European Conference of Prosecutors
Conférence européenne des procureurs
Conferenza europea dei procuratori

NUOVE SFIDE DAL CIBERSPAZIO – L'INDIVIDUAZIONE DEI RESPONSABILI

Nunzia Ciardi
Vice Direttore dell'Agenzia italiana per la Cybersicurezza Nazionale

Tema III – I reati finanziari nell'ambiente virtuale – un programma per la reciproca assistenza giudiziaria

Palermo, 5-6.05.2022

PROCURA GENERALE
della Corte di cassazione

Presidency of Italy
Council of Europe
November 2021 - May 2022

Présidence de l'Italie
Conseil de l'Europe
Novembre 2021 - Mai 2022

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EUROPEAN CONFERENCE OF PROSECUTORS

PALERMO, 5-6TH MAY 2022

THEME III – FINANCIAL CRIMES IN THE VIRTUAL ENVIRONMENT – CHALLENGES FOR MUTUAL LEGAL ASSISTANCE

6th May 2022

New challenges from the cyberspace – the quest for attribution

V01_29042022

Innanzitutto, permettetemi di ringraziare gli organizzatori di questa prestigiosa Conferenza per l'invito a prendervi parte. È per me sempre un gran piacere partecipare a dibattiti stimolanti e costruttivi, soprattutto su un tema che vede nella collaborazione e nello scambio tra istituzioni diverse e Paesi diversi la chiave di volta per la risoluzione di molti importanti problemi.

Lo sviluppo e la crescente pervasività di Internet e di nuove o emergenti tecnologie dell'informazione e della comunicazione hanno trasformato e continuano a trasformare profondamente la società contemporanea. Una significativa accelerazione sta caratterizzando la digitalizzazione di processi e contenuti, favorendo l'interconnessione tra gli individui e l'ambiente in cui questi vivono nonché ampliando significativamente i confini del cd. cyberspazio, nel cui ambito si svolgono, oramai, attività essenziali per il regolare svolgimento della vita individuale e collettiva.

Se, da un lato, il progresso tecnologico e lo sviluppo del cyberspazio contribuiscono a generare notevoli opportunità e benefici in termini di crescita economica, sociale, politica e culturale della collettività, dall'altro la espongono a nuove vulnerabilità, rischi e minacce, sempre più diffusi, diversificati e sofisticati. Condizione imprescindibile per far fronte a tali minacce è la disponibilità di opportuni strumenti – normativi, di policy e tecnologici – e capacità – istituzioni, risorse e competenze – da impiegare tanto a scopo preventivo quanto di risposta.

Tra le minacce cyber figurano quelle perpetrate da attori di natura non-statuale (individui o organizzazioni), per il perseguimento di finalità criminali. È il cd. fenomeno del cybercrime che, in termini generali, può essere definito come l'impiego di nuove o emergenti tecnologie e tecniche, associate al dominio cyber, per finalità delittuose. Si tratta di un fenomeno non nuovo e ben conosciuto, che consiste in una variegata serie di attività criminose che spaziano dalle frodi informatiche, all'accesso abusivo ad un sistema informatico, al drammatico fenomeno della pedopornografia on line, al terrorismo, al furto d'identità, fino all'organizzazione del gioco d'azzardo, di scommesse clandestine e di mercati illegali *on-line*.

Naturalmente, queste tipologie di attività criminali cyber non esauriscono la categoria del cybercrime, che è e un fenomeno articolato e in continua, rapida, evoluzione ed espansione, soprattutto per le capacità di attori criminali nuovi o tradizionali, più o meno organizzati, di operare in un "ambiente" in costante trasformazione, nonché di sfruttare abilmente le opportunità offerte dal processo di innovazione tecnologica. **Da questo punto di vista, il cybercrime continuerà ad evolvere e a trasformarsi di pari passo con il progresso tecnologico.** E l'espansione del fenomeno sarà tanto maggiore, continua e rapida quanto più il compimento di questi tipi di crimini si dimostrerà attrattivo per i singoli o i gruppi criminali, ovvero sarà "conveniente" in termini di rapporto costi-benefici. Da intendersi però non solo ed esclusivamente da un punto di vista economico.

Infatti, quello economico, sebbene sia il principale, non è l'unico incentivo a rendere il crimine informatico, in particolare, alcune sue fattispecie, attrattivo per gli individui o le organizzazioni che compiono queste attività. Alla possibilità di realizzare significativi proventi, bisogna aggiungere il percepito o, in molti casi, reale minor rischio che la condotta criminosa sia scoperta dalle autorità di *law enforcement* e che il responsabile venga incriminato.

Tale minor rischio è innanzitutto dovuto a diverse caratteristiche (tecniche e di funzionamento) proprie dell'ambiente cyber e delle tecnologie ad esso connesse, in particolare alla possibilità da queste garantite di assicurare, previa adozione di opportune soluzioni, l'anonimato degli utenti della rete. Come ben evidenziato nel rapporto pubblicato nel 2019 da Europol e Eurojust, relativo alle sfide al contrasto al cybercrime, la condizione di anonimato, garantito attraverso il ricorso a soluzioni crittografiche, determina la cd. "loss of location", che comporta la difficoltà di stabilire il "chi", il "come" e il "dove" di un'azione cyber criminale.

All'ostacolo rappresentato dall'anonimato si deve poi aggiungere la relativa inidoneità degli strumenti normativi, che dettano discipline preventive, a "tenere il passo" rispetto alle opportunità offerte dal progresso tecnologico ai criminali informatici. Si devono poi considerare i limiti degli strumenti operativi e delle procedure a cui possono ricorrere le autorità di *law enforcement* per l'esercizio di efficaci attività di indagine e di repressione.

A quest'ultimo riguardo, oltre alla difficoltà di reperire, formare e aggiornare competenze tecniche e specialistiche - tema di assoluta centralità - sussistono intrinseche difficoltà di svolgere efficacemente le attività di indagine e di contrasto, le quali, spesso, per la natura stessa del crimine in oggetto, assumono una connotazione transnazionale e presuppongono la collaborazione bi- o multilaterale transfrontaliera, non sempre agevole da attuare concretamente. È evidente infatti che, quasi sempre, il raggio operativo del crimine informatico non si limita ad un solo Stato e a pochi individui sottoposti alla sua giurisdizione, ma può estendersi fino a ricomprendere molteplici giurisdizioni nazionali. **La rete ha sbriciolato ogni confine spazio-temporale**. Ordinariamente, è all'estero che si consuma, almeno parzialmente, la condotta criminosa e, tanto le tracce informatiche (sovente abilmente manipolate attraverso i più vari strumenti di anonimizzazione), quanto le tracce finanziarie (conti correnti e strumenti finanziari, sistemi di pagamento elettronico, corrieri di denaro, criptovalute ecc.), frequentemente, riconducono fuori dal territorio nazionale. E dunque è naturale che l'attività investigativa soffra limitazioni e ostacoli originati dalla mancanza di uniformità delle legislazioni nazionali, che gli accordi internazionali in materia finora sembrano non riuscire a superare. Infatti, quello della criminalità cibernetica non è ancora un concetto giuridico definito, né compiutamente né in modo condiviso, comparendo - in relazione a specifici profili- in fonti sovranazionali ed europee.

Dunque, come dicevamo, **alta redditività e basso rischio** sono i principali elementi che sostengono l'espansione del crimine informatico; sono quelli che lo rendono fortemente attrattivo anche per il crimine organizzato "tradizionale", il quale, a tendere, potrebbe connotarsi sempre più come "cyber-mafia" o, comunque, servirsi di o generare sodalizi con esperti criminali informatici.

Infatti, così come hanno dimostrato di saper approfittare delle opportunità di arricchimento offerte dalla globalizzazione, le organizzazioni criminali di tipo mafioso sembrano interessate ed intenzionate ad acquisire, direttamente o indirettamente, le capacità tecniche e le competenze che consentono loro di condurre attività criminose nell'ambiente cyber o per il suo tramite. L'acquisizione indiretta di capacità e competenze avviene attraverso il ricorso a professionisti singoli o ad altre organizzazioni criminali, che hanno sviluppato elevati gradi di specializzazione ed offrono *know-how*, *tool* e servizi sempre più complessi e raffinati, "pronti all'uso", secondo un modello che viene definito "crime-as-a-service". Da questo punto di vista, **le competenze informatiche** diventano sempre più uno **degli asset appetibili per le holding criminali.**

Anche se spesso sembra che le grandi mafie transnazionali non abbiano ancora investito in maniera massiccia, strutturata e uniforme nel crimine informatico, secondo diversi osservatori, negli ultimi anni, soprattutto in concomitanza con la pandemia, si è riscontrata una certa contiguità tra organizzazioni criminali "tradizionali" e realtà cybercriminali. Si starebbero cioè definendo le condizioni affinché il rapporto tra i due mondi criminali diventi maggiormente consolidato.

Un ambito nel quale tale sodalizio è più evidente o potrebbe presto addirittura configurarsi come inquadramento organico è quello del cd. cybercrime finanziario. Questa tipologia di reati, infatti, pone il vantaggio per la criminalità di fornire un immediato riscontro economico alle attività delittuose. Grazie all'utilizzo di criptovalute, il brokeraggio, le frodi e le transazioni finanziarie occulte potrebbero diventare una significativa area di business per il crimine organizzato. Ma non solo. In realtà, vi sono diverse evidenze investigative che dimostrano come alcune mafie già da tempo utilizzano le monete virtuali per il pagamento di partite di stupefacenti. Come recentemente affermato dalla Direzione Investigativa Antimafia italiana ormai sono anni che alcune organizzazioni criminali utilizzano questo agile strumento per trasferire in Sudamerica le somme di denaro con cui pagare narcotrafficanti e produttori di droga colombiani.

A prescindere dalla specifica condotta illecita, **le transazioni di criptovaluta** legate all'attività criminale hanno raggiunto un nuovo record nel 2021 e **sono quasi raddoppiate** rispetto all'anno precedente, anche se la loro quota si sta riducendo in un mercato in forte espansione. Secondo uno studio della società Chainalysis sull'utilizzo della moneta virtuale, nel 2021 sono transitati attraverso conti legati ad attività illegali l'equivalente di 14 miliardi di dollari, una cifra quasi doppia rispetto ai 7,8 miliardi nel 2020. Secondo lo stesso studio, le transazioni illegali rappresentano però solo lo 0,15% dell'utilizzo totale delle criptovalute che lo scorso anno hanno movimentato transazioni per 15,8 trilioni.

Tuttavia, qualora si compisse quella saldatura definitiva tra crimine informatico e organizzazioni mafiose, che dispongono di gigantesche risorse di capitali, la percentuale delle transazioni illegali sul totale dell'utilizzo delle valute virtuali sarebbe destinato a crescere, così come il suo impatto sull'economia legale e sulla società nel suo complesso.

Guardando, appunto, ai profili appena delineati dal punto di vista delle autorità di *law enforcement*, tanto l'anonimato garantito dalla rete e da nuove soluzioni tecnologiche, quanto la

transnazionalità del crimine informatico, rappresentano gli elementi che rendono difficoltosa la cd. *attribution,* tecnica e/o operativa, di un'azione criminale condotta tramite, nel o a danno del cyberspazio. Ostacolano, in ultima analisi, il processo che permette di individuare l'esecutore o il responsabile di un'azione criminale.

In quanto processo, l'attribuzione può essere definita come una serie di operazioni fattuali (*e.g.* raccolta di informazioni) o di ragionamento svolte in modo strutturato e logico al fine di ascrivere o imputare, con il fatto e con giudizio, un'azione malevola cyber ad un'agente. Più semplicemente, l'attribuzione è quel procedimento attraverso il quale si cerca di rispondere a due fondamentali domande: "Chi è stato (agente o esecutore materiale) a compiere una determinata azione?"; "Chi è il responsabile (soggetto suscettibile di giudizio) di quell'azione?". Domande le cui risposte vengono formulate sulla base di differenti, seppur strettamente interrelati, piani d'indagine.

La determinazione del "che cosa", del "come", del "dove" e del "chi" è dunque ostacolata dall'utilizzo da parte dei soggetti criminali di soluzioni di crittografia o altri simili espedienti, che garantiscono loro l'anonimato o "l'invisibilità", ovvero è ostacolata dalla transnazionalità della condotta criminosa che rende difficoltosa la definizione della competenza e della giurisdizione e limita le indagini, in particolare, la raccolta dell'*evidence.*

Ancora una volta, non può non rilevarsi come la "de-territorializzazione" dei fenomeni di cyber-crime si scontri con una giurisdizione tradizionalmente legata al territorio. Da questo punto di vista, un risultato normativo di segno chiaramente positivo si è conseguito con l'istituzione della Procura europea (EPPO [1]). L'intuizione della costruzione quale ufficio unico a struttura decentralizzata, e la previsione di poteri esecutivi diretti, mirano ad attuare una concreta cooperazione rafforzata che, nei reati economici-finanziari che la Procura europea persegue, rende superate una serie di strumenti tradizionali. La procura europea sembra, pertanto, poter essere una intelligente e fruttuosa risposta all'esigenza di superamento dei confini territoriali, almeno nell'ambito dell'Unione.

Pensiamo a esempio al *cyberlaundering* che rappresenta una manifestazione parziale dell'ampio fenomeno del cybercrime. Come osservato dalla dottrina penalistica, il *cyberlaundering* appartiene alla categoria dei reati informatici in senso lato, ovvero alle condotte criminose, nella specie il riciclaggio, compiute avvalendosi di uno strumento informatico come mezzo e non come oggetto materiale del reato.

---

[1] La Procura europea (EPPO), istituita dal Regolamento (UE) 2017/1939, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea, è un organismo indipendente dell'Unione europea che indaga, persegue e porta in giudizio i reati che ledono gli interessi finanziari dell'UE (quali frodi, corruzione, riciclaggio, frodi IVA transfrontaliere). L'EPPO è diventata operativa il 1° giugno 2021 e vede l'adesione di 22 Stati membri rispetto ai quali ha poteri diretti. L'EPPO ha una struttura a due livelli. Un livello centrale con sede a Lussemburgo e costituito da un procuratore capo europeo e un collegio dei procuratori che definiscono gli obiettivi strategici dell'organo. Un livello nazionale costituito dai procuratori europei delegati e dalle camere permanenti. I procuratori europei delegati nei 22 paesi dell'UE partecipanti sono responsabili dello svolgimento di indagini penali e dell'azione penale e operano in piena indipendenza dalle rispettive autorità nazionali, mentre le camere permanenti monitorano e indirizzano le indagini e adottano decisioni operative.

Se le prime manifestazioni criminose rivolte allo sfruttamento delle nuove tecnologie a fini di riciclaggio risalgono a diversi anni orsono, è stato solo con l'avvento delle valute virtuali che il fenomeno ha avuto una crescita esponenziale, in quanto le operazioni con tali strumenti permettono il consolidamento dei proventi delittuosi, **senza alcun previo passaggio per la dimensione reale dell'economia.** È possibile dunque affermare che il *cyberlaundering* compiuto servendosi delle valute virtuali rappresenta oggi la nuova frontiera del riciclaggio. Secondo il già citato studio di Chainalysis, nel 2021, attraverso il ricorso alle valute virtuali, si stima che sia stato riciclato l'equivalente di 8.6 miliardi di dollari, il 30% in più rispetto alle somme di danaro che sarebbero state riciclate, sempre tramite criptovalute, nel 2020. In totale, a partire dal 2017, si stima che sia di 33 miliardi di dollari il valore delle somme riciclate.

Ma cosa sono esattamente le valute virtuali o le criptovalute? In termini generali, si tratta di valute che non esistono in forma fisica (anche per questo viene definita "virtuale"), ma che si generano e si scambiano esclusivamente per via telematica. Tra le principali criptovalute utilizzate dagli utenti di Internet figurano Bitcoin, Ripple, Ethereum, Solana, per citarne alcune. Le criptovalute hanno caratteristiche peculiari; il loro funzionamento si basa su: (i) un insieme di regole (detto "protocollo"), iscritte in un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni; (ii) una sorta di "libro mastro" (*distributed ledger* o *blockchain*), che conserva immodificabilmente la storia della transazioni; (iii) una rete decentralizzata di partecipanti che aggiornano, conservano e consultano la *blockchain* delle transazioni, secondo le regole del protocollo. Una volta emesse, le valute virtuali possono essere acquistate o vendute su una piattaforma di scambio (cd. *exchange platform*), utilizzando denaro a corso legale (per esempio, EUR, USD, ecc.). Le piattaforme di scambio su cui si acquistano e vendono valute digitali non sono attualmente regolamentate.

A rendere particolarmente attraente la valuta virtuale agli occhi degli investitori è la perfetta fusione dei vantaggi della moneta reale e di quelli della moneta elettronica in essa riscontrabile. Come la moneta fisica, quella virtuale è accessibile a chiunque, ha carattere anonimo ed è agevolmente trasferibile; come la moneta elettronica, consente di effettuare agevolmente pagamenti a distanza e garantisce transazioni rapide e a basso costo. Le transazioni in valuta virtuale sono un formidabile veicolo di business, poiché consentono agli operatori economici di entrare in contatto con le più svariate realtà internazionali e di interagire con le stesse a costi ridotti e con possibilità di perfezionare in modo istantaneo trasferimenti di ingenti somme di denaro. Di recente, la preoccupazione sulla forza attrattiva del mercato delle criptovalute è particolarmente sentita anche a seguito del conflitto Russia-Ucraina, per il timore che si possano utilizzare le criptovalute per aggirare le severe sanzioni economiche adottate contro la Russia.

Per le ragioni appena esposte, le valute virtuali hanno attirato su di loro l'attenzione dei criminali informatici e delle cyber-mafie. In particolare, l'anonimato o lo pseudo-anonimato garantito agli utenti di valute virtuali è il principale elemento che induce la criminalità a sfruttare la piazza finanziaria digitale **per polverizzare le ingenti liquidità di origine illecita**. Infatti, le infrastrutture basate sulla tecnologia *blockchain*, sebbene permettano a chiunque di visionare le transazioni effettuate dagli altri nodi della rete, verificandone l'importo e individuando gli indirizzi dell'ordinante e del beneficiario, non consentono, tuttavia, di risalire all'identità dei singoli utenti. Sul pubblico registro le transazioni sono infatti catalogate in stringhe numeriche esadecimali corrispondenti agli indirizzi di invio/recezione della valuta (*transaction address*). Peraltro, gran parte dei protocolli di gestione delle transazioni consente agli utenti di formare identificativi differenti per ogni singola transazione, rendendo difficoltosa, se non impossibile, l'identificazione dei titolari degli accounts coinvolti.

La criptomoneta, dunque, consente di inviare e ricevere denaro con garanzie di anonimità come nessun altro sistema al mondo. Non si può non notare che anche gli Stati storicamente più legati al segreto bancario ammettono oggi ampie deroghe e riserve in forza degli accordi internazionali di mutua collaborazione in materia penale e/o tributaria. Del resto, anche se il riciclaggio del denaro si realizzasse in Paesi che garantiscono appieno il segreto bancario o in Stati che non prevedono presidi antiriciclaggio, i criminali dovrebbero comunque trovare un espediente per rientrare in possesso dei capitali ripuliti senza compiere operazioni sospette. L'utilizzo del circolante virtuale risolve a monte il problema, poiché, quale che sia lo Stato di residenza del destinatario finale delle somme, non esistono segnali "spia" o indicatori della illiceità della transazione.

Inoltre, la rapidità degli scambi di moneta virtuale rappresenta un serio ostacolo all'identificazione della provenienza delittuosa del denaro, mentre l'accettazione su larga scala della valuta assicura l'*integrazione* del profitto attraverso semplici operazioni di acquisto di beni o servizi o scambio in altri valori virtuali. **A differenza dell'infrastruttura bancaria tradizionale, un ecosistema decentralizzato riduce drasticamente i tempi di transazione e permette uno scambio *peer to peer*, senza passare per soggetti terzi gravati dagli obblighi antiriciclaggio.**

In breve, la ripulitura del denaro online attraverso le criptovalute presenta per i criminali numerosi vantaggi, tra cui: la possibilità di agire in qualsiasi momento e in modo anonimo, senza che sia necessario interfacciarsi *de visu* con persone fisiche; l'opportunità di assoldare direttamente sul web terzi fiduciari per il compimento delle operazioni intermedie (*money mules*); le difficoltà nell'individuazione del *locus commissi delicti* e dell'identità dei soggetti coinvolti nella filiera del riciclaggio. Poiché la maggior parte delle valute virtuali sono accettate come mezzo di pagamento da un crescente numero di operatori economici, il rientro nel circuito dell'economia lecita potrà realizzarsi anche senza la previa conversione in moneta avente corso legale, semplicemente acquistando beni o servizi. L'utilizzo delle valute virtuali massimizza i vantaggi, rendendo assai più agevole la movimentazione dei capitali.

Quanto descritto può dare il senso delle difficoltà che le autorità di *law enforncement* incontrano nel realizzare efficaci attività di prevenzione e contrasto ed evidenzia l'esasperazione delle principali sfide e dei limiti relativi alla lotta al cybercrime già accennati.

L'espansione del fenomeno dei cryptoasset sembra porre una sfida significativa alle autorità regolatorie, e cioè quella di governare l'innovazione operando un bilanciamento tra le esigenze stringenti di tutela e l'accesso a servizi adeguati. In questo senso, segnali decisamente positivi si possono rilevare nell'attività dell'Unione europea che sta acquisendo una vera e propria leadership, avendo optato per lo strumento legislativo del Regolamento, con l'obiettivo, appunto, di creare un quadro normativo di riferimento immediatamente applicabile in tutto il mercato unico. Ci si riferisce alla c.d. proposta MiCAR[2] (presentata dalla Commissione europea in data 24 settembre 2020e attualmente in fase attiva di trilogo[3]), con cui vengono definite una serie di

[2] COM/2020/593 final. Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 ("Regolamento MiCA" o "MiCAR").

[3] Negoziazione tra Commissione, Consiglio e Parlamento.

regole applicabili alle offerte di cripto-attività non assimilabili a strumenti finanziari, depositi o depositi strutturati ai sensi della legislazione dell'UE in materia di servizi finanziari.

Altro fenomeno indicativo è l'estorsione condotta attraverso l'impiego di *ransomware* che rappresenta una tipologia di crimine informatico dilagante, insidioso e in progressiva evoluzione, che interessa non solo le infrastrutture informatiche di interi comparti economici/industriali, ma anche, in modo diffuso, quelle in uso a utenti individuali.

Stando a quanto evidenziato dai principali report sulla cybersecurity riferiti all'anno 2021[4], **il 35% delle intrusioni in sistemi informatici** integra il ricorso a ransomware. Si tratta di una tipologia di attacchi che, rispetto al 2020, mostra **una crescita** nell'ordine del **105%-107%.** In termini numerici non percentuali, la minaccia ransomware è complessivamente consistita in circa 623,3 milioni di azioni malevole, con significative conseguenze, non solo economiche, ma anche sociali, nella misura in cui ha determinato l'interruzione dell'erogazione di un servizio pubblico essenziale. Il riscatto medio pagato per recuperare i dati, che si attesta sui 812.360 dollari, è quintuplicato rispetto allo scorso anno e il 46% delle aziende i cui dati sono stati criptati a seguito dell'attacco ha deciso di pagare il riscatto. Nel nostro Paese il 55% delle aziende colpite ha dichiarato che l'impatto sulla propria operatività di business è stato molto alto e che il tempo di recupero dei dati è stato di "fino a una settimana" per il 36%, "fino a un mese" per il 34%, mentre solo l'11% del campione ha ripristinato la normalità in "meno di un giorno".

Ma che cosa è più esattamente il ransomware? Si fa, in particolare, riferimento ad una specifica tipologia di attività criminosa, recentemente salita agli onori della cronaca e che, oltre a profili strettamente penalistici, può sollevare questioni riguardanti anche la salvaguardia della sicurezza nazionale dello Stato. Si tratta dell'impiego dei cd. *ransomware*, ovvero di software malevoli **che cifrano i dati e li rendono indisponibili al loro legittimo titolare,** - soggetto o organizzazione che sia. Per il "rilascio" di questi dati viene richiesto il pagamento di un riscatto in moneta virtuale. È una minaccia sempre più diffusa e che interessa un'ampia gamma di organizzazioni, private e pubbliche. I profili di sicurezza nazionale connessi alla minaccia emergono quando il *ransomware* colpisce e compromette sistemi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato.

La condotta consumata attraverso il ransomware è caratterizzata da due fasi: la prima, a scopo preparatorio, consistente in un'intrusione informatica seguita da una esfiltrazione dei dati; la seconda, integrante la minaccia telematica con richiesta di pagamento di riscatto. **L'esfiltrazione diviene strumentale al compimento dell'estorsione che, spesso, si configura come "doppia" o "tripla**". I criminali, infatti, possono richiedere alla vittima il pagamento di una somma in criptovaluta per: (i) ottenere la chiave di decodifica dei dati, sbloccarne l'accesso e ripristinare il funzionamento del sistema (estorsione singola); (ii) scongiurare la pubblicazione di dati sensibili che potrebbe generare un danno d'immagine o di altro tipo; (iii) infine, evitare di subire un attacco DDoS (Distributed Denial of Service) contro eventuali servizi erogati dalla vittima.

L'organizzazione e il compimento di un'azione estorsiva che impiega il *ransomware* si può basare su strutture tanto centralizzate quando completamente decentralizzate. La parcellizzazione e decentralizzazione delle competenze e, soprattutto, delle azioni di cui sopra, spesso si associano alla distribuzione geografica, in diversi Paesi, dei loro esecutori e di chi ne è vittima.

---

[4] "*Navigating New Frontiers"* - Trend Micro 2021 Annual Cybersecurity Report, Marzo 2022; *Microsoft Digital Defence Report*, Ottobre 2021.

Al riguardo si deve, però, rilevare che non sembrano esistere precedenti giurisprudenziali che condannino la vittima di un *ransomware* che abbia pagato il riscatto richiesto. Infatti, il reato di favoreggiamento sembrerebbe non potersi applicare in caso di persona fisica/privato, dal momento che, subendo la condotta, quest'ultimo verrebbe a configurarsi come mera vittima, soggetto passivo della commissione del reato, anche qualora decidesse di pagare il riscatto.

In alcuni Paesi è stato affrontato il tema di rendere illegale il pagamento del riscatto ma alla fine si è ritenuto che i problemi che sarebbero potuti derivare da una previsione del genere avrebbero superato gli eventuali vantaggi.

A diversa conclusione, invece, si potrebbe addivenire nel caso di pagamento del riscatto attraverso i soggetti terzi che si propongono alla vittima quali intermediari. In tal caso, potrebbe invero ben ipotizzarsi il reato di favoreggiamento, eventualmente introducendo, anche a chiari fini di manifestarne la contrarietà all'ordinamento giuridico, una specifica fattispecie di reato di favoreggiamento informatico.

Delineata brevemente la complessità del quadro - sia pure riferito a un numero ridotto di esempi-ci si chiede quali potrebbero essere le strade percorribili.

In linea di principio, occorrerebbe innanzitutto intervenire con riguardo all'utilizzo di soluzioni crittografiche che garantiscono l'anonimato e ostacolano l'*attribution*. Si tratta di una questione assai dibattuta, molto delicata e "spinosa", in quanto la crittografia o le altre soluzioni che assicurano l'anonimato in rete (ad es. VPN, Tor) rappresentano, in determinate realtà, uno degli strumenti che tutelano gli individui/utenti dall'azione repressiva esercitata da regimi non democratici. Si pensi a regimi che tendono ad opprimere la libertà fondamentali degli individui di informazione ed espressione, anche *on-line*.

E anche se, come abbiamo detto, la crittografia può diventare un fattore abilitante per la commissione di crimini informatici non sembra praticabile– politicamente, giuridicamente, **ma neppure tecnicamente aggiungerei**– la via di limitare o vietare *tout court* l'utilizzo di soluzioni di crittografia, ovvero di indebolirne l'efficacia. Occorre necessariamente agire su altri piani.

La transnazionalità del cybercrime, risultante spesso dalla "parcellizzazione" funzionale e geografica delle azioni che integrano l'attività criminosa, **dovrebbe forse spingerci a una importante - quanto delicata - riflessione comune su alcuni aspetti della rete e delle società digitalizzate.** Una riflessione più allargata possibile. Che parta dagli elementi meno complessi e divisivi come l'importanza di norme applicabili a più giurisdizioni possibili (auspicabilmente di portata globale), in modo tale da evitare conflitti tra autorità di *law enforcement*, che possono ostacolare, ad esempio, la raccolta e circolazione del materiale probatorio. I fattori fondamentali per il successo di un'indagine sul cybercrime a dimensione internazionale sono infatti quello della velocità degli atti investigativi e della raccolta dei dati e di altra *evidence*. Dati la cui mancanza limita o impedisce la possibilità di eseguire correttamente *l'attribution*.

Nella consapevolezza di tali presupposti, la Convenzione di Budapest si ispira al massimo favore per la cooperazione internazionale. In questo senso, è di fondamentale importanza disporre di norme e procedure che favoriscano e sostengano l'efficace coordinamento e la cooperazione internazionale tra le autorità di *law enforcement*, limitando all'indispensabile le formalità burocratiche. Da un punto di vista pratico, il contrasto al crimine informatico è tanto più efficace quanto più è prevista ed incentivata la possibilità di collaborazione transfrontaliera, da attuarsi anche attraverso la costituzione di *joint investigation teams*, e quanto maggiore è la propensione

degli investigatori e degli inquirenti alla comunicazione e allo scambio informativo, alla rapida raccolta, conservazione e scambio dell'*evidence*, alla condivisione di esperienze, strumenti e professionalità tecniche. Propensione che va stimolata e coltivata costantemente, anche attraverso idonei programmi di formazione per gli operatori, **fino al punto in cui possa divenire una vera e propria mentalità o cultura professionale.** Come diversi casi della prassi dimostrano, l'efficace cooperazione internazionale diviene la chiave di volta per assicurare alla giustizia i responsabili della condotta criminale.

www.coe.int/ccpe

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE