizzato alla luce della normativa penale vigente modificata ed integrata dalla legge 18 marzo 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*¹⁰. L'obiettivo del sequestro delle chiavi private è infatti quello di “congelare” le criptovalute in ambito strettamente processuale impedendo al possessore di utilizzare strumenti di

¹⁰ Cfr. soprattutto CORASANITI G. e CORRIAS LUCENTE, G. *Cybercrime, responsabilità degli enti, prova digitale*, Commento alla legge 18 marzo 2008 n. 48, Padova 2009, p. 3 e ss. Cfr. da ultimo BUSILLO S. *Conservazione e produzione della prova digitale nella*

nuova disciplina europea: il potenziale di allineamento con i principi espressi dalla giurisprudenza di settore, in *Freedom, Security & Justice: European Legal Studies*, 2023, p. 27.

mixing per oscurare la loro tracciabilità sulla *blockchain*. Il che appare particolarmente poi rilevante in caso di indagini penali o azioni di contrasto al riciclaggio e all'autoriciclaggio dei proventi criminosi ¹¹.

A livello europeo è stata sviluppata una *Counter Ransomware Iniziative* (CRI) ¹² che ha definito alcuni obiettivi principali per contrastare la crescente minaccia del ransomware attraverso la cooperazione tra i paesi membri. Gli obiettivi principali della CRI includono già forme di cooperazione con la giustizia e soprattutto responsabilizzazione degli operatori in criptovalute in tal senso. Sul piano tecnico viene suggerita una attività di genere “disruptive” idonea a contrastare le operazioni degli attori ransomware e dei loro facilitatori, perseguendoli nella misura consentita dalle leggi nazionali attraverso una attenzione sistematica in grado di contrastare la capacità “tecnica” degli attori ransomware di trarre profitto dai proventi illeciti implementando e applicando misure di anti-riciclaggio e contrasto al finanziamento del terrorismo, inclusi i requisiti “conosci il tuo cliente” (KYC) per le criptovalute. Il che evidentemente richiede ed implica ancora di più una costante cooperazione sul piano internazionale pubblico/privato e una continua condivisione delle informazioni utili in tale ambito specie sul terreno investigativo ¹³.

Una collaborazione alla condivisione sull'uso improprio delle infrastrutture per lanciare attacchi si può ritenere davvero essenziale per garantire che garantendo che le infrastrutture nazionali non siano utilizzate proprio per realizzare per tali attacchi. Inoltre si evidenzia l'esigenza di sviluppare specifiche capacità analitiche e soprattutto organizzare in ambito locale strumenti pratici per costruire la resilienza sviluppando e moltiplicando politiche di best practice per l'implementazione nei vari paesi. In tale prospettiva assume rilievo fondamentale il senso globale della resilienza “condivisa” per migliorare in senso collettivo con una cooperazione estesa a diversi soggetti per iniziative efficaci ed immediate contro fenomeni criminali informatici così complessi

¹¹ Cfr. ANTINUCCI M., SCAMPOI D., *Il sequestro e la confisca di bitcoin*, in *Diritto penale e processo*, 2024, p. 1083; ONNIS S., *Il reato di autoriciclaggio: rassegna di giurisprudenza sui principali aspetti della fattispecie*, in *Responsabilità civile e previdenza*, 2024, p. 760; COMPOSTELLA R., CIPRIANI R., *Reimpiego in “bitcoin” di denaro proveniente da reato e autoriciclaggio: una soluzione (troppo) semplice per una realtà (molto) complessa*, in *Banca borsa e titoli di credito*, 2024, p. 182. ERRICO G., *Sequestro preventivo di valute virtuali, tra incertezze e prospettive*, in *Giurisprudenza italiana*, 2024, p. 435; APOLLONIO A., VALLONE

M., “Cyber-Laundering” di proventi mafiosi tra prassi criminale, investigazioni e (lacune del) diritto penale, in *Cassazione penale*, 2023, p. 2691.

¹² <https://digital-strategy.ec.europa.eu/en/news/international-counter-ransomware-initiative-strengthening-cybersecurity-cooperation-actions>.

¹³ Ed in questo senso appare straordinaria l'esperienza delle squadre investigative comuni, cfr. COLAIACOVO G., *Squadre investigative comuni e investigazioni congiunte: una prima lettura*, in *Diritto penale e processo*, 2022, pp. 1147.

attraverso iniziative di sensibilizzazione, formazione e preparazione. In tal senso viene evidenziata l'importanza di politiche per scoraggiare non solo i privati ma anche i governi e le istituzioni dal pagare riscatti, al fine di ridurre l'incentivo economico per gli attaccanti. Questi obiettivi sono già supportati da vari gruppi di lavoro all'interno della ENISA che è l'organizzazione europea della cybersicurezza, ciascuno focalizzato su aspetti specifici come resilienza, diplomazia, interruzione delle operazioni criminali, contrasto al finanziamento illecito e *partnership* pubblico-private¹⁴.

Un modo più analitico per controllare il flusso di criptovalute è attraverso gli obblighi di verifica e segnalazione imposti ai soggetti che permettono l'entrata e l'uscita dal mondo "virtuale", come gli *exchange*. Questi operatori dovrebbero essere in condizioni di effettuare ed assicurare su impulso degli investigatori adeguate verifiche sulla provenienza dei fondi e sulla titolarità effettiva, agendo come una sorta di "dogana" per impedire che criptovalute di origine illecita inquinino la valuta reale, ma non è sempre possibile a causa della immediatezza dello scambio e della sua caratteristica di carattere globalizzato. Le operazioni di polizia spesso si avvalgono ordinariamente della cooperazione internazionale per bloccare i fondi e coordinare le indagini, ed un ruolo sempre più importante è quello assunto da Europol. Ed è proprio, infatti, Europol a fornire il principale riferimento organizzativo e di strategia per il contrasto al fenomeno¹⁵. Per le indagini, le autorità ci si avvale anche di software specializzati per l'estrazione, la conservazione e la copia dei dati presenti nei sistemi informatici. Questi strumenti possono contribuire ad analizzare efficacemente la *blockchain* e a ricostruire perciò la provenienza e il flusso delle criptovalute (attraverso analisi sistematica delle chiavi pubbliche peraltro integralmente disponibili delle transazioni). Sono possibili quindi analisi molto più sofisticate e sistematiche sul fenomeno. Ma ciò richiede un preciso e determinato

¹⁴ <https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-only-the-tip-of-the-iceberg>.

Già il rapporto ENISA del 2022 segnalava un totale di 623 incidenti *ransomware* nell'UE, nel Regno Unito e negli Stati Uniti per un periodo di riferimento da maggio 2021 a giugno 2022. I dati sono stati raccolti da report di governi e aziende di sicurezza, dalla stampa, da blog verificati e in alcuni casi utilizzando fonti correlate dal dark web. Tra maggio 2021 e giugno 2022 circa 10 terabyte di dati sono stati rubati ogni mese da attori della minaccia ransomware. Il 58,2% dei dati rubati includeva dati personali dei dipendenti. Sono stati trovati al-

meno 47 attori unici della minaccia ransomware. Per il 94,2% degli incidenti, non si è stati in grado di sapere se l'azienda ha pagato il riscatto o meno. Tuttavia, quando la negoziazione fallisce, gli aggressori di solito espongono e rendono disponibili i dati sulle loro pagine web. Questo è ciò che accade in generale ed è una realtà per il 37,88% degli incidenti. Si può quindi concludere che il restante 62,12% delle aziende ha raggiunto un accordo con gli aggressori o ha trovato un'altra soluzione..

¹⁵ <https://www.europol.europa.eu/publications-events/publications/ransomware-what-you-need-to-know>.

impegno delle istituzioni che non può limitarsi ad un singolo ambito, ma deve fondarsi su una analisi integrata, collegiale e interdisciplinare di cybersicurezza applicata. Maggiore utilità potrebbe avere allora potenzialmente la *sospensione delle negoziazioni di crypto-attività* ove si ritenga (come si dirà possibile almeno in astratto sulla base poi del recente regolamento (UE) 2023/1114 relativo ai mercati delle crypto-attività c.d. MICA che è entrato in vigore nel 2024) che la situazione dell'emittente o del soggetto che le gestisce pregiudichi gli interessi dei possessori, in particolare dei detentori al dettaglio. Le autorità competenti potrebbero agire in tal senso (e quindi Consob e Banca d'Italia in base alle competenze di attuazione del nuovo regolamento MICA con il contributo della Agenzia per la cybersicurezza nazionale) come peraltro espressamente previsto all'art. 9 comma 4 del decreto legislativo 5 settembre 2024, n. 129 che fissa l'importante principio di cooperazione tra più autorità competenti in un quadro che poi si ricollega alle funzioni di cui al decreto legislativo 4 settembre 2024, n. 138 (*Recepimento della direttiva (UE) 2022/2555, cd NIS 2 relativa a misure per un livello comune elevato di cibernsicurezza nell'Unione*).

Si sostiene spesso come potrebbero essere utili anche politiche più restrittive che potrebbero delinearsi nel vietare o quanto meno limitare la commercializzazione, la distribuzione o la vendita di talune crypto-attività, o tipi di attività ad esse relative, se esistono fondati motivi di preoccupazione per la tutela degli investitori o per la stabilità dei mercati. Inoltre tutti i prestatori di servizi per le crypto-attività dovrebbero sempre adottare misure per garantire la sicurezza dei sistemi e dei dati, prevenire i conflitti di interesse e proteggere i fondi e le crypto-attività dei clienti. Essi dovrebbero anche avere ed esercitare politiche di continuità operativa per garantire la conservazione dei dati in caso di interruzioni dei sistemi. Ma ogni emissione di token collegati ad attività o prestazione di servizi per le crypto-attività si muove in un ambito ambiguo ed incerto nel quale è molto difficile da un lato ogni intervento tecnico data l'immediatezza delle operazioni, sia definire un quadro di operazioni effettivamente controllabili preventivamente da parte delle autorità competenti, che valutano se i richiedenti, ad esempio soddisfino requisiti necessari e collaborino con le autorità per la lotta al riciclaggio e al finanziamento del terrorismo ¹⁶. Può quindi auspicarsi una azione combinata e costante, ma soprattutto rapida, delle autorità competenti in ambito MICA per incidere sulle criptovalute du-

¹⁶ Cfr. DAVI E., "Bitcoin e cyber self-laundering": lo sguardo sospettoso della Cassazione sull'impiego di criptovaluta, in *Il Foro italiano*, 2023, p. 15.

MINTO A., *Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non Fungible Tokens ("NFT")*, in *Rivista di diritto bancario*, 2023, p. 31; RAZZANTE R., *Il pa-*

rante le trattative per esempio si potrebbe basare su una combinazione di sequestro delle chiavi private, controllo degli operatori, blocco dei conti, cooperazione internazionale e utilizzo di *tecnologie investigative avanzate* nonché su una *forte cooperazione con le vittime* anche attraverso le associazioni di categoria e la istituzione di interventi di sostegno alla luce di quanto è già avvenuto per il racket e l'usura¹⁷ e il tutto nel quadro di una efficiente cooperazione istituzionale pubblico-privato per favorire cybersicurezza e resilienza dei rispettivi sistemi informatici.

4. POLITICHE DRASTICHE COME PER I SEQUESTRI DI PERSONA?

Il dibattito sull'opportunità di vietare il pagamento dei “ricatti” in caso di attacchi *ransomware*, analogamente a quanto avviene per i sequestri di persona in base alla legge n. 8 del 1991 in Italia, presenta analogie solo apparenti. Infatti mentre per il sequestro di persona solitamente viene avviata una trattativa che ha tempi molto lunghi di definizione, in genere anche molti mesi mentre per quello che riguarda il *ransomware* la richiesta è contenuta direttamente nel messaggio di avvio del software malevolo e si concreta quasi sempre se non totalmente nella indicazione di un link attraverso il quale procedere al versamento in criptovaluta entro un termine che in genere non supera, a seconda della vittima, pochi giorni al massimo impostato automaticamente attraverso un timer che è integrato nella interfaccia. Appare anche evidente che lo strettissimo termine temporale imposto per tale versamento impostato automaticamente non renderebbe possibile in pratica un intervento giurisdizionale tanto più se impostato nello schema del sequestro preventivo alla luce della legge n. 8 del 1991 tenendo conto anche che bisogna tenere conto del termine di 24 ore previsto per la denuncia dell'episodio di compromissione del sistema. Proibire cautelatamente il pagamento dei “ricatti” in criptovaluta potrebbe certo diminuire l'attrattiva economica degli attacchi ma di certo non escluderebbe di per sé il rischio di connessioni attraverso intermediari (magari attraverso operazioni riportate come manutenzione di sistemi compromessi) che possano svolgere sostanzialmente la medesima azione intervenendo sul sistema compromesso effettuando il pagamento richiesto eventualmente dissimulando la spesa, anche frazionata di un possibile intervento di manutenzione sul sistema medesimo. Tutto ciò peraltro avviene in pochissime ore al massimo nel termine di pochi giorni e potrebbe prendere del tutto vano tanto un possibile

norma delle regole UE su “blockchain” e “crypto asset”, in *Notariato*, 2023, p. 579.

¹⁷ Ci si riferisce alle leggi n. 103 del 1996, Disposizioni in materia di usura e legge

n. 44/1999 istitutiva del Fondo di solidarietà per le vittime delle richieste estorsive e dell'usura.

intervento giudiziario quanto addirittura un intervento amministrativo a meno che esso non sia presidiato da una comunicazione automatica e vincolata dell'intervenuta transazione in criptovaluta non ricollegabile ad attività correnti del soggetto compromesso soprattutto, da intendere quale movimentazione anomala e quindi tale da poter essere eventualmente bloccata a seguito di successivi controlli, ma anche su questo punto potrebbe adombrarsi l'ipotesi di falsi positivi tanto più in un quadro di potenziale frazionamento della somma estorta o di adempimento dell'operazione da parte di un terzo abilitato. Di certo il terreno ideale sembra essere quello della repressione coordinata e della prevenzione di futuri attacchi. In alcuni casi, il pagamento del riscatto è visto come l'unica soluzione per ripristinare rapidamente le operazioni e minimizzare le perdite.

Ma non vi è ovviamente alcuna garanzia che i *files* illeggibili vengano decriptati una volta effettuato il pagamento. Pagare il riscatto è solo apparentemente la soluzione più facile, perché oltre al danno diretto economico, si corre infatti il rischio di non ricevere affatto i codici di sblocco, o quello molto più concreto di essere inseriti proprio per ciò successivamente in "liste di pagatori" potenzialmente quindi soggetti a periodici (e appunto programmabili anche con tecniche di intelligenza artificiale) nuovi attacchi *ransomware*. La soluzione migliore sembra ancora quella preventiva di carattere tecnico sempre che sia possibile e soprattutto noto il sistema di decrittazione utilizzato. Un divieto drastico — tanto più se eventualmente penalmente sanzionato come avvenne per i sequestri di persona — potrebbe lasciare le vittime senza alternative immediate. Imporre sanzioni di carattere penale o amministrativo (che poi in ogni caso sembra essere la via migliore) a chi paga un riscatto per proteggere dati sensibili essenziali o garantire la continuità dei servizi essenziali potrebbe persino sollevare questioni etiche, soprattutto quando sono in gioco valori fondamentali la sicurezza pubblica o la vita delle persone, come nel caso di una infrastruttura sanitaria. Le criptovalute, come soprattutto sono allora un facilitatore fondamentale per gli attacchi *ransomware*, rappresentando appunto circa il 98% dei pagamenti dei riscatti. La loro sostanziale anonimità rende difficile in ogni caso tracciare con precisione i flussi di denaro rendendole l'ideale strumento per ogni condotta criminale di carattere estorsivo a tutti i livelli.

Ma ciò non significa che non siano possibili indagini, anzi, esse possono sfruttare adeguatamente le tecniche disponibili di analisi del flusso delle chiavi pubbliche e utilizzare strumenti tradizionali e combinati per ricostruire l'intera condotta criminosa, avvalendosi degli strumenti già disponibili offerti dalla Convenzione di Budapest sul Cybercrime del 2001 aggiornata con protocolli re-

centi che si riferiscono al *cloud* ¹⁸. Gli importi dei riscatti possono variare significativamente. Le richieste iniziali possono essere molto elevate, ma spesso poi vengono progressivamente ridotte durante le negoziazioni (ovviamente in questo caso le indagini possono anche incentrarsi sulla messagistica potenzialmente tracciabile e sulla ricorrenza della medesima) I criminali informatici utilizzano tattiche di estorsione spesso diversificate e dinamiche per forzare il pagamento dei riscatti, che includono la minaccia di divulgare informazioni sensibili o di rendere inutilizzabili i sistemi. Queste tattiche possono influenzare sensibilmente in modo “adattativo” la somma finale pagata dalle vittime e tutto lascia intendere che vi sia una precisa profilazione delle vittime in termini di capienza economica e di disponibilità al pagamento del riscatto in termini estorsivi pur di rientrare nella disponibilità del sistema violato (che in pratica viene letteralmente “bloccato” fino all’invio del codice di decriptazione una volta completata la procedura di accredito).

Le analisi disponibili dimostrano comunque la variabilità e la crescente possibilità di negoziazione ¹⁹, il che sicuramente assimila tali tecniche a quelle prima utilizzate per i sequestri di persona. Anche se il pagamento del riscatto può sembrare la via più semplice, spesso le aziende devono affrontare costi aggiuntivi per il ripristino dei sistemi, la gestione della crisi e le possibili azioni giudiziarie. L’intervento di esperti nella gestione di un attacco ransomware può portare ai migliori risultati per le vittime. Ma si tratta di attività che hanno margini temporali strettissimi.

Va sottolineato anche come nonostante la grande quantità di attacchi, poi solo una piccola percentuale delle vittime finisce per pagare effettivamente il riscatto ²⁰, ovviamente spesso tendendo a mascherare tale operazione quale costo delle operazioni di manutenzione del sistema informatico. Il che apre scenari certamente rilevanti sotto il profilo civilistico sul piano della validità di clausole nei contratti di manutenzione informatica stipulati da soggetti pubblici e privati. I negoziati portano a una riduzione dell’importo iniziale richiesto, evidenziando come le cifre iniziali siano spesso gonfiate, inoltre il pagamento non garantisce il ripristino dei dati e incentiva semmai ulteriormente i criminali a

¹⁸ <https://www.coe.int/en/web/cybercrime/the-budapest-convention> e soprattutto <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=224>.

¹⁹ il ransomware Akira risulterebbe avere negoziato pagamenti tra 75.000 e 1.075.995 di dollari, con richieste iniziali che arrivano anche a 10.000.000 di dollari a

seconda del destinatario. Altri ransomware, come Avaddon, Babuk, BlackBasta, e Conti, mostrano una vasta gamma di pagamenti negoziati.

²⁰ Ad esempio, in un report sul gruppo Ransomhub, si è scoperto che solo l’11,2% delle vittime ha pagato il riscatto. Mancano comunque dati certi sulla situazione italiana.

compiere altri attacchi, potendosi verosimilmente immaginare che tutti i pagatori, peraltro già profilati come potenziali vittime siano soggetti appunto a nuova profilazione proprio in rapporto alla documentata disponibilità.

Un recente *Report dell'Associazione di Ginevra* delle imprese assicuratrici ²¹ sottolinea proprio l'importante ruolo degli assicuratori privati, insieme ai Governi, nel rafforzare la resilienza della società rispetto ai casi di ransomware, e nel garantire che si possano realizzare tutti i benefici della digitalizzazione proprio attraverso la copertura assicurativa del rischio informatico. Il Rapporto esplora il significativo valore aggiunto dell'assicurazione informatica al di là del trasferimento del rischio, nell'ambito del dibattito in corso sull'opportunità di vietare i pagamenti di riscatti o le coperture assicurative associate.

Nella prospettiva dei privati l'assicurazione informatica fornisce una minima protezione finanziaria e supporto operativo vitali in caso di attacco, ma comporta anche problematiche di accertamento assicurativo *ex post* non sempre facilmente definibili ²². L'assicurazione per eventi ransomware non si limita infatti spesso a fornire copertura per il pagamento di riscatti, perché può prevedere anche la copertura di danni ulteriori subiti dalle vittime o da terzi e, ad esempio, organizzare il supporto di esperti nella gestione degli incidenti. L'assicurazione — in questa prospettiva — aiuta le organizzazioni a identificare e affrontare le vulnerabilità della sicurezza informatica e ad adottare una migliore prevenzione dei rischi in un panorama in rapida evoluzione. Si delinea, quindi, un ruolo istituzionale essenziale più articolato soprattutto sul piano della prevenzione e dell'assistenza per contrastare gli attacchi ransomware, poiché le politiche pubbliche dovrebbero mirare a scoraggiare le violazioni, contrastare i modelli di business criminale mediante l'uso illecito e sistematico di criptovalute. Il processo di qualificazione messo in atto dagli assicuratori aiuta poi spesso le organizzazioni di imprese assicurate, esattamente come avviene per i trasporti oggetto di rischio di rapina, a sviluppare una strategia di sicurezza comprensiva che tenga conto delle specificità funzionali del fenomeno.

Per determinare la copertura e i premi più adeguati, inoltre le compagnie assicurative valutano il rischio esistente attraverso le cautele già messe in atto dai potenziali clienti. Se questi soddisfano i rigorosi requisiti di qualificazione e sono in grado di

²¹ <https://www.panoramassicurativo.ania.it/articoli/83720>.

²² Il ransomware ha rappresentato il 75% di tutte le richieste di risarcimento per le assicurazioni informatiche nel 2020 (AM Best) ed è probabile che sia stata anche la categoria di eventi di perdita più costosa nel

2021 (WTW). Il Rapporto analizza le complesse questioni politiche che circondano il ransomware e le possibili soluzioni per contrastare questa epidemia di criminalità informatica, compreso il contributo delle assicurazioni al rafforzamento della resilienza informatica delle aziende.

identificare i rischi informatici ricorrenti, l'assicurazione in genere sa che sono state messe a punto misure di sicurezza efficaci.

Di fronte a minacce estorsive, tanto più in un quadro normativo evolutivo che si è gradualmente ampliato non solo istituendo una specificità di indagini in tema di criminalità organizzate, potrebbero ravvisarsi di maggiore utilità anche misure organizzative a favore delle vittime, esattamente come previsto per altre attività estorsive o di usura, in un contesto però molto diverso e caratterizzato in ambito informatico.

Occorre anche cioè tendere ad ogni livello ad incentivare la resilienza, esattamente come avviene per la sicurezza stradale promuovendo così una cooperazione tra imprese assicurative e la necessaria adozione di più efficaci misure di carattere preventivo e un contesto istituzionale interattivo di effettiva analisi dei dati sul cybercrime in termini giuridici, economici e sociali. In ogni caso è immaginabile, ove si voglia perseguire una idea di sanzione anche sul piano civilistico rispetto ai contratti assicurativi (misura contenuta peraltro nello schema messo in pratica nel 1991 contro i sequestri di persona) — al di là dei problemi di conformità alla legislazione di settore europea che potrebbero sorgere — prevedere semmai una specificazione delle sanzioni civili in modo da circoscrivere l'ambito ai soli aspetti di rimborso della copertura per la spesa direttamente collegata al pagamento del "riscatto" e semmai allargare la previsione, per renderla più adeguata alla realtà odierna ai contratti di assistenza e manutenzione operativa di software tramite i quali spesso avviene concretamente il pagamento delle somme estorte solitamente utilizzando criptovaluta. In caso di attacco, il processo di elaborazione delle richieste di risarcimento consente alle aziende di accedere con facilità all'assistenza operativa e finanziaria prevista dalla polizza sottoscritta.

Il processo di risarcimento in concreto ad opera delle imprese assicurative inoltre prevede poi, in molti casi, passaggi di controllo sistematico per cui per presentare una richiesta di indennizzo, le organizzazioni devono dunque implementare tecnologie, procedure e pratiche per acquisire le prove e le informazioni necessarie, ad esempio analisi forensi, registri, rapporti e richieste di riscatto. Le organizzazioni che hanno predisposto un piano di *incident response* potranno così dimostrare in ogni sede di aver sostenuto le spese correlate alle comunicazioni il cui rimborso è previsto dalla polizza, come la ricerca di esperti in relazioni pubbliche, le notifiche relative al rispetto delle normative, il coordinamento dell'invio delle informazioni agli stakeholder interni ed esterni.

Ogni piano di *incident response* stabilisce infatti preventivamente i ruoli, le responsabilità, la pianificazione e i protocolli di comunicazione necessari a contenere e a estirpare le minacce attive. È inoltre indispensabile che le aziende conoscano le specifiche della propria polizza assicurativa, ad esempio i limiti di

copertura e i requisiti per la presentazione delle richieste di risarcimento. Le principali tutele e le opzioni di copertura tipiche includono attualmente la copertura per il recupero dei dati, il risarcimento finanziario, il supporto legale, l'assistenza per le relazioni pubbliche e i danni alla reputazione, le attività di *incident response* (ma su queste tuttavia mancano specifiche analisi per verificare se tra esse vada ricompreso talora il rimborso delle cifre corrisposte a seguito di ransomware). Tali tutele coprono le possibili ripercussioni sulle finanze, la reputazione e l'operatività dell'azienda conseguenti a un attacco ransomware. La collaborazione tra compagnie assicurative e aziende consente a queste ultime di prevedere anche polizze personalizzate basate sulle esigenze, i requisiti e i livelli di rischio specifici. Se ben progettate, possono garantire all'azienda la copertura più completa possibile e ridurre nettamente la probabilità di lacune nella sicurezza. Sul premio assicurativo incidono numerose variabili, tra cui la dimensione dell'azienda, il settore di appartenenza, i livelli di esposizione al rischio e l'importo della copertura richiesta.

Inoltre, dimostrando di aver predisposto misure continuative di mitigazione dei rischi del ransomware, nel tempo le aziende assicurate potranno sempre di più ridurre i premi. Sebbene la domanda di assicurazioni specifiche di copertura del rischio informatico sia elevata, l'aumento dei costi delle assicurazioni informatiche sta rendendo estremamente difficile per le aziende, in particolare le piccole e medie imprese, trovare una copertura. Le problematiche sono note e peraltro rispecchiano in tutta Europa ormai un diaframma tra la presa d'atto di un fenomeno criminale di particolare rilevanza rispetto al quale l'assicurazione costituisce un potenziale argine e l'incremento dei costi, anche sensibili, che proprio l'aumento del rischio di eventi dannosi di fatto incrementa²³. Gli assicuratori in genere richiedono sempre di più preliminarmente requisiti di sicurezza di fondo e sistemi più severi e certificati per le aziende assicurate. Alcuni non predispongono nemmeno un preventivo assicurativo a meno che una società non disponga già di misure molto elevate di autenticazione a più fattori, crittografia dei dati, zero-trust o politiche indicative

²³ Secondo MARSH MCLENNAN, i prezzi delle assicurazioni informatiche risultano aumentati del 110% nel primo trimestre del 2022. Un nuovo ceppo di ransomware, HardBit, chiede persino alle vittime di condividere i dettagli delle loro polizze informatiche in modo che gli hacker possano calcolare un riscatto che verrà coperto dalla polizza. Gli assicuratori dispongono di dati storici limitati sui costi degli attacchi informatici, il che rende difficile creare modelli

di rischio accurati e fissare prezzi stabili. Solo quando le compagnie assicurative hanno visto aumentare le loro perdite, rispondono aumentando i premi e limitando la copertura. L'assicurazione AXA ha smesso di coprire i pagamenti per ransomware per le polizze rilasciate in Francia. Lloyd's of London non coprirà più attacchi informatici sponsorizzati dallo stato, un'altra fonte di gravi perdite.

di adeguata sicurezza di fondo. Alcune imprese assicurative stanno peraltro già assumendo un ruolo più di consulenza, offrendo agli assicurati e agli imprenditori l'accesso a strumenti di sicurezza integrati alla polizza e fornitori di servizi per aiutarli a mitigare il rischio ransomware.

Il tema generale può allora essere meglio sviluppato perché integra le disposizioni sull'obbligo di notifica di incidente informatico come previsto dall'art. 25 del decreto legislativo 4 settembre 2024, n. 138 (Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione c.d. NIS 2) concepito proprio in funzione di rafforzamento della cibersicurezza delle strutture pubbliche e private di rilevante interesse nazionale in qualche modo sincronizzandole in tema di sicurezza dei dati personali (*data breach*) con l'art 33 del Regolamento UE 2016/679 (GDPR)²⁴ che in materia di sicurezza. In sostanza entrambi i sistemi si comprendono in rapporto ad una esigenza primaria, da un lato la cibersicurezza comune e dall'altro il rispetto per i dati raccolti dal trattamento (informatico), pur tuttavia in assenza di opportuni strumenti di "lettura" delle informazioni raccolte per la valutazione in chiave diagnostica e di monitoraggio e di analisi, specie di fronte a fenomeni così complessi, che si caratterizzano in ambito internazionale e richiedono tecnologie specifiche di accertamento da svolgere anche in tempi ragionevolmente brevi in rapporto agli interessi rispettivamente protetti entrambi di rilievo primario: il diritto di impresa e la sicurezza informatica nel suo insieme.

Peraltro proprio sui *data breach* occorrerebbe una analisi statistica dei dati disponibili tra Garante per la protezione dei dati personali²⁵ e Agenzia per la cibersicurezza nazionale²⁶, al primo sono trasmesse denunce anche molto dettagliate a seguito di diffusione illecita di dati personali (anche derivante da reati

²⁴ Cfr. RENNA M., *Data breach disclosure duties*, in *European Journal of Privacy Law & Technologies*, 2019, p. 79; MORRIS A., MACUIRE M., STUTTARD N., *Preventing Data Breaches from occurring in European Journal of Privacy Law & Technologies*, 2018, p. 132. Sui profili civilistici cfr. COLACINO G., "Data breach", *danni non patrimoniali e art. 32 g.d.p.r.: il problema della polifunzionalità del rimedio risarcitorio*, in *Rassegna di diritto civile*, 2023, p. 48.

²⁵ Il Garante può in tal caso prescrivere misure correttive ai sensi dell'58, paragrafo 2, del Regolamento UE 2016/679 nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, *anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione*. Sono

previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di Euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale. Inoltre proprio il Garante riceve i dati statistici ricevuti dagli uffici giudiziari ai sensi all'art. 154 comma 6 del Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali in materia di criminalità informatica, ancora vigente. È opportuna comunque una completa revisione di tali comunicazioni introducendo una condivisione tra diverse autorità coinvolte, per esempio anche Agid e Autorità per le garanzie nelle comunicazioni che pure sono chiamate a svolgere un ruolo strategico in tema di infrastrutture private e pubbliche.

²⁶ Cfr. RICOTTA F. N. A., *Agenzia per la "cibersicurezza" nazionale, sicurezza*

informatici) e all'Agenzia informazioni sull'incidente informatico nello specifico, che però non sempre può essere ricondotto a condotte criminose. Un coordinamento in materia basato su una lettura coordinata dei dati appare sempre più strategico e fondamentale, unito ad una esigenza altrettanto indispensabile che è quella di provvedere alla acquisizione di elementi statistici attraverso un confronto di carattere continuo ed efficace nella massima cooperazione tra istituzioni diverse e tra queste e i privati cui si riferisce l'ambito di *governance* o di regolamentazione non privo di interesse per l'esercizio della stessa funzione giudiziaria requirante nell'ambito dei reati informatici²⁷.

Pur tuttavia occorre fare di più rispetto alla pura e semplice repressione penale da un lato facilitando l'analisi tecnologica rispetto alle evoluzioni possibili in modo da non intervenire troppo tardi sul piano istituzionale e di assicurare nel contempo una presenza istituzionale efficace tanto nella cooperazione interna che nelle dinamiche complesse e transnazionali di tale forma di criminalità e la più efficace cooperazione in funzione di analisi dei fenomeni criminali informatici rispetto ai quali può articolarsi anche un ruolo istituzionale a vari livelli strategico e coordinandosi con i gruppi di ricerca universitari sulla sicurezza informatica (qualcosa di simile peraltro avviene già in tutte le materie specialistiche come l'ambiente, la tutela del patrimonio artistico e nell'ambito delle stesse discipline sanitarie).

5. LE PROBLEMATICHE EVIDENZIATE IN TEMA DI RICICLAGGIO INFORMATICO MEDIANTE CRIPTOVALUTE.

La Corte di cassazione ha affrontato più volte il tema del

della Repubblica e investigazioni dell'Auto-rità giudiziaria, in *Diritto penale contemporaneo*, 2023, p. 97.

²⁷ Il tema della *governance* della cybersicurezza diviene allora strategico in ambito istituzionale sviluppandosi più di recente in una coordinata serie di relazioni tutte coordinate al miglior livello di soddisfazione di un interesse comune tra pubblico e privato. Cfr. COCCHI T., *La Cybersicurezza nel prisma del diritto dei contratti pubblici: un tentativo di ricostruzione delle regole del gioco tra requisiti di partecipazione, criteri di aggiudicazione ed esigenze di certezza*, in *Munus*, 2024, p. 177; FIORINELLI G., GIANNELLI M., *Il DDL Cybersicurezza (AC 1717). Problemi e prospettive in vista del recepimento della NIS 2 [Network and Information Systems - Reti e Sistemi informativi]. Introduzione*, in *Rivista italiana di informatica e diritto*, 2024, p. 9; CASAROSA F., *L'armonizzazione degli obbli-*

ghi di notifica: il DDL Cybersicurezza fra la NIS 2, in *Rivista italiana di informatica e diritto*, 2024, p. 11; GIANNELLI M., *Il contributo dei livelli di governo substatali al raggiungimento degli obiettivi del ddl Cybersicurezza*, in *Rivista italiana di informatica e diritto*, 2024, p. 15; NANNIPERI L., *Cybersicurezza e appalti pubblici: verso un nuovo (e incerto) quadro regolatorio* in *Rivista italiana di informatica e diritto*, 2024, p. 19; PIETRANGELO M., *Per un modello nazionale di cybersicurezza cooperativa e resilienza collaborativa*, in *Rivista italiana di informatica e diritto*, 2024, p. 25. MORONI L., *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *federalismi.it*, 2024, p. 179; RIZZA M. A., SERINI F., *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2024, p. 115.

riciclaggio e dell'autoriciclaggio in relazione alle criptovalute, evidenziando come l'acquisto di valute virtuali con proventi illeciti possa ostacolare l'identificazione della provenienza del denaro, integrando così il reato di autoriciclaggio. In particolare, è stato sottolineato che l'utilizzo di criptovalute può costituire uno strumento per occultare l'origine illecita dei fondi, rendendo più complessa la tracciabilità delle transazioni.

Integra così il delitto di autoriciclaggio la condotta di chi, in qualità di autore del delitto presupposto di truffa, impieghi le somme accreditategli dalla vittima trasferendole, con disposizione "on line", su un conto intestato alla piattaforma di scambio di "bitcoin" per il successivo acquisto di tale valuta, così realizzando l'investimento di profitti illeciti in operazioni finanziarie a fini speculativi, idonee a ostacolare la tracciabilità dell'origine delittuosa del denaro²⁸. In tema di intermediazione finanziaria, inoltre la vendita "on line" di moneta virtuale "bitcoin" pubblicizzata quale forma di investimento per i risparmiatori — ai quali vengano offerte informazioni sulla redditività dell'iniziativa — è attività soggetta agli adempimenti previsti dalla normativa in materia di strumenti finanziari, di cui agli artt. 91 e seguenti del TUF, la cui omissione integra il reato di cui all'art. 166, comma 1, lett. c), TUF²⁹.

Pur in un quadro solo apparentemente incerto³⁰ la giurisprudenza penale di legittimità sembra perciò confermare e rafforzare un percorso uniforme nella considerazione della valuta digitale come strumento specifico delle condotte di riciclaggio³¹.

L'introduzione e l'attuazione delle disposizioni del MICA Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività, e la correlativa attuazione con decreto legislativo 129/2024 consentono oggi di delineare una prospettiva del tutto nuova e che può essere proprio determinante nel contrasto al ransomware e per-

²⁸ Cass. sez. 2, sentenza n. 27023 del 07/07/2022.

²⁹ Cass. sez. 2, sentenza n. 26807 del 17/09/2020.

³⁰ Corte d'Appello di Milano, sentenza n. 1879 del 13 giugno 2024, nella quale ci si sofferma sulla dimensione monetaria delle criptovalute ed alla distinzione rispetto al concetto (formale) di moneta elettronica. La moneta elettronica è rappresentata da un valore (oggettivamente) monetario denominato in una valuta avente corso legale, mentre le criptovalute sono rappresentazioni digitali di valore non emesse da banche centrali o enti creditizi e non hanno corso legale. Pertanto, l'emissione di criptovalute non autorizzata non rientrerebbe necessariamente nel reato di emissione abusiva di moneta elettronica, a meno che non

presenti caratteristiche specifiche che la assomiglino a quest'ultima. Tale decisione tuttavia non poteva tener conto delle novità regolamentari europee intervenute proprio in tale ambito che sembrano muoversi in direzione opposta, almeno sul piano regolatorio e di governance (di fatto affidata alle stesse autorità monetarie).

³¹ Cassazione penale, Sez. 5 Sentenza n.33204 del 27/08/2024, Sez. 5 Sentenza n.29649 del 19/07/2024, Sez. 2 Sentenza n.23276 del 10/06/2024, Sez. 4 Sentenza n.20341 del 23/05/2024, Sez.3 Sentenza n.17835 del 07/05/2024, Sez. 5 Sentenza n.2538 del 19/01/2024, Sez. 6 Sentenza n.46833 del 21/11/2023 Sez. 5 Sentenza n.37767 del 14/09/2023, Sez. 2 Sentenza n.28279 del 30/06/2023, Sez. 2 Sentenza n.2585 del 20/01/2023.

sino delle frodi informatiche che si basano sulle medesime piattaforme. I principali soggetti oggi tenuti all'obbligo di segnalazione di operazioni sospette includono anche i cambiavalute virtuali (*exchange*), i prestatori di servizi relativi alle criptovalute, e più in generale, tutti i soggetti che, in ragione della loro attività, entrano in contatto con transazioni che potrebbero essere legate a flussi finanziari illeciti. Anche i prestatori di servizi di wallet digitale sono tenuti a tali obblighi. Questi soggetti sono spesso definiti come “*soggetti obbligati*” dalle normative antiriciclaggio.

La segnalazione all'UIF (Unità di Informazione Finanziaria) nel caso di operazioni sospette deve avvenire quando sussiste un fondato motivo per ritenere che un'operazione sia sospetta o che la provenienza dei fondi *possa essere illecita*. Il sospetto deve essere desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento, o da qualsiasi altra circostanza conosciuta. Il che o include anche la capacità economica e l'attività svolta dal soggetto cui l'operazione è riferita. Così ad esempio in genere operazioni di importo inusualmente elevato o la scarsa chiarezza delle informazioni ricevute possono costituire di per sé elementi di sospetto ³².

Per poter identificare le operazioni sospette, i soggetti obbligati dovrebbero essere sempre in condizione di effettuare una adeguata verifica della clientela, identificando i clienti, verificando i dati forniti tramite documenti di identità confrontandoli con fonti esterne affidabili. Questa verifica dovrebbe poter essere eseguita all'instaurazione di un rapporto continuativo, *ma anche in caso di prestazioni occasionali*. Il che apre certo anche una serie di problemi pratici spesso molto delicati, anche in rapporto ai profili di trattamento dei dati personali. L'adeguata verifica in teoria dovrebbe includere così anche la verifica della titolarità effettiva dei capitali virtuali. L'identificazione del cliente potrebbe avvenire anche attraverso mezzi di identificazione elettronica o altre procedure di identificazione a distanza. Le operazioni sospette in criptovalute devono essere segnalate all'UIF. La segnalazione è obbligatoria e il mancato rispetto di questo obbligo può comportare sanzioni amministrative e penali. L'obbligo di segnalazione si accompagna al divieto di informare il cliente dell'avvenuta segnalazione, per evitare di compromettere le indagini. La normativa di riferimento in Italia è ancora principalmente il d.lgs. 231/2007, come modificato dal d.lgs. 90/2017, che aveva già introdotto appositi obblighi specifici riferibili anche ai prestatori di servizi relativi a valute virtuali ³³.

³² Cfr. lo studio UIF (2024) <https://uif.bancaditalia.it/publicazioni/quaderni/2024/quaderno-25-2024/quaderno-25-2024.pdf>.

³³ Queste norme sono poi state ulteriormente integrate dal d.lgs. 125/2019 che stabilisce l'obbligo di iscrizione in una se-

La normativa italiana ha già avuto modo di recepire in sostanza le raccomandazioni del GAFI (*Gruppo di Azione Finanziaria Internazionale*). Si tratta di un quadro normativo esistente che potrebbe essere ulteriormente rafforzato attraverso il contributo di carattere tecnico e organizzativo proprio per impedire il conseguimento del profitto delle ipotesi estorsive di carattere informatico, peraltro in coerenza con il rafforzamento del contrasto alle frodi informatiche, sempre di più anche queste basate su criptovalute.

Già una prima relazione dell'UIF e di Banca d'Italia del 2019 ³⁴ segnalava infatti: *“È inoltre da considerare l'utilizzo di Virtual asset connesso con sospetti di abusivismo e con violazioni della disciplina in materia di: i) offerta al pubblico di prodotti finanziari, qualora siano promessi rendimenti periodici collegati all'operatività in Virtual asset; ii) prestazione di servizi di investimento, laddove agli investitori sia offerta la possibilità di effettuare “operazioni regolate per differenza aventi come sottostante (anche) valute virtuali”*. Infatti *“per il corretto apprezzamento delle situazioni è necessario valutare attentamente le caratteristiche dei soggetti, anche specializzati, a vario titolo coinvolti nell'operatività in Virtual asset, nonché la presenza di: collegamenti, diretti o indiretti, con soggetti sottoposti a procedimenti penali o a misure di prevenzione ovvero con persone politicamente esposte o con soggetti censiti nelle liste pubbliche delle persone o degli enti coinvolti nel finanziamento del terrorismo; soggetti con residenza, cittadinanza o sede in Paesi terzi ad alto rischio ovvero in una zona o in un territorio notoriamente considerati a rischio, in ragione anche dell'elevato grado di infiltrazione criminale; soggetti operanti in aree di conflitto o in Paesi che notoriamente finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche, ovvero in zone limitrofe o di transito rispetto alle predette aree; strutture proprietarie artificiosamente complesse od opache volte a rendere difficoltosa l'individuazione del titolare effettivo; soci e/o esponenti apparentemente privi delle competenze tecniche che tipicamente il settore richiede”*.

La Banca d'Italia e la Consob, in qualità di autorità di vigilanza del sistema finanziario italiano, non dispongono ancora sul piano tecnico di strumenti diretti per bloccare singole transazioni in criptovalute. La Banca d'Italia ha tuttavia emesso avvertenze riguardo all'utilizzo delle valute virtuali, sottolineando che queste

zione speciale del registro dei cambiavalute per chi offre servizi legati alle valute virtuali. L'art. 55 del d.lgs. 231/2007 prevedeva già sanzioni per chi falsifica i dati relativi al cliente o utilizza dati falsi, mentre

l'art. 39 sanzionava le comunicazioni al cliente circa l'avvenuta segnalazione.

³⁴ https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/comunicazione_vv_2019.pdf.

non hanno corso legale in Italia e non sono emesse o garantite da alcuna autorità centrale. Inoltre, la stessa Banca d'Italia ha sempre evidenziato i rischi associati all'uso delle criptovalute, tra cui l'assenza di tutela legale specifica in caso di contenzioso o fallimento delle piattaforme di scambio ³⁵. La Consob peraltro ha sottolineato in più di una occasione che le piattaforme di scambio su cui si acquistano e vendono valute digitali e forme di investimento non sono sempre adeguatamente regolamentate, il che implica l'assenza di una sostanziale tutela legale specifica per gli investitori. Inoltre, la Consob ha evidenziato rischi concreti in tale situazione, tra cui la possibilità di truffe seriali e l'uso costante per attività illegali ³⁶.

Con l'introduzione del Regolamento (UE) 2023/1114 relativo ai mercati delle crypto-attività (*MiCAR*), si prevede infine una maggiore tendenziale e soprattutto interagente regolamentazione del settore. In base al nuovo quadro regolamentare europeo la Banca d'Italia e la Consob risultano designate come autorità competenti per la supervisione delle crypto-attività in Italia. La Banca d'Italia avrà competenze in materia di vigilanza prudenziale sugli emittenti di token di moneta elettronica (EMT) e token collegati ad attività (ART), nonché sui *prestatori di servizi in crypto-attività* (CASP). La Consob sarà invece competente per la trasparenza del mercato, la correttezza delle informazioni e la tutela degli investitori. Ad entrambe è assicurato il supporto tecnico della Agenzia per la cybersicurezza nazionale, che può risultare strategico proprio sul tema della decrittazione della *blockchain*, ove si considerino le sue specifiche competenze in materia di crittografia ³⁷.

Le autorità interessate ad un'azione sinergica potranno intervenire principalmente attraverso la regolamentazione e la super-

³⁵ È la comunicazione del 2022 in materia di tecnologie decentralizzate nella finanza e crypto-attività.

<https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-crypto.pdf>.

³⁶ Si veda in particolare la sezione informativa sugli investimenti in criptovaluta apposita: <https://www.consob.it/web/investor-education/criptovalute>.

Si veda anche il rapporto 2023 sui crypto asset <https://www.consob.it/documents/11973/1421036/rsc2023.pdf/56d24ca2-0437-98ad-bd7f-e0d4596f140c>.

³⁷ L'articolo 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, attribuisce infatti all'ACN la competenza per lo sviluppo e la diffusione di standard, linee guida e raccomandazioni al fine

di rafforzare la sicurezza e la protezione dei dati, anche attraverso la crittografia. L'ACN è responsabile per la promozione dell'uso della crittografia in ambito non classificato il che include la pubblicazione di linee guida, attività ed eventi mirati a questo scopo. Nella sua organizzazione L'ACN ha istituito un apposito Centro nazionale di crittografia, che agisce come centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato. Inoltre proprio l'ACN partecipa ai tavoli multilaterali sull'utilizzo della crittografia nei processi di certificazione internazionale e collabora con il Crypto Group del SOG-IS per definire un elenco di algoritmi crittografici raccomandati per la protezione di dati sensibili e partecipa alla revisione del Common Criteria Development Board per introdurre funzioni di sicurezza dedicate alla crittografia

visione degli operatori del mercato, imponendo perciò requisiti e controlli — anche interni — per garantire la trasparenza e la sicurezza delle operazioni. Le loro attività si concentrano sulla regolamentazione del mercato e sulla tutela degli investitori, evidenziando i rischi associati all'uso delle criptovalute e promuovendo una maggiore consapevolezza tra gli utenti. Il Regolamento MiCA (*Markets in Crypto-Assets*) dell'Unione Europea introduce un quadro normativo certo per le crypto-attività, mirato a garantire insieme la tutela dei consumatori e l'integrità del mercato finanziario.

Sebbene il MiCA non preveda strumenti specifici per contrastare direttamente il fenomeno del ransomware, esso stabilisce requisiti di trasparenza e obblighi per gli emittenti di crypto-attività e i fornitori di servizi correlati. Questi requisiti possono indirettamente contribuire almeno a mitigare l'uso illecito delle criptovalute, incluso il loro impiego in attacchi ransomware.

Inoltre, l'entrata in vigore del Regolamento DORA (Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario *Digital Operational Resilience Act*) rafforza tendenzialmente una più ampia di sicurezza informatica, focalizzandosi proprio sugli intermediari nel settore e minimizza, definendone i requisiti di sicurezza, i rischi tecnologici per gli enti finanziari nell'UE, inclusi appunto tutti i fornitori di servizi crypto autorizzati dal MiCA. Il DORA richiede già che tali entità implementino appositi piani di contingenza per incidenti informatici e sviluppino quadri di gestione del rischio delle tecnologie dell'informazione e della comunicazione (TIC), contribuendo così forse anche indirettamente a una maggiore resilienza effettiva contro minacce come il *ransomware*.

Un semplice richiamo ai “considerando” del regolamento appare di per sé utilissimo in tale direzione. Ci si riferisce in particolare ai “considerando” n. 51 e 52 del DORA che fanno appunto riferimento specifico agli attacchi informatici che “*tendono a perseguire guadagni finanziari direttamente alla fonte, esponendo quindi le entità finanziarie a conseguenze significative.*” E che appunto sottolineano l'opportunità di “*armonizzare la segnalazione degli incidenti connessi alle TIC mediante l'introduzione di un obbligo per tutte le entità finanziarie di segnalare direttamente alle rispettive autorità competenti*”. Con l'intento espresso di “*agevolare la tempestiva assistenza che può essere fornita alle entità finanziarie, se del caso. Gli Stati membri*

nelle certificazioni Common Criteria. Tale ruolo risulta fondamentale e realizza un impegno continuativo nello studio e nella promozione della crittografia anche tramite

collaborazioni con università ed enti di ricerca per lo studio di algoritmi di cifratura e delineando percorsi formativi in crittografia applicata alla cybersicurezza.

dovrebbero, inoltre, poter stabilire che le entità finanziarie stesse debbano fornire tali informazioni alle autorità pubbliche al di fuori del settore dei servizi finanziari” In tale prospettiva proprio i flussi di informazioni “*dovrebbero consentire alle entità finanziarie di beneficiare rapidamente di qualsiasi contributo tecnico pertinente, di consulenza sui rimedi e del successivo seguito dato da tali autorità. Le informazioni sugli incidenti gravi connessi alle TIC dovrebbero essere oggetto di comunicazione reciproca: le autorità di vigilanza finanziaria dovrebbero fornire all’entità finanziaria tutti i riscontri o gli orientamenti necessari, mentre le AEV dovrebbero condividere, in forma anonima, le analisi delle minacce informatiche e le vulnerabilità concernenti un determinato incidente, per promuovere una più ampia difesa collettiva*”. Infine (considerando 53) “*Tutte le entità finanziarie dovrebbero essere tenute a effettuare segnalazioni di incidenti, ma tale obbligo non dovrebbe interessarle tutte allo stesso modo. Infatti, si dovrebbe procedere a una debita calibrazione delle soglie di rilevanza pertinenti, nonché delle tempistiche delle segnalazioni, nel contesto degli atti delegati basati sulle norme tecniche di regolamentazione che le AEV devono elaborare, al fine di cogliere unicamente gli incidenti gravi connessi alle TIC. Inoltre, le specificità delle entità finanziarie dovrebbero essere prese in considerazione nello stabilire il calendario per gli obblighi di segnalazione*”.

L’adozione di standard di sicurezza informatica, come l’autenticazione a più fattori e l’architettura *zero-trust*, può sicuramente rappresentare una prima misura per prevenire che almeno siano compromessi e diffusi dati sensibili. Ciò insieme alla formazione continua, ed a più livelli, del personale di soggetti pubblici e privati sulla sicurezza informatica, risulta sempre più importante per proteggere le organizzazioni dagli attacchi ransomware. Ma a tali misure dovrebbe accompagnarsi anche l’utilizzo di opportune tecniche di *blockchain analysis*, che permette di tracciare sistematicamente le transazioni sospette e identificare attività illecite legate alle criptovalute analizzandone i flussi che peraltro sono trasparenti. Promuovere la consapevolezza sui rischi associati alle criptovalute e fornire linee guida su come proteggersi dagli attacchi ransomware è allora un elemento cruciale. La formazione degli utenti e delle organizzazioni sulle migliori pratiche di sicurezza informatica può concretamente produrre il risultato di una riduzione delle vulnerabilità agli attacchi, ma ciò a condizione che sia presente e si attui contestualmente un approccio integrato, che combini normative regolamentari ed autoregolamentari, efficace e completa cooperazione internazionale, avanzate misure di sicurezza informatica, monitoraggio delle transazioni e educazione degli utenti rappresenta la strategia più efficace per contrastare l’uso illecito delle criptovalute.

6. L'ESIGENZA DI UN APPROCCIO PIÙ INTEGRATO ED EFFICACE ALLE CONDOTTE ESTORSIVE E FRAUDOLENTE CYBER.

La nuova condotta estorsiva introdotta con l'art. 16 della legge 28 giugno 2024, n. 90 sembra allargare l'ambito del reato di estorsione³⁸ (art. 629 del codice penale) con la previsione di un nuovo comma 3 della norma, definendo così un reato non più caratterizzato da una condotta di violenza o minaccia rivolta direttamente alla persona — onde indurla in genere a versare un contributo patrimoniale alle organizzazioni criminali sul territorio — ma piuttosto operante in modo indeterminato attraverso, reati peraltro che la medesima normativa aggrava significativamente le condotte tipiche ricollegabili dei reati informatici tipici come l'accesso abusivo e il danneggiamento informatico. Già in tale condotta si sono poste significativamente numerose problematiche in relazione ai caratteri di tale attività intimidatoria³⁹, peraltro caratterizzante le associazioni di tipo mafioso ex art. 416 *bis* del codice penale. Tale condotta si concreterebbe infatti con un ricollegamento alle (preliminari) condotte antecedenti su dati o sistemi (*“mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies del codice penale”* ovvero nella minaccia di compierle) nel costringimento di *“a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno”*⁴⁰. Tale previsione, che in fondo configura una nuova forma di *“estorsione informatica”*, non si è però accompagnata ad interventi concreti sul terreno del più ampio possibile coordinamento investigativo, tanto più che tale genere di figure criminose si avvale di organizzazioni complesse di carattere transnazionale⁴¹. Ma non si può concepire forse una visione frammentata e limitata della criminalità informatica, ed occorre promuovere una stabile azione di contrasto e di coordinamento di tipo efficace, che non frammenti le singole informazioni e che sappia perciò utilizzarle in modo utile. La stessa organizzazione della Agenzia per la cybersicurezza nazionale⁴² dovrebbe sempre più adattarsi in tale direzione, in una

³⁸ Cfr. soprattutto FIORINELLI G., *Il “ransomware” nel DDL Cybersicurezza: dalla fattispecie di estorsione “informatica” al coordinamento tra indagini e “incident response”*, in *Rivista italiana di informatica e diritto*, 2024, p. 35.

³⁹ Cfr. VERCARA A., *L'estorsione online: “sextorsion” e l'estorsione a mezzo “ransomware”*, in *Rivista penale*, 2022, p. 657.

⁴⁰ La pena prevista è molto elevata (reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000 e reclusione da otto a ventidue anni e della multa

da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità ».

⁴¹ Cfr. BARBIROTTI P.I., *Le Dichiarazioni di Oxford sulle cyberoperazioni e il diritto internazionale: sviluppi recenti*, in *OIDU - Ordine Internazionale e Diritti Umani*, 2021, p. 1285.

⁴² Cfr. FORCIONE I., *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regola-*

prospettiva di leale (e tecnologica) collaborazione istituzionale tra più organismi diversi, tra autorità di settore ed agenzie aventi differenti funzioni e ruolo, in un quadro di virtuosa interazione pubblico/privato in vista di un obiettivo comune.

Il ruolo della Direzione nazionale antimafia ed antiterrorismo cui si richiamano espressamente le disposizioni della legge n. 90, dell'organismo cioè requirente competente sui reati di estorsione appunto in relazione al collegamento con il preminente reato di cui all'art. 416 *bis* del codice penale, risulta allora a dir poco significativo nella sua funzione generale di impulso e coordinamento rivolta agli uffici giudiziari, che però a sua volta talora è riferita a specifiche figure di reato rientranti molte volte nella competenza distrettuale, ma sicuramente esclusa nei casi di reati-spia come le frodi informatiche o altre figure di reato apparentemente minori che possono apparire invece prodromiche e che invece sono ancora disperse in diversi uffici giudiziari, sia sul piano degli assetti criminali associativi che sotto il profilo della diffusione di tecniche innovative sul piano della commissione di reati informatici.

Non si è avuto modo, tuttavia, di predisporre un quadro di interventi di più ampio respiro in modo da evitare tanto il rallentamento delle indagini proprio nel momento iniziale che è quello più delicato e fondamentale senza i quali poi lo stesso ruolo strategico della Direzione nazionale antimafia e antiterrorismo ne risulta perciò sensibilmente attenuato, in quanto proprio il quadro attuale di prassi e le stesse regole processuali determinative della competenza territoriale tende a favorire una ampia dispersione delle notizie di reato e degli elementi informativi che spesso possono essere concretamente sintomatici di un traffico illecito in criptovaluta che invece potrebbero essere determinanti. Manca inoltre, ancora, una adeguata struttura di analisi cooperativa, da intendere concentrata sulle forme evolutive della criminalità informatica sul piano tecnologico e sulle buone pratiche di indagine e di contrasto ad essa.

Tra queste in materia di criptovalute vanno considerate anche le ipotesi seriali di frode informatica ⁴³, che per lo più si giovano delle stesse approssimazioni in tema di sicurezza informatica che sono alla base del *ransomware*, e che vanno contrastate con la

zione europea e interna, in *Diritto amministrativo*, 2022, p. 1113.

⁴³ Tra le tipologie di frode più comuni nel settore crypto, gli schemi Ponzi rappresentano ancora la minaccia più insidiosa. Questi si caratterizzano per la promessa di rendimenti irrealistici e utilizzano una struttura piramidale mascherata da progetto blockchain innovativo. Casi celebri come OneCoin e BitConnect hanno causato per-

dite per miliardi di dollari, dimostrando come anche investitori apparentemente sofisticati possano cadere vittime di questi inganni quando si combinano marketing aggressivo e pressione sociale. Non meno pericolosi poi sono i cosiddetti "pump and dump", schemi di manipolazione del mercato in cui gruppi organizzati coordinano acquisti massicci di una determinata criptovaluta per gonfiarne artificialmente il prezzo,

medesima forza, anche nel rispetto di quanto poi prevede espressamente la Direttiva europea del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio cui l'Italia ha dato una attuazione limitata senza un preciso riferimento agli artt. 16 e 17 della Direttiva che appunto prevedeva la messa in campo anche di una serie coordinata di iniziative a favore delle vittime di reato.

È eloquente il richiamo al considerando n. 27 della Direttiva che risultava già chiarissimo in tale prospettiva definendo come “... *comunicare senza indebiti ritardi i reati alle autorità pubbliche è fondamentale nella lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, in quanto spesso è il punto di partenza di indagini giudiziarie. Occorre adottare misure per incoraggiare le persone fisiche e giuridiche, in particolare le istituzioni finanziarie, a comunicare i reati alle autorità di contrasto e alle autorità giudiziarie. Alla base di tali misure possono esservi diversi tipi di azione, tra cui atti legislativi contenenti l'obbligo di comunicare una sospetta frode, o azioni non legislative, come la creazione o il finanziamento di organizzazioni o meccanismi che favoriscono lo scambio di informazioni, oppure campagne di sensibilizzazione*”.

È chiaro anche come che una concezione integrale e integrata della sicurezza informatica, unita ad una più ampia idea del contrasto ai reati informatici (che non possono essere peraltro ridotti alla sola e sintetica idea della repressione dell'accesso abusivo ai sistemi informatici, nella sola c.d. “*lotta agli hackers*” che è alla base stessa poi della legge n. 90 del 2024) porterebbe un effetto straordinario con un autentico un approccio multi-livello alla sicurezza. Dal punto di vista pratico occorrono invece politiche di regolamentazione più dinamiche e soprattutto attente, che siano in grado di incentivare l'utilizzo esclusivo di *exchange* regolamentati, l'attivazione dell'autenticazione a due fattori (che è la base minima di sicurezza praticabile) e la conservazione dei fondi principali in *cold wallet*.

● Occorre invece puntare su una più efficace azione nazionale

per poi vendere improvvisamente causando il crollo del valore. Le vittime sono tipicamente piccoli investitori che, attirati dal rapido aumento dei prezzi, acquistano al picco perdendo significative somme di denaro. Le Initial Coin Offering (ICO) fraudolente rappresentano un'altra significativa frode. In questi casi, truffatori creano progetti apparentemente legittimi, completi di white paper plagiati e team fake, con l'unico scopo di raccogliere fondi e sparire. La mancanza di regolamentazione specifica e la fa-

cilità di creare token hanno reso questa forma di frode particolarmente diffusa. Il phishing e il furto di wallet digitali costituiscono una minaccia costante.

Attraverso email fraudolente, siti web clonati e malware sofisticati possono essere sottratte chiavi private dei wallet, ottenendo così accesso diretto ai fondi delle vittime. Il social engineering su piattaforme come Telegram e Discord è diventato uno strumento frequentemente utilizzato per raggirare gli utenti meno esperti.

congiunta di prevenzione e di assistenza immediata, sul modello di quanto realizzato da Europol ⁴⁴, che ha definito una linea assolutamente conforme che unisce assistenza on line ed immediata alle vittime e fruibilità di tools specifici oltre che di informazioni essenziali sulla difesa pubblica e privata. Il progetto di Europol rappresenta allo stato un fondamentale esempio di buona prassi operativa concepito on line ⁴⁵. Anche negli Stati Uniti ormai da tempo si assiste alla proliferazione di specifiche iniziative di informazione interattiva e di assistenza in materia ⁴⁶.

Peraltro negli Stati Uniti anche l'FBI ha adottato un approccio integrale ai temi del ransomware e delle frodi nelle criptovalute con programmi di informazione in rete ⁴⁷ e con un apposito *Internet Crime Complaint Center* ⁴⁸ avente funzioni di veicolazione e di analisi. Peraltro in materia di frodi informatiche va registrata l'identica politica comunicativa messa in atto, ormai da diversi anni, dalla *Federal Trade Commission* ⁴⁹. In Italia oltre al ruolo importante e di sensibilizzazione svolto già dalla Banca d'Italia in materia anche sul piano informativo ⁵⁰ e dalle Camere di Commercio attraverso Unioncamere ⁵¹ ma ancora mancano sul territorio stabili riferimenti specializzati e specifici strumenti operativi, anche sul piano regolamentare, adeguati di efficace contrasto alle attività criminali che si esplicano tramite criptovaluta.

Risulta in definitiva fondamentale sviluppare e rafforzare un approccio analogo in Italia, destinato ad operare in ambito nazionale ed aperto alle esigenze e alle esperienze europee e transnazionali (in vista poi dell'imminente Convenzione delle Nazioni Unite sul *cybercrime* ⁵²) e soprattutto concepito in modalità interattiva, come sembra fondamentale tenendo conto sempre delle

⁴⁴ <https://www.nomoreransom.org/it/index.html>.

⁴⁵ Si veda anche l'assistenza tecnologica unita alla analisi che avviene direttamente on line anche per verificare le richieste e il loro progredire <https://www.nomoreransom.org/crypto-sheriff.php?lang=it>.

⁴⁶ Si vedano le iniziative della FBI <https://www.fbi.gov/news/stories/ic3-virtual-complaint-desk-for-online-fraud#:~:text=The%20Internet%20Crime%20Complaint%20Center%2C%20or%20IC3%2C%20is,800%20complaints%20every%20day%20through%20its%20website%2C%20www.ic3.gov>. Che pubblicizzano anche tipici schemi di frode <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams>.

⁴⁷ <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware>.

⁴⁸ <https://www.ic3.gov/Home/Index>.

⁴⁹ <https://reportfraud.ftc.gov/>.

⁵⁰ Le iniziative di Banca d'Italia sono state molteplici: <https://www.bancaditalia.it/media/approfondimenti/2022/cryptol/Comunicazioni-della-Banca-d-Italia-DLT-crypto.pdf>.

E soprattutto:

<https://www.bancaditalia.it/focus/cybersicurezza/truffe-cyber/avvisi-tentativi-truffa/index.html?dotcache=refresh>.

<https://www.bancaditalia.it/focus/cybersicurezza/truffe-cyber/>.

https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/comunicazione_vv_2019.pdf.

⁵¹ <https://www.unioncamere.gov.it/newsletter-mosaico-europa/un-toolkit-tutelarsi-dai-furti-informatici>.

⁵² <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

buone prassi europee⁵³. Ma il cammino in questo senso da percorrere, anche se appare già tracciato, appare ancora impervio e lungo ed ogni difficoltà organizzativa può essere superata tenendo conto dell'importanza degli interessi coinvolti nel quadro globale.

Abstract

Negli ultimi anni, il crimine informatico ha registrato un incremento significativo, con le criptovalute che svolgono un ruolo cruciale. Gli attacchi ransomware colpiscono privati, aziende e enti pubblici, provocando la perdita di dati sensibili. Per contrastare efficacemente il ransomware, è necessario adottare un approccio pragmatico basato su una continua specializzazione e una gestione condivisa delle informazioni. In questo contesto, la normativa italiana richiede la segnalazione delle operazioni sospette in valuta digitale. A livello europeo, il Regolamento MiCA e il Regolamento DORA mirano a garantire la sicurezza delle operazioni con criptovalute e la resilienza contro minacce come il ransomware e la nuova condotta di estorsione informatica introdotta con l'art. 16 della legge 28 giugno 2024, n. 90, richiede un effettivo ed efficace coordinamento investigativo ed operativo.

Cybercrime has seen a significant increase in recent years, with cryptocurrencies playing a crucial role. Ransomware attacks affect individuals, businesses, and government agencies, resulting in the loss of sensitive data. To effectively combat ransomware, a pragmatic approach based on continuous specialization and shared information management must be adopted. In this context, Italian legislation requires suspicious transactions in digital currency to be reported. At the European level, the MiCA Regulation and the DORA Regulation aim to ensure the security of cryptocurrency transactions and resilience against threats such as ransomware and the new cyber extortion conduct introduced with art. 16 of Law No. 90 of 28 June 2024, requires effective and effective investigative and operational coordination.

Parole chiave

Ransomware - tutela dati personali - Regolamento MICA - Regolamento DORA - sicurezza informatica - estorsione informatica.

⁵³ Cfr. MATTARELLA A., *Il "cybercrime" nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Na-*

zioni Unite, in *Diritto penale e processo*, 2022, p. 309.