PANDEMIA E CYBER CRIMINE

Il 2020 è stato, lo sappiamo, un anno nefasto per il mondo intero. La pandemia di Covid-19 ha imposto un radicale stravolgimento delle nostre abitudini quotidiane, ha alterato il nostro modo di concepire i rapporti interpersonali, di rapportarci al lavoro, allo studio, all'informazione.

Proprio con riferimento all'accesso alle informazioni - ma sarebbe meglio parlare di accesso ai mezzi di informazione -, abbiamo assistito ad un vorticoso susseguirsi di notizie "sulla pandemia", spesso del tutto contrastanti, a volte chiaramente tendenziose e altre volte prive di ogni accurato vaglio che ne legittimi la diffusione.

È facile paragonare questo inarrestabile turbinio informativo ad una tromba d'aria che lascia dietro di sé una distesa di macerie e spaesamento, l'incapacità di saper discernere il verosimile dall'inattendibile, l'autorevole dal mero chiacchiericcio.

Sulla passerella delle parole di tendenza qualcuno ha pensato bene di descrivere il fenomeno riesumando il termine "infodemia", coniato dal giornalista David J. Rothkopf (Washington Post) nel 2003 per descrivere quelle notizie false o, quantomeno ambigue, che continuavano a susseguirsi con riferimento all'epidemia SARS.

Comunque la si chiami, la circolazione di questa quantità eccessiva e caotica di notizie porta il lettore, tanto quello passivo quanto quello più critico, ad un senso di incertezza, costringendolo ad una bulimica ricerca di conferme e smentite tramite l'utilizzo dei nuovi mezzi di diffusione informatica. Ciò comporta l'inevitabile allargamento della platea di utenti della rete anche a soggetti normalmente poco adusi alle nuove tecnologie; soggetti che, nei casi di maggiore vulnerabilità, divengono facili prede di possibili attacchi informatici che, nell'ultimo anno, hanno visto incrementata esponenzialmente la loro frequenza. Se, infatti, *internet* costituisce il mezzo grazie al quale si sono potute rimodulare gran parte delle nostre occupazioni (si pensi allo *smart working* o alla didattica a distanza), è vero anche che nel 2020 si è assistito ad un aumento delle aggressioni della *cyber*-criminalità.

È ciò che emerge dall'annuale bilancio della Polizia postale che ha censito, nel corso del 2020, quasi centomila casi di truffe *online* che vanno dai falsi siti *e-commerce* per la vendita di mascherine, *gel* igienizzanti e altri dispositivi di protezione individuale, alle finte raccolte fondi a scopo di beneficienza ma anche, e forse è questo l'aspetto più allarmante, alle intrusioni di pedofili nelle aule virtuali utilizzate per la gestione della didattica a distanza. Si pensi solo che, da quando le scuole sono state chiuse, diverse sono state le segnalazioni di accessi non autorizzati nelle piattaforme dedicate alla formazione, con un aumento del 110% rispetto all'anno precedente.

A fronte di un calo delle attività criminose "tradizionali", dovuto alle misure di contenimento, si è registrata un'impennata dei reati informatici, a testimonianza di un parallelismo tra le abitudini di vita dei soggetti a rischio di manipolazione e le attività criminali che su di esse si modellano.

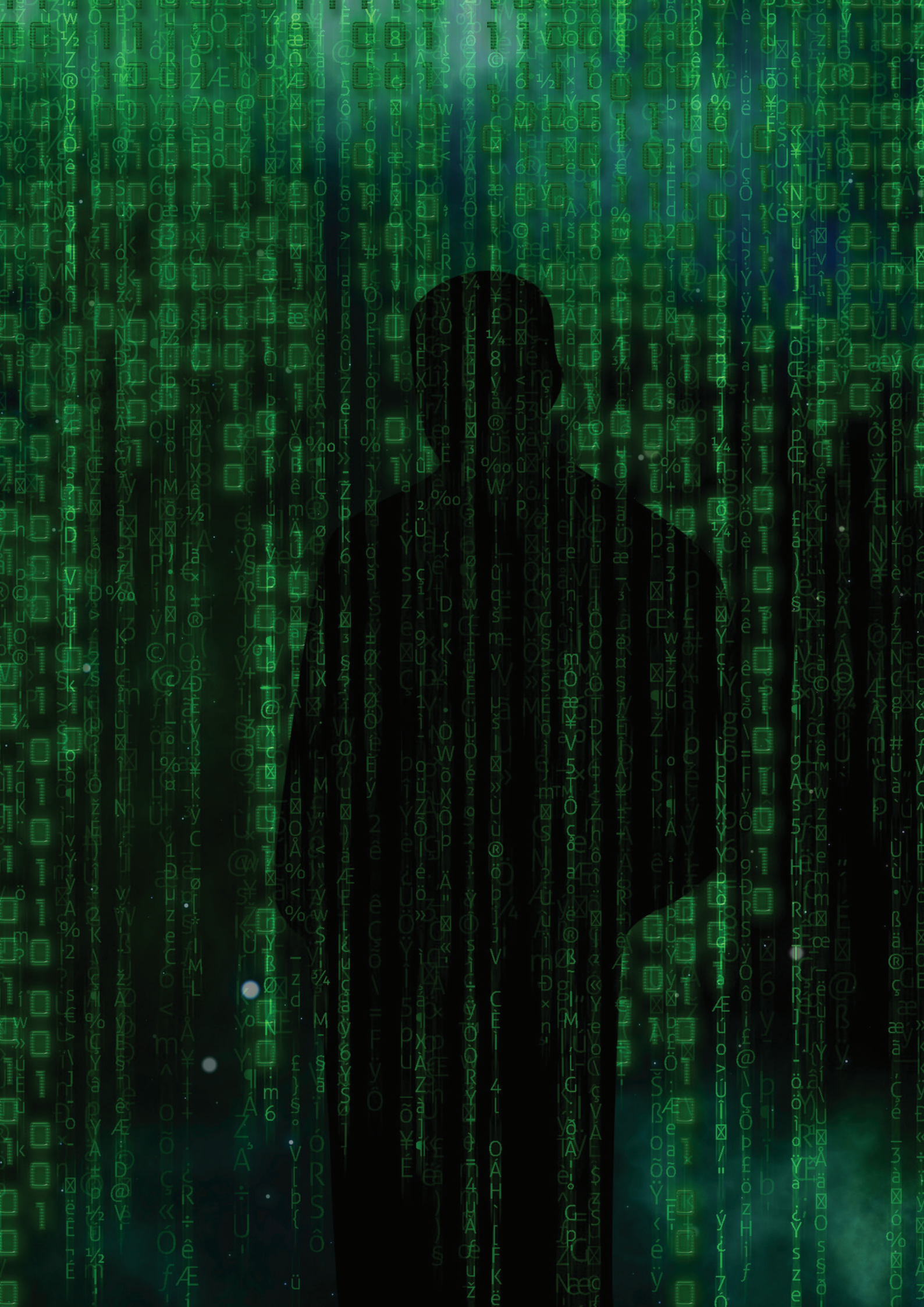
A conferma di tale correlazione, si è assistito ad un incremento di episodi criminosi anche in ulteriori ambiti interessati dalle conseguenze della pandemia, con particolare riferimento al mondo del lavoro, con falsi annunci finalizzati ad ottenere danaro e a carpire identità digitali e a quello della salute, con il numero degli attacchi informatici alle strutture sanitarie è più che raddoppiato rispetto al 2019.

Sempre in base alle statistiche fornite dalla Polizia postale, due sono stati i fenomeni che, più degli altri, hanno monopolizzato lo scenario criminale del 2020.

In primo luogo, gran parte degli attacchi avvengono con il consueto metodo del *phishing*, ossia attraverso *e-mail* che invitano a cliccare su *link* o allegati che, come dei veri e propri cavalli di Troia, consentono di scaricare nel pc della vittima *malware* e *ransomware*, rispettivamente *virus* in grado di carpire i dati personali dell'utente e *software* capaci di limitare l'accesso al dispositivo infettato o cifrare i *file* ivi contenuti, al fine di richiedere un riscatto (*ransom*, in inglese) da pagare per rimuovere detta limitazione o il ripristino del *file* criptato.

È ovvio, quindi, che il *phishing* funziona e prolifera laddove è più riconoscibile l'apparente dominio utilizzato per legittimare la credibilità del messaggio.

Si pensi al caso, ormai noto, delle *e-mail* a



firma di una sedicente dottoressa dell'Organizzazione mondiale della Sanità, che invitava il destinatario ad aprire un allegato infetto (un *malware*, appunto) contenente precauzioni per evitare l'infezione da *Coronavirus*.
Ecco, quindi, la capacità di adattamento del *cyber* criminale che, facendo leva sulle decine e decine di raccomandazioni che quotidianamente ciascuno di noi riceve per scongiurare il rischio di contagio, utilizza un dominio di primo livello che sia il più noto possibile, al fine di conferire una presunta legittimità all'*e-mail* fraudolenta (OMS, Microsoft, eBay ecc…).
Altro fenomeno preso in considerazione dal rapporto annuale della Polizia di Stato e, in particolare, dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), è costituito da un vero e proprio attacco al sistema produttivo del Paese, registrandosi un generale aumento delle minacce legate all'adozione su larga scala dei modelli di lavoro a distanza, c.d. *smart working*. Tali modelli, se da un lato hanno consentito la prosecuzione di attività essenziali, hanno altresì prodotto una considerevole estensione del perimetro informatico delle aziende, con una conseguente maggiore esposizione ad azioni ostili esterne. L'utilizzo di infrastrutture personali ha, di fatto, aumentato vertiginosamente il rischio, per le aziende, di attacchi informatici ad ampio spettro e di sottrazione di dati sensibili. La situazione è ancora più allarmante se si considera che, in molti casi, tali attacchi informatici non sono neppure accompagnati da richieste di riscatto, circostanza che lascia intendere l'esistenza di veri e propri centri di criminalità organizzata di difficile individuazione, intenzionati più all'esfiltrazione di dati che all'ottenimento di un profitto.
Si pensi solo alle conseguenze che potrebbero derivare dalla manomissione di un sistema di sicurezza informatica di un'azienda sanitaria che detiene, ad esempio, studi sull'efficacia di un vaccino anti-Covid19 o dati relativi al trattamento terapeutico dei contagiati, ben più disastrose della perdita, per quanto ingente, di una somma di denaro corrisposta a fronte della richiesta di riscatto per la rimozione delle conseguenze pregiudizievoli di un attacco *hacker*. Parallelamente al continuo ampliarsi dei luoghi virtuali in cui i criminali possono mettere in atto i propri intenti illeciti e all'inarrestabile evoluzione degli strumenti tecnologici di cui si dotano, si accrescono le difficoltà, per le autorità giudiziarie, di risalire agli effettivi autori del reato. Se, infatti, la giurisprudenza è ormai orientata a risolvere i problemi connessi all'individuazione del giudice competente in materia di truffa informatica ricollegando la consumazione del reato al compimento dell'atto di disposizione patrimoniale da parte della vittima, da ciò derivano evidenti criticità sul piano dell'attività investigativa, non potendosi garantire che ad uno stesso ufficio giudiziario pervengano tutte le denun-

"I modelli di smartworking hanno prodotto l'estensione del perimetro informatico delle aziende con una maggiore esposizione ad azioni ostili esterne"


HACKED

ce eventualmente presentate nei confronti della stessa persona o della stessa struttura criminale nel caso in cui le vittime dei raggiri si trovino in luoghi diversi.
Inoltre, applicandosi le regole generali di cui all'art. 8 c.p. per il radicamento della competenza nel luogo di consumazione del reato, viene sostanzialmente disattesa una delle declinazioni applicative dell'art. 25 della Costituzione che, con riferimento alla precostituzione del Giudice naturale chiamato a conoscere della fattispecie criminosa, dovrebbe agevolare il compimento delle indagini e la raccolta dei mezzi di ricerca della prova in ragione della vicinanza proprio con il luogo di commissione del reato. A ciò si aggiunga che le truffe informatiche sono, nella maggior parte dei casi, il frutto di un'ingegnosa architettura criminale progettata per eludere o rendere estremamente difficoltosi gli accertamenti da parte delle autorità giudiziarie. Si pensi al c.d. *bullet proof hosting*, ossia l'offerta (di per sé lecita) di un servizio di *hosting* spesso inaccessibile anche in ragione della loro strategica collocazione in Paesi, dall'Est Europa all'Asia, con un'inefficiente regolamentazione in materia.
Di certo, una maggiore complessità e transnazionalità delle strutture criminali gioca a favore dei *cyber* criminali, derivandone una maggiore difficoltà di collaborazione tra giurisdizioni e procedure di Paesi diversi. La polizia di un Paese europeo, ad esempio l'Italia, per ottenere i dati da una società che possiede un *server* in Romania ma è registrata a Panama, dovrà inviare una specifica e motivata richiesta sulla base di un trattato internazionale di mutua assistenza investigativa. Le indagini ci mettono mesi e, nel frattempo, il sito o l'attività criminale si ricollocano spazialmente in diversi Paesi "ospitanti".
Lo stesso accade quando un fornitore di *hosting* comincia ad attirare su di sé le attenzioni delle autorità. Si riposiziona nel mercato dei servizi informatici con un altro nome ma con identico comportamento, e così via. Se questo è lo scenario criminale che ha saputo sfruttare al meglio le paure e gli effetti causati dalla pandemia in corso, è evidente che un effettivo contrasto all'incremento delle condotte fraudolente che quotidianamente si perpetrano tramite il *web* dovrà trovare la propria regia in un sistema di cooperazione internazionale che sappia orchestrare al meglio i mezzi e le forze delle autorità inquirenti nazionali. Nell'assenza di un effettivo piano internazionale di contrasto al "*cyber*-crimine", il rischio continuerà ad essere quello di vedere vanificate le attività delle forze di polizia nazionali e degli avvocati che, sostanzialmente impossibilitati a svolgere investigazioni difensive in un campo così tecnico ed elusivo, si trovano impotenti dinanzi ad indagini preliminari che si protraggono per mesi, spesso senza alcun risultato, nonostante i gravissimi pregiudizi che le condotte criminose descritte possono causare ai loro assistiti.

Avvocato Andrea Loiaconi

"La Complessità e transnazionalità delle strutture criminali gioca a favore dei cyber criminali"

Avv. Andrea Loiaconi
Si occupa di contenzioso, arbitrati, mediazione, contrattualistica commerciale. Penale e compliance aziendale.
Collabora con lo studio Tonucci dal 2016 .
Laurea in Giurisprudenza presso l'Università degli Studi Roma Tre (2016). Scuola di Specializzazione per le Professioni Legali (2016 – 2018). Iscritto all'Ordine degli Avvocati di Roma (2019).