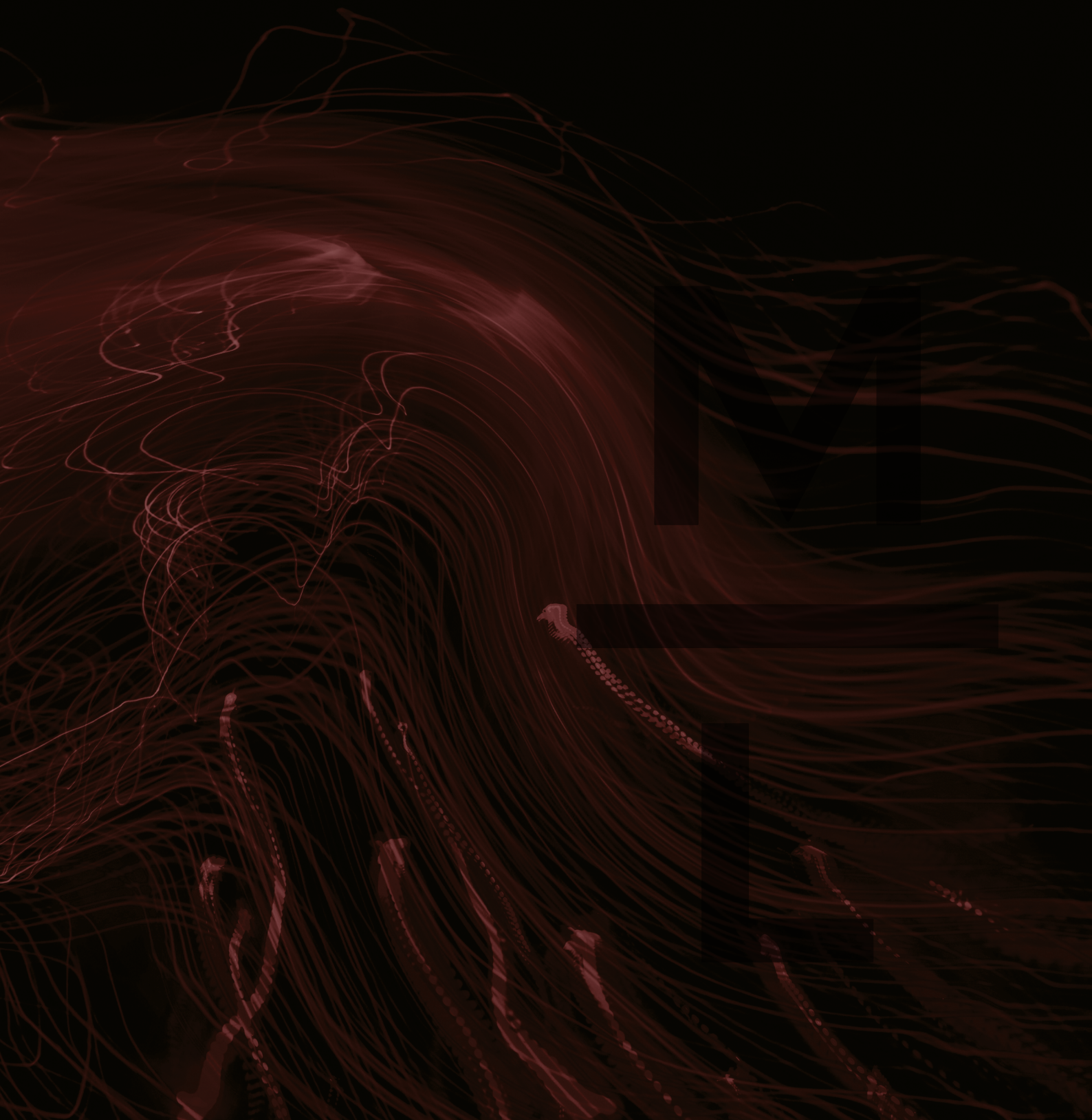
Vol. 2 Julho 2026

3D DIGITAL DEFENSE DISPATCH



DAVID SILVA RAMALHO

Em dezembro de 2025, lançámos o primeiro número do 3D. Quando começámos a sua preparação, quase um ano antes, a ideia era fazermos uma *newsletter*, onde condensássemos um apanhado de notícias, legislação e jurisprudência sobre cibercrime e prova digital. Fechámos a primeira versão da *newsletter*, mas o resultado parecia incompleto, pouco útil, e sem conteúdo diferenciador. Decidimos, então, experimentar outro modelo. Um modelo em que pudéssemos contar com especialistas de referência na área, dispostos a contribuir, de forma livre e informal, com a sua opinião sobre os temas aos quais se dedicam diariamente.

Foi assim que, algures em janeiro de 2025, falei com o Jan Kerkhofs, Diretor da Cyber Unit da Procuradoria Federal da Bélgica, e lhe perguntei se estaria disposto a contribuir com um artigo sobre o Sky ECC, o caso que mudou o paradigma da investigação criminal na Europa, e que o próprio Jan liderou. A resposta foi afirmativa, e o projeto ganhou outra dimensão.

No final do mês de janeiro de 2025, falei com o Alexandre Senra, Procurador do Ministério Público Federal do Brasil, entusiasta e incomparável especialista em tudo o que tenha cripto no nome, que conheci aproximadamente um ano antes durante um curso do Conselho da Europa em São Paulo, e lhe dirigi o convite para aceder a dar-nos uma entrevista. O Alexandre aceitou, e a *newsletter* transformou-se numa revista.

Por fim, tive a sorte de o Nuno Igreja Matos e a Inês Costa Bastos, colegas de escritório e amigos, quererem dividir a preparação do primeiro número comigo, e ainda por cima estarem dispostos a contribuir com dois textos de grande qualidade. O resultado foi um primeiro número difícil de superar.

Assim que fizemos a publicação, começámos a preparar o número seguinte. Agora com a pressão do que tínhamos lançado em dezembro, decidimos demorar o tempo que fosse preciso para fazermos um segundo número que não ficasse atrás do primeiro. Sete meses depois, aqui estamos.

A ideia para o começo do segundo número já existia desde o primeiro. Quando decidimos começar a Revista com um artigo sobre o caso Sky ECC, focado quase exclusivamente na perspetiva do *enforcement* e da necessidade de meios, pensámos que faria sentido incluir no segundo número um artigo que se focasse no outro lado, das garantias de defesa. Foi assim que, em janeiro de 2026, logo após o lançamento do 3D, falei com a Maša Galič, Professora da *Vrije Universiteit Amsterdam*, e Autora incontornável na área, que tive o gosto de conhecer em Cracóvia, nos idos de 2022, e lhe apresentei a ideia de escrever um artigo sobre o tema. O resultado é um artigo brilhante, em que a Autora vem questionar os meios utilizados no caso e os seus resultados, seja quanto à fiabilidade e autenticidade da prova, seja quanto à compatibilização das coordenadas do caso com as garantias de defesa dos visados.

Ainda em janeiro, em conversa com a Cláudia Pina, acabada de regressar à magistratura vinda da *European Judicial Cybercrime Network*, propus que escrevesse um texto sobre um tema da sua preferência, aproveitando o conhecimento e a experiência acumulados por essas paragens. A Cláudia escolheu um tema sobre o qual se tem escrito muito pouco e cuja relevância é indiscutível, o das ameaças híbridas. E escreveu-o, como na sua recente obra, com base no método do caso, e numa escrita que torna impossível interromper a leitura.

Mas como é impossível falar de novas tecnologias sem falar em inteligência artificial, e sendo essa uma omissão relevante no primeiro número, decidimos incluir um artigo especificamente sobre esse tema. Contactei o Angelo Costanzo, juiz do Supremo Tribunal de Justiça italiano (a *Corte Suprema di Cassazione*), com quem tive o gosto de partilhar um painel em Siracusa algures em fevereiro de 2023, e que se tem dedicado amplamente ao estudo dessa e de outras matérias no Direito, e ele preparou um texto, tão complexo quanto interessante, sobre a intersecção entre lógica, raciocínio jurídico e inteligência artificial.

Por fim, a Ana Xavier Nunes, teve a generosidade de aceitar o convite para contribuir com um texto sobre cibersegurança, e com esse texto, também de qualidade superior, fechámos os contributos escritos todos.

Faltava, no entanto, uma entrevista, para mantermos a estrutura do primeiro número. Tomei a liberdade de contactar o Nick Furneaux. Ao contrário de todos os outros autores que contribuíram para o 3D, não conhecia o Nick pessoalmente, mas já tinha lido os seus livros "Investigating Cryptocurrencies" e "There's no such thing as crypto crime", e sabia que é uma das referências mundiais na matéria do *tracing* de criptoativos, por isso decidi arriscar. Com a resposta afirmativa do Nick, fechámos a lista de convidados externos (com uma entrevista que, mérito do Nick, é excelente).

Restou a parte mais morosa, de compilação de notícias, legislação, *soft law*, jurisprudência dos vários cantos do globo, e que levou a que este número só tenha saído agora. Bem sei que na era da inteligência artificial esta tarefa deveria ser mais fácil, mas há coisas, para já, que não dispensam supervisão humana. Se dúvidas houvesse, basta ler a história de ficção com que fechamos este número, e que foi redigida por inteligência artificial. A (baixa) qualidade do texto permite concluir que ainda há margem para a imaginação humana.

Fica, assim, fechado mais um número do 3D.

ARTIGOS

NOTÍCIAS

O QUE TEM O ACESSO AOS DADOS BRUTOS A VER COM ISTO?

MAŠA GALIČ
Professora Auxiliar de Privacidade e Direito (Processual) Penal
Vrije Universiteit Amsterdam

Em 21 de janeiro de 2026, um tribunal de primeira instância espanhol em Valência absolveu vários arguidos acusados de tráfico de estupefacientes, num dos muitos processos relativos aos "criptofones" Sky ECC atualmente pendentes por toda a Europa. A decisão é relevante porque se insere num grupo muito restrito de decisões judiciais europeias em que rejeitaram a fiabilidade da prova digital obtida através de operações de *hacking* transfronteiriço. O tribunal debruçou-se sobre uma das questões fundamentais relativas à partilha de prova digital obtida através de uma Decisão Europeia de Investigação (DEI): como deve ser avaliada a autenticidade e fiabilidade das comunicações encriptadas obtidas através da cooperação baseada numa DEI? Neste texto, abordo brevemente esta questão, situando o raciocínio do tribunal espanhol no contexto da discussão mais ampla sobre a fiabilidade da prova digital.

I. A FIABILIDADE COMO CONCEITO MULTIDIMENSIONAL

As questões relativas à autenticidade e fiabilidade das comunicações encriptadas intercetadas prendem-se com problemas mais amplos de fiabilidade da prova digital, problemas demasiado complexos para serem respondidos numa contribuição breve como esta. No contexto da prova digital, os próprios termos – autenticidade e fiabilidade – são multidimensionais e frequentemente utilizados de forma inconsistente, tanto na doutrina jurídica como pelos tribunais. Na verdade, discernir as distinções exatas entre autenticidade, validade, integridade e fiabilidade no contexto digital, conceitos todos eles igualmente utilizados na decisão espanhola, não é tarefa fácil.

Além disso, o processamento de material digital em investigações criminais desenvolve-se habitualmente em várias fases: (1) recolha e preservação dos dados; (2) extração, armazenamento, seleção e análise; (3) tradução do material digital em relatórios escritos (conforme é ainda exigido em muitos ordenamentos jurídicos nacionais); e (4) apreciação dos relatórios escritos em julgamento[1]. Cada fase suscita preocupações distintas em matéria de fiabilidade e, por conseguinte, exige garantias distintas.

Na fase inicial de recolha e preservação dos dados, a questão central é a cadeia de custódia: onde, como e por quem foram os dados obtidos, e como foram processados? A cadeia de custódia exige, portanto, a autenticidade dos dados (relativa à sua origem e identidade) e a integridade dos dados (referente ao estado dos dados, que devem permanecer intactos e inalterados)[2]. Na prática, isto é habitualmente assegurado através de imagens forenses, *hashing*[3] e *logging* detalhado. Mesmo quando tais procedimentos são seguidos, contudo, os casos Sky ECC suscitam dificuldades estruturais. O método e as ferramentas de *hacking* utilizados pelas autoridades

1 Ver a discussão em C. Taylor Parkins-Ozephius (2025), "Syntax error! Een verkenning van betrouwbaarheidsconcepten bij digitaal bewijs in strafzaken", *Expertise en Recht* 4.

2 Um valor de *hash* é uma representação condensada do conteúdo binário (digitalizado) de material digital, que é calculada com o objetivo de verificar a integridade do material digital, bem como para a identificação e classificação eficiente de arquivos. Cf. Netherlands Forensic Institute (2021), "Technical Supplement – Forensic Use of Hash Values and Associated Hash Algorithms", disponível em https://www.forensicinstitute.nl/documents/2018/02/13/forensic-use-of-hash-values-and-associated-hash-algorithms.

3 ibidem.

francesas permanecem confidenciais. Embora tal sigilo seja legalmente admissível ao abrigo do direito francês, neerlandês e, aparentemente, também espanhol, esta confidencialidade deixa os Estados recetores largamente dependentes das garantias prestadas pela autoridade de execução quanto à integridade e autenticidade dos dados.

II. DA CADEIA DE CUSTÓDIA À CADEIA DE PROVA

Durante a segunda fase, em que os dados são extraídos, filtrados, armazenados e analisados, a cadeia de custódia permanece um requisito essencial, uma vez que os dados recolhidos devem manter-se intactos também durante o seu tratamento. Esta fase, contudo, introduz um requisito adicional: a cadeia de prova (*chain of evidence*). A cadeia de prova exige resposta sobre as escolhas que foram feitas durante o tratamento dos dados, incluindo as correspondentes interpretações? Esta fase do tratamento diz respeito, portanto, não apenas à preservação dos dados, mas também à validade das ferramentas e das escolhas interpretativas aplicadas. Que conjuntos de dados foram selecionados? Que filtros foram utilizados? Os resultados são consistentes e reprodutíveis? Estas questões incidem sobre a validade metodológica e não a mera integridade.

Foi durante esta fase, especificamente no que respeita à cadeia de prova, que as coisas correram mal no caso espanhol. Segundo a decisão, as autoridades francesas filtraram o conjunto de dados pelo menos duas vezes antes de o partilhar com Espanha. A polícia espanhola recebeu um *link* para descarregar um ficheiro ZIP, copiou-o para duas *pen drives* USB (uma depositada junto de um tribunal, outra para uso operacional) e prosseguiu com a investigação. Porém, os agentes espanhóis reconheceram que os ficheiros recebidos das autoridades francesas não eram acompanhados de valores de *hash* ou assinaturas digitais. A única garantia era a de que a *pen* USB entregue ao tribunal continha tudo o que tinham descarregado.

Isto significa que a cadeia de custódia durante esta fase não foi tecnicamente estabelecida. Além disso, a decisão não contém qualquer exame da cadeia de prova: nenhuma informação sobre os critérios de filtragem utilizados pelas autoridades francesas (ou pela Europol), nenhuma validação das ferramentas analíticas e nenhuma avaliação da reprodutibilidade.

Apesar destas deficiências, o tribunal espanhol considerou inicialmente que a fiabilidade podia, ainda assim, ser suficientemente estabelecida a partir das declarações prestadas pelos agentes espanhóis que descarregaram o ficheiro e pela documentação francesa anexa à Decisão Europeia de Investigação.

III. PROVA ÚNICA E ARTIGO 6.º DA CEDH

A viragem decisiva na decisão espanhola veio de outra direção. O tribunal concluiu pela absolvição porque as comunicações Sky ECC constituíam a única prova contra os arguidos. O tribunal espanhol concluiu que, para que o direito a um processo equitativo previsto no artigo 6.º da CEDH fosse garantido, a defesa teria de ter tido acesso aos "dados brutos" ("*raw data*") obtidos a partir da interceção ordenada sobre os servidores utilizados pela empresa SKY ECC.

Este raciocínio alinha-se, pelo menos em espírito, com a doutrina de Estrasburgo: a igualdade de armas e o princípio acusatório exigem que a defesa seja colocada em posição de testar eficazmente a prova da acusação. Contudo, a decisão é concetualmente imprecisa. O acesso aos dados brutos, por si só, não pode sanar defeitos na cadeia de custódia[4]. Nem pode estabelecer retroativamente a integridade dos ficheiros transferidos. [Tal como as declarações dos agentes que descarregaram o ficheiro não podem substituir a ausência de quaisquer garantias

[4] V. a minha análise sobre os níveis e tipos de acesso aos vários tipos de conjuntos de dados na jurisprudência do Tribunal Europeu dos Direitos Humanos: M. Galič (2021), "De rechten van de verdediging in the context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken", 2 *Boom Strafblad*; versão em inglês disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3838680.

técnicas]. No máximo, os dados brutos, combinados com informação sobre as ferramentas e métodos de filtragem, poderiam permitir à defesa avaliar a consistência e reprodutibilidade da filtragem, no que respeita à cadeia de prova. Mas isso não foi posto em causa no caso em apreço.

IV. UM PASSO MODESTO, MAS IMPORTANTE

Apesar de todas as suas limitações, a decisão de Valência representa um afastamento importante da abordagem largamente deferente adotada pelos tribunais em várias outras jurisdições com processos Sky ECC. Embora o enfoque do tribunal espanhol no acesso aos dados brutos não aborde adequadamente os problemas subjacentes de informática forense, a decisão constitui, ainda assim, uma primeira tentativa judicial de reconhecer que as operações de *hacking* transfronteiriço em larga escala criam *black boxes* probatórias que podem não ser compatíveis com o artigo 6.º da CEDH apenas à luz de um mero princípio abstrato de confiança mútua.

GUERRA HÍBRIDA NO CIBERESPAÇO – DA OPERAÇÃO EASTWOOD À BARRAGEM DE STÂNCA-COSTEȘTI: QUANDO O CIBERESPAÇO SE TORNA CAMPO DE BATALHA

CLÁUDIA PINA
Juíza de Instrução Criminal

I. A AMEAÇA NÃO DECLARADA

A guerra híbrida não tem frente de batalha. Não existe declaração formal de hostilidades, não há uniformes, não há um inimigo claramente identificável. O que existe é uma orquestração calculada de instrumentos económicos, cibernéticos, informacionais e de sabotagem, destinados a pressionar, desestabilizar e enfraquecer um Estado sem que esse Estado, nem os seus aliados, possam invocar legitimamente os mecanismos clássicos da resposta militar.

Esta é a sua força e a sua perversidade jurídica. As ameaças híbridas operam deliberadamente abaixo do limiar formal da guerra, ocupando aquilo uma zona cinzenta, um espaço entre o conflito armado e a paz. É precisamente nesta zona que o Direito enfrenta as maiores dificuldades: as regras do Direito Internacional Humanitário aplicam-se a conflitos armados; o Direito Penal nacional tem capacidade de resposta limitada quando os agentes operam a partir de jurisdições não cooperantes e o Direito Internacional Público carece de mecanismos de resposta rápida para atos que, individualmente, podem parecer menores, mas que constituem, em conjunto, uma agressão sistemática.

Porém, esta zona cinzenta não é um vácuo normativo. O Direito existente, Penal interno, europeu e internacional, já nos fornece instrumentos para qualificar, perseguir e dissuadir estes atos. O que falta não são normas. Falta capacidade probatória, coordenação institucional e vontade política. Os dois casos que se seguem ilustram este argumento: o primeiro, real, mostra o que o sistema de justiça já consegue fazer; o segundo, hipotético, mas fundado em dados reais, mostra o que poderá ser chamado a tratar.

Os Grupos de Ameaça Persistente Avançada, designados na literatura técnica como APT (*Advanced Persistent Threats*), são o braço operacional desta estratégia. Não são *hackers* solitários movidos por curiosidade ou ganância imediata. São estruturas organizadas, frequentemente financiadas ou toleradas por Estados, que seguem ciclos operacionais metódicos: reconhecimento, infiltração, expansão e exploração.

II. OPERAÇÃO EASTWOOD: CIBERCRIME, TERRORISMO E OS LIMITES DO ENQUADRAMENTO JURÍDICO

Era primavera na Europa Central. Nos ecrãs de dezenas de ministérios, parlamentos e organismos públicos, o acesso tornava-se impossível, não por falha técnica, mas por intenção. Algures, num servidor cuja localização era deliberadamente opaca, um grupo chamado NoName057(16) desencadeava a sua rotina de destruição silenciosa.

O grupo pró-russo NoName057(16) operava há meses disciplinadamente, combinando ataques de negação de serviço distribuída (DDoS) com uma estrutura de recrutamento "gamificada". Cerca de 4000 utilizadores foram mobilizados através de aplicações de mensagens como o Telegram, recebendo recompensas em criptomoedas por cada ataque bem-sucedido. Os alvos eram cuidadosamente selecionados: infraestruturas críticas e organismos governamentais em países europeus que apoiavam a Ucrânia ou manifestavam alinhamento com a NATO. Os ataques eram cronometrados para coincidir com momentos politicamente sensíveis, cimeiras, votações parlamentares, anúncios de apoio militar, amplificando o impacto mediático.

A resposta a esta ameaça foi coordenada. Sob a égide do Eurojust e da Europol, doze países participaram numa operação que desmantelou a infraestrutura central do grupo, emitiu sete mandados de detenção internacionais e perturbou mais de 100 servidores em todo o mundo. Os participantes recrutados em redes sociais foram notificados da sua responsabilidade criminal. O rosto de um dos alegados líderes, cidadão russo, ficou registado na lista dos mais procurados da União Europeia, um ato de nomeação pública que possui valor dissuasivo e simbólico.

Os ataques DDoS são um exemplo de *cyber-dependent crime*: ilícitos que só existem no ciberespaço e que dependem inteiramente de meios digitais para serem cometidos. A Operação Eastwood enquadrou a conduta do NoName057(16) como criminalidade organizada e criminalidade informática. É uma opção juridicamente sólida, mas que deixa por explorar sanções mais graves.

Os elementos objetivos e teleológicos do grupo podem permitir concluir que a sua atuação se enquadra na definição de infração terrorista para os efeitos do art. 3.º n.º 2 da Diretiva (UE) 2017/541 e art. 2.º n.º 3 da Lei 52/2003, de 22 de agosto: atos suscetíveis de intimidar gravemente uma população, compelir governos a alterar políticas e desestabilizar as estruturas políticas, económicas ou sociais fundamentais de um Estado. Tanto a Diretiva como a Lei 52/2003 referem-se expressamente os ataques a infraestruturas críticas como categoria autónoma. No caso do APT NoName, a intenção dos ataques não era pecuniária, mas política e intimidatória, e o momento dos mesmos confirma-o, permitindo a integração no conceito.

A qualificação como terrorismo poderia ter permitido, em algumas jurisdições, acesso a meios de obtenção de prova reservados, prazos de detenção preventiva alargados, bloqueio de ativos e acesso facilitado a dados na posse de entidades privadas. Nos ordenamentos jurídicos dos países participantes na operação, esta via estava disponível. Que não tenha sido utilizada reflete uma hesitação compreensível, pois qualificar como terrorismo um ataque tolerado ou financiado por um Estado soberano implica uma tomada de posição de elevada carga diplomática. Esta ambiguidade na qualificação, esta hesitação de passar da qualificação como simples organização criminosa para grupo terrorista é ela própria um problema que carece melhor coordenação em casos transnacionais desta natureza.

Mesmo sem a qualificação do NoName como grupo terrorista, os seus membros principais, ainda que residentes em jurisdições não cooperantes como a Federação Russa, não estão imunes ao direito penal interno dos Estados visados. As condutas em causa, descritas no art. 5.º da Convenção de Budapeste e legislação nacional dos Estados visados, são passíveis de permitir, de acordo com o Direito Processual Penal de cada Estado, a instrução de processos em ausência e a emissão de mandados internacionais para o momento em que as condições se alterem e seja possível trazer cada um dos autores do crime perante um Tribunal, dado que a negação plausível do Estado patrocinador não apaga a responsabilidade individual dos operadores identificados.

III. A NOITE EM QUE O PRUT SE TORNOU UMA ARMA: CRIME DE GUERRA DIGITAL?

A barragem de Stânca-Costești, construída entre 1974 e 1978 como projeto conjunto entre a Roménia e a então URSS, ergue-se sobre o rio

Prut, fronteira entre a Roménia e a República da Moldávia. A sua localização é singular: o Prut nasce na Ucrânia, nos Cárpatos, serve de fronteira natural entre a Roménia e a Moldávia ao longo de 711 quilómetros, e desagua no Danúbio, tornando a barragem um ponto de confluência de três soberanias e uma das infraestruturas transfronteiriças mais sensíveis da Europa Oriental.

O reservatório tem uma capacidade total de 1285 milhões de metros cúbicos e 59 km² de área. A barragem mede 48 metros de altura e 740 metros de comprimento. A sua função primária é a proteção das planícies do Prut: foi construída para evitar a repetição das catastróficas cheias de 1970. Em 2008, com a barragem em modo controlado a libertar água a 845 m³/s de forma controlada, as autoridades classificaram a situação como ameaça para as 15 000 pessoas nas 13 localidades a jusante e procederam à evacuação parcial. Mesmo assim, mais de 300 habitações foram afetadas e cerca de 180 completamente destruídas.

Na madrugada de 24 de abril chovia intensamente. As águas do Prut corriam altas. O reservatório de Stânca-Costești estava a 91% da capacidade. Apesar disso, era um cenário normal de primavera para os operadores de turno, o que estes não sabiam era que havia meses que não estavam sozinhos nos sistemas.

Em novembro, membros de um APT com ligações documentadas a serviços de informação militares de um Estado adversário tinham obtido acesso remoto ao sistema SCADA de gestão da barragem através de uma vulnerabilidade não corrigida num módulo de controlo industrial. O vetor de entrada foi um ataque de *phishing* dirigido a um engenheiro de manutenção subcontratado para a manutenção dos sistemas. Infiltrado o *malware,* este permaneceu em modo *living off the land*, hibernando silenciosamente até que o gatilho de 90% da capacidade da albufeira fosse atingido.

Como programado, às 03h33m, com vento forte, chuva intensa, caudal afluente elevado e equipas de manutenção reduzidas ao turno mínimo noturno, as comportas de descarga foram abertas de forma repentina e não controlada. Nos primeiros minutos, os operadores pensaram numa falha de sistema. Tentaram repor os comandos digitalmente, sem sucesso.

Enquanto os operadores tentavam desesperadamente ativar as redundâncias físicas, equipas de socorro são enviadas para um leito de rio que já se transformou numa torrente mortal. Precisamente uma hora depois, no lado ucraniano, explosões cirúrgicas destroem os diques de proteção, libertando uma parede de água que viaja como um pistão hidráulico sobre o caudal já cheio, atingindo a barragem com uma força cinética imparável.

A decisão torna-se impossível: fechar as comportas e arriscar o colapso estrutural total, ou mantê-las abertas e deixar o caudal fluir em direção à Moldávia. Devido à geografia baixa da margem esquerda, a catástrofe é brutalmente assimétrica, resultando em mais de seis mil mortos moldavos e na aniquilação das suas equipas de salvamento, face a cerca de mil vítimas romenas. Nas redes sociais, a desproporção de meios, com a Roménia a mobilizar meios de emergência da UE enquanto a Moldávia procura recuperar da catástrofe com escassos recursos, é utilizada para alimentar a narrativa de que Bucareste conhecia o ataque e sacrificou o "país irmão" para se salvar, selando uma rutura geopolítica definitiva e traumática.

Nenhum Estado declarou guerra. Um porta-voz do Adversário negou qualquer envolvimento, sugerindo que os serviços secretos ucranianos estariam envolvidos na sabotagem das infraestruturas no seu próprio país para o culpabilizar.

IV. ENQUADRAMENTO JURÍDICO

Para que um ciberataque possa ser qualificado como crime de guerra ao abrigo do artigo 8.º do Estatuto de Roma, são necessários três elementos cumulativos: a existência de um nexo suficiente com um conflito armado em curso, efeitos graves sobre a população civil, e intencionalidade no sentido do artigo 30.º do mesmo

Estatuto. No cenário descrito, os três elementos estão presentes.

O primeiro elemento, o chamado *war nexus*, exige que o ato esteja suficientemente ligado a um conflito armado em curso. O conflito armado internacional entre a Rússia e a Ucrânia fornece esta âncora. A ligação é geográfica, doutrinária e estratégica. O rio Prut nasce nos Cárpatos ucranianos, e a bacia hidrográfica superior da barragem de Stânca-Costești inclui território ucraniano. Uma descarga catastrófica afetaria diretamente os distritos moldavos que constituem hoje corredor logístico e humanitário crítico para o esforço de guerra ucraniano, nomeadamente as infraestruturas de Ungheni e o corredor ferroviário Iași-Chișinău.

A Moldávia, Estado candidato à União Europeia com presença militar russa na Transnístria, é ela própria um ator frágil cujo colapso institucional ou humanitário serviria objetivos estratégicos russos identificados. A destruição de infraestruturas hídricas como instrumento de pressão estratégica é, além disso, uma característica documentada da conduta no conflito ucraniano: o colapso da barragem de Kakhovka, em junho de 2023, privou de água potável centenas de milhares de pessoas no sul da Ucrânia e a investigação do Tribunal Penal Internacional sobre esse evento analisa precisamente os artigos 8.º(2)(b)(ii) e (iv), do Estatuto de Roma, relativos ao ataque intencional a bens civis e ao dano excessivo à população civil.

O Manual de Tallin, guia não vinculativo, mas de referência, produzido pelo NATO CCDCOE, estabelece que uma operação cibernética constitui um ataque na aceção do Direito Internacional Humanitário quando pode razoavelmente prever-se que cause danos, destruição, mortes ou ferimentos. O critério é o efeito não os meios utilizados. Um *malware* que abre a comporta de uma barragem é juridicamente equivalente, para efeitos do Direito Internacional Humanitário, à mão de um sabotador que a abre manualmente.

As barragens beneficiam ainda de proteção reforçada ao abrigo do artigo 56.º do Protocolo Adicional I às Convenções de Genebra, que as classifica como instalações que contêm forças perigosas. O seu ataque é proibido mesmo quando constituam objetivos militares, se os efeitos previsíveis forem a libertação de forças que causem perdas severas na população civil. Esta proteção reforçada é espelhada na Regra 42 do Manual de Tallin. No cenário da barragem de Stânca-Costești, não existe sequer vantagem militar a obter: a descarga noturna de água sobre populações civis adormecidas não serve qualquer objetivo de combate identificável.

O artigo 30.º do Estatuto de Roma exige que o agente tenha conhecimento das circunstâncias e preveja as consequências no curso normal dos eventos. No cenário descrito, a escolha deliberada do momento, noite, reservatório a 91% da capacidade, caudal máximo afluente, evidencia precisamente o conhecimento e a previsão de que a descarga causaria vítimas civis. A Câmara Preliminar do Tribunal Penal Internacional tem reconhecido que este padrão de intencionalidade pode ser inferido das circunstâncias operacionais, independentemente de confissão ou prova documental direta.

O maior obstáculo processual é probatório, não normativo. A atribuição de um ciberataque a um agente específico, com o grau de certeza exigido pelo processo penal, é tecnicamente complexa: os APT operam através de infraestruturas deliberadamente fragmentadas, com servidores em múltiplas jurisdições, endereços IP mascarados e código partilhado para criar confusão de atribuição. Contudo, o princípio da responsabilidade do superior hierárquico, previsto no artigo 28.º do Estatuto de Roma, contorna parcialmente este obstáculo: um superior, militar ou civil, pode ser responsabilizado penalmente por crimes cometidos por subordinados se sabia ou deveria ter sabido que estavam a ser cometidos, e não adotou medidas razoáveis para os prevenir ou punir. Aplicado o princípio a operações cibernéticas de um Estado, este princípio permite subir a cadeia de comando além do operador individual, mesmo que este se encontre em território russo. A negação plausível não é um escudo jurídico absoluto.

Em dezembro de 2025, o Tribunal Penal Internacional publicou a sua Política sobre Crimes Cibernéticos ao abrigo do Estatuto de Roma, confirmando pela primeira vez de forma expressa e sistematizada a intenção de investigar e perseguir crimes internacionais facilitados por meios cibernéticos. O documento não cria novas normas; aplica o Estatuto de Roma ao ciberespaço, confirmando que a forma digital não altera a substância criminosa dos atos. Um ataque à barragem de Stânca-Costești, cometido em associação com o conflito armado em curso na Ucrânia, satisfaz os critérios desta Política em três dimensões: é um ato perpetrado por meios cibernéticos, causa efeitos físicos graves sobre populações civis e ocorre num contexto geopolítico com nexo suficiente a um conflito armado internacional.

V. O QUE PODE FAZER O SISTEMA DE JUSTIÇA?

A resposta do sistema de justiça a ameaças híbridas de origem cibernética tem de ser estruturalmente honesta sobre os seus limites. A retaliação contra o Estado patrocinador, as sanções, a diplomacia coerciva e as medidas de contra-ataque cibernético pertencem à caixa de ferramentas da diplomacia e da segurança nacional, não ao sistema de Justiça. O papel deste é a produção de prova e a atribuição de responsabilidade penal individual, mesmo quando a perseguição efetiva permanece frustrada pelas fronteiras de Estados não cooperantes. Quatro boas práticas emergem da experiência da Operação Eastwood e dos desenvolvimentos recentes do direito penal internacional.

A primeira é a nomeação pública e a perseguição judicial. Através de mandados de detenção europeus ou internacionais, listas de procurados e procedimentos penais públicos, o sistema de justiça constitui mecanismos de pressão e dissuasão que transcendem a mera sanção individual: aumentam o custo reputacional e operacional para o adversário e para o mercado de recrutamento de *proxies*. O ato de tornar o rosto e o nome de um operador de APT públicos, ainda que resida em Moscovo, constrange a sua mobilidade futura e sinaliza ao ecossistema criminal que a impunidade tem limites.

A segunda é a cooperação judiciária internacional. As Ordens Europeias de Investigação e os instrumentos de assistência judiciária em matéria penal permitem consolidar provas de atribuição com valor processual em múltiplas jurisdições simultaneamente. A Operação Eastwood demonstrou que doze países conseguem coordenar uma ação conjunta, incluindo buscas, apreensões e notificações digitais, num único *Action Day*. Esta coordenação deve ser a norma em casos similares.

A terceira é a articulação com o ecossistema de inteligência, defesa e setor privado. A instrução de processos complexos de ciberataque exige informação técnica de fontes que o sistema de justiça não produz autonomamente, designadamente inteligência de sinais, análise forense digital de equipamentos, e dados de empresas de cibersegurança. A integração processual desta informação, na medida do possível para que possa servir de meio de prova é condição necessária para processos de atribuição com valor penal.

A quarta é a preservação de prova para o futuro. Mesmo quando a perseguição imediata é inviável, a documentação rigorosa dos ataques cibernéticos com impacto humanitário constitui a base para que, quando a janela política se abrir, tribunais nacionais ou, subsidiariamente, o Tribunal Penal Internacional, possam agir.

VI. CONCLUSÃO

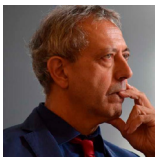
A barragem de Stânca-Costești não é uma metáfora. É uma infraestrutura real, com dados de capacidade publicados, com 15 000 pessoas documentadas nas suas zonas de risco a jusante, com um histórico de cheias catastróficas e com sistemas de controlo digital que partilham as vulnerabilidades estruturais de qualquer SCADA de geração anterior. O cenário descrito neste artigo é ficção de enquadramento, mas é construído sobre factos hidrológicos reais, precedentes operacionais documentados e uma análise das

consequências que os próprios registos oficiais das cheias de 2008 permitem projetar.

A guerra híbrida no ciberespaço dissolve as fronteiras entre crime e guerra, entre o digital e o cinético, entre responsabilidade estatal e responsabilidade individual. O Direito existente já oferece uma resposta em dois planos complementares: no plano do Direito interno e europeu, os ataques híbridos de origem estatal devem ser qualificados, conforme a sua natureza e gravidade, como crimes informáticos, criminalidade organizada ou infrações terroristas ao abrigo da Diretiva 2017/541 e Lei 52/2003, com todos os instrumentos processuais que cada qualificação disponibiliza, independentemente da localização dos operadores. No plano do Direito internacional, quando verificado o nexo com um conflito armado em curso, a existência de efeitos graves sobre população civil e a intencionalidade exigida pelo Estatuto de Roma, o caminho do crime de guerra perante o Tribunal Penal Internacional garante alcance sobre os principais instigadores e memória institucional do ato.

O desafio não é de lacuna normativa. É de capacidade probatória, de coordenação internacional e de vontade institucional. A Operação Eastwood mostrou que é possível agir no plano penal contra *proxies* estaduais em guerra híbrida. O cenário da barragem do Prut mostra que a possível escala do próximo passo exige que o sistema de justiça, nacional e internacional, estejam devidamente coordenados antes que a onda chegue.

DO PRÉ-CONSCIENTE À CIBERSEGURANÇA



ANGELO COSTANZO
Juiz do Supremo Tribunal
de Justiça de Itália

I. BI-LÓGICA

A lógica do século XX forneceu dois instrumentos poderosos para refinar a ideia de que o raciocínio é um processo verbal, mas, ao mesmo tempo, é uma ação interna da psique[1].

O primeiro é constituído pelas **lógicas não clássicas**, que legitimaram desvios de princípios lógicos (não contradição, terceiro excluído) que a tradição tem entendido como fundamentais, mas que nos argumentos são ordinariamente relativizados.

O segundo é oferecido pela "bi-lógica", que dá forma a uma perspetiva mais ampla, na qual argumentos informais e demonstrações formais podem ser entendidos como formas de raciocínio situadas ao mesmo nível de emergência a partir dos fundamentos pré-lógicos do pensamento[2].

As ideias centrais da "bi-lógica" são as seguintes. Quando consciente, a mente pode abordar os seus objetos de dois modos: um analítico (distinguindo, dividindo) e o outro analógico (assimilando, unificando). O primeiro modo liga os objetos que distinguiu através de relações lógicas. O segundo modo trata o conjunto dos seus objetos como uma totalidade homogénea: revela aspetos do campo observado que por vezes não são acessíveis de outro modo, mas, por estar enraizado no solo do pré-consciente, pode induzir em erro o pensamento discursivo. A "bi-lógica" acede aos níveis de pensamento subjacentes aos dois modos, interpretando estados mentais como interações entre a tendência para seguir relações simétricas e a propensão para estabelecer relações assimétricas.

O **princípio lógico simetrizante** trata os objetos e as suas classes como componentes de classes mais amplas, propaga assimilações inconscientes, não movidas pelo discernimento. São governados por **relações simétricas**: a atividade onírica, as fantasias, as pulsões, as emoções mais intensas, a criatividade (que, contudo, exige que a capacidade de distinguir os objetos que são entretanto unificados não se perca, porque, tal como *ex contradictione quodlibet sequitur, também ex indistinctione quodlibet sequitur*).

O **princípio lógico assimétrico** faz proliferar distinções, trata um objeto particular como componente de uma classe (seguindo o esquema das ramificações conceptuais da "*árvore de Porfírio*" clássica) e, enquanto os produtos da "simetrização" tendem a tornar-se indistinguíveis, os da "genericização" são claramente distinguíveis entre si, de modo que são tratáveis por uma lógica com dois valores de verdade ("verdadeiro, falso"). A aplicação total do princípio simetrizante conduziria à ausência de negação e à identificabilidade total (indiscernibilidade) entre objetos. Por outro lado, uma vez que interage com o "princípio assimétrico",

[1] Aristotle, *Second Analytics*, I, 76b 24-25.

[2] O autor da bi-lógica é I. Matte-Blanco, a cujos principais trabalhos aqui nos referimos: *The Unconscious as infinite Sets. An Essay in Bi-Logic*, Duckworth, 1975; *Thinking, Feeling, and Being. Clinical Reflection on the Fundamental Antinomy of Human Beings and World*, Routledge, 1988.

é possível regimentar – de diferentes modos e graus – a desordem, evitando assim o caos lógico. O resultado é uma "bi-lógica", que, contudo, só pode ser descrita através da sua componente assimétrica: a **lógica clássica** (um baluarte contra a força desintegradora das emoções e dos impulsos).

II. ARGUMENTAÇÃO E *ARS DISTINGUENDI*

Grande parte dos dados e das suas correlações perde-se na transição da elaboração pré-consciente para a elaboração consciente de um argumento expresso nas formas de um discurso, mas esta passagem é indispensável para a comunicação e útil para o controlo dos seus conteúdos.

Em todo o caso, a leitura bi-lógica de um argumento (dos argumentos individuais e da sua conexão num raciocínio) nem sempre é possível, nunca é simples, envolve o risco de graves mal-entendidos ou meras inferências e, em qualquer caso, está inevitavelmente destinada a permanecer incompleta.

Contudo, mesmo dando apenas alguns passos nessa direção, é possível clarificar algumas raízes psicológicas do raciocínio, os seus graus de **cogência** e as falácias que o podem viciar: o raciocínio manifesto desenvolve-se sobre o pano de fundo de bases extensas, destinadas a permanecer entimemáticas, de pressupostos inexplícitos e subtilezas nem sempre partilhadas entre quem se expressa e quem lê ou escuta.

A argumentação com que se desenvolve o tratamento de um tema pode evocar, organizar e entrelaçar de diferentes modos uma variada multitude de relações, cada uma caracterizada pela sua própria proporção entre relações simétricas e assimétricas.

O poder persuasivo de um argumento é influenciado pela combinação de assimetrização e simetrização, entre lógica (de identidade, que sustenta inferências dedutivas) e lógica analógica (de semelhança, que sustenta inferências indutivas e abdução). Este entrelaçamento é eficaz se respeitar um cânone fundamental: a cogência lógica tem (se reconhecida) uma eficácia persuasiva em si mesma, à qual a força (psicogénica) das várias formas de simetrização pode acrescentar-se, mas não substituir-se.

As relações lógicas entre os dados utilizados ligam os vértices de estruturas complexas, que incorporam miríades de associações latentes entre dados e avaliações que habitualmente permanecem inexpressas, mas que por vezes reemergem e, de vários modos e por várias razões, se inserem sub-repticiamente nas articulações do discurso explícito.

Este reservatório de informação e conexões fornece o material necessário para o exercício da *ars distinguendi*, uma arte natural, porque ligada à atitude espontânea da mente de associar e dissociar noções e juízos, que se refina com a experiência nos vários campos do conhecimento e da prática.

A *ars distinguendi* tem valor em todas as áreas do conhecimento, mas no direito, em particular, constitui um exercício constante e necessário para apreender a especificidade dos casos e evitar as inconsistências que derivam de tratar situações dissemelhantes de modo semelhante, isto é, diferenciáveis com base num princípio jurídico relevante para o caso ou com base numa hipótese diferente de reconstrução dos factos.

A busca de razões para excluir o que foi admitido como semelhança e transformá-lo numa diversidade essencial pode depender dos diferentes níveis de análise: dois objetos podem parecer semelhantes a um nível, mas a outro podem diferir.

Na realidade, a "árvore de Porfírio" (a das ramificações conceptuais) pode desenvolver-se de diferentes modos e de diferentes modos se pode subir ou pousar nos seus ramos. O impulso intelectual que leva a associar ou dissociar noções nasce de uma opção no âmbito da psicologia e da formação cultural do intérprete, que pode traduzir-se num dado juridicamente relevante se estiver ancorada a circunstâncias factuais

significativas em relação aos dados normativos (especialmente os princípios) oferecidos pelo ordenamento jurídico.

A *ars distinguendi* é a base dos argumentos mais importantes que se desenvolvem no campo jurídico: para resolver as incompatibilidades entre dados normativos (quando os critérios legislativos para a resolução de antinomias não ajudam), para rejeitar uma interpretação anterior, para encontrar uma exceção, para afastar uma máxima de experiência comum. A interpretação rigorosa pode aumentar a incerteza jurídica, porque levanta novos problemas ao revelar complexidades inesperadas, mas beneficia a Justiça[3].

III. RACIONALIDADE ARTIFICIAL E RACIOCÍNIO JURÍDICO

Tal como a transição do pré-consciente para o pensamento discursivo implica uma redução dos dados e correlações que podem ser conscientemente utilizados, também a transição da argumentação para as cristalizações dos significados dos termos e das inferências que se alcança com os métodos da inteligência artificial implica um empobrecimento adicional do raciocínio, devido a simplificações e mecanizações que podem ser úteis desde que quem as utiliza se mantenha vigilante quanto aos limites dos instrumentos de que faz uso.

Em particular, os algoritmos com racionalidade artificial prestam-se a ser utilizados em várias áreas de interesse para decisões juridicamente relevantes, mas (no estado atual do seu desenvolvimento) não conseguem seguir caminhos que vão além das diretrizes da lógica formal para entrar no campo da argumentação.

A inteligência artificial não pode substituir o jurista, mas pode fornecer-lhe auxílios.

A. SISTEMAS PERICIAIS DEDUTIVOS FIÁVEIS

Os algoritmos oferecem os melhores e menos problemáticos resultados quando produzem sistemas periciais – aqueles que operam segundo uma lógica inteiramente controlada por quem os concebe e pelo utilizador que (estudando e atualizando-se) é capaz de compreender o seu funcionamento, de modo a utilizá-los como instrumentos de apoio a operações que também poderia completar por si próprio.

Os modelos lógicos que governam os sistemas periciais baseiam-se em regras centradas na conexão inferencial entre antecedente e consequente (se... → então...). Há anos que existem aplicações práticas úteis para acelerar operações baseadas numa lógica dedutiva, como, por exemplo, entre as mais simples: o cálculo da prescrição de crimes ou a quantificação de indemnizações ou compensações por danos com base em critérios predeterminados.

Além disso, a informática jurídica pode ajudar a descobrir procedimentos pseudológicos: introduzindo no itinerário jurídico cânones de correção ou, pelo menos, de transparência da impropriedade. Isto aplica-se tanto à análise de textos legislativos (à sua redação e às inferências que deles se podem extrair) como à análise de sentenças e medidas administrativas (quanto aos seus conteúdos e às inferências que deles se podem extrair). Os diferentes critérios interpretativos e inferenciais podem conduzir a uma pluralidade de resultados plausíveis, mas nem todos esses resultados derivam de operações intelectuais que respeitam os princípios da lógica formal.

Para este efeito pode ser utilizado o **direito computacional**, que diz respeito à representação de factos e regras através da lógica formal e ao uso de técnicas de raciocínio mecânico para derivar as consequências de factos e regras tal como representados através de proposições formalizadas. A principal limitação atual do **direito computacional** é a mesma da lógica computacional geral: não vai além do **cálculo proposicional**, isto é, do "cálculo lógico" em que a análise das inferências é conduzida ao nível das

[3] Quintilianus, *Institutio oratoria*, II, XIII, 1.

proposições sem investigar a estrutura interna das próprias proposições.

Mesmo com esta limitação, alguns algoritmos poderiam ser proveitosamente utilizados para verificar a correção lógica de uma parte dos argumentos relativos à prova dos factos, identificando falácias formais no raciocínio e, em primeiro lugar, a sua manifesta ilogicidade.

Para este fim, contudo, é necessária uma purificação da linguagem com que os argumentos probatórios são expressos, de modo a cuidar adequadamente da sua forma lógica e torná-los tratáveis por programas que utilizam *sistemas lógicos periciais*, o que implica uma evolução cultural na formação dos juristas para os habilitar a explorar este potencial.

B. MÁQUINAS INTELIGENTES INEXPERIENTES E ARMADILHAS DA LÓGICA INDUTIVA

O funcionamento de algoritmos abertos à aquisição de informação, para além daquela com que são equipados como premissas iniciais, através de formas de aprendizagem automática pelos próprios sistemas. Baseia-se em generalizações extraídas de casos (avaliados como) semelhantes.

Estes algoritmos não têm a capacidade de considerar adequadamente as circunstâncias de cada caso concreto, também porque, em qualquer caso, não são capazes de obter toda a informação que seria necessária.

As redes neuronais visam superar estas limitações por meio de estratégias de adaptação flexível ao ambiente, com uma paródia do sistema neural animal. Mas a incerteza permanece inerente aos sistemas baseados em aprendizagem automática, que não permite excluir que o novo caso examinado, embora semelhante aos anteriores nas características consideradas pela rede, não se ajuste à previsão. Esta condição não é resolvida, podendo mesmo ser agravada, pela possibilidade de tais sistemas (que, portanto, se revelam inexperientes) utilizarem grandes massas de dados como exemplos dos quais extrair correlações e generalizações. Além disso, ao contrário de uma árvore de decisão em que se centra um sistema pericial, a rede neuronal não fornece diretamente explicações compreensíveis para os seus resultados, pelo que é comparável a uma caixa negra desprovida, por definição, de transparência.

C. INTELIGÊNCIA ARTIFICIAL E RACIONALISMO DIALÉTICO

O modelo de argumentação traçado para o raciocínio probatório em julgamento inspira-se no racionalismo dialético e, nesta direção, a *Carta de Ética sobre o uso da inteligência artificial nos sistemas judiciais e seu ambiente*, adotada em 3 de dezembro de 2018 pela Comissão Europeia para a Eficiência da Justiça (CEPEJ), exige coerência **lógica** dos cálculos algorítmicos num processo decisório em conformidade com os princípios do direito processual. Por outras palavras, o resultado algorítmico deve ser corroborado por prova que é elaborada segundo o método dialético e que requer intervenção humana.

Dentro de algum tempo, será também possível desenvolver uma nova lógica formal (mais ampla do que os modelos dedutivos tradicionais) para conceber modelos de raciocínio jurídico (não redutíveis a meros silogismos) e projetar sistemas periciais capazes de apreender a dialética de argumentos opostos e de utilizar técnicas para os atacar e refutar. Trata-se de formalizar o chamado raciocínio derrotável (*defeasible reasoning*), isto é, o raciocínio que é convincente, mas que não é dedutivamente válido porque poderia ser desmentido por exceções específicas e, portanto, sujeito a refutação[4].

Menos facilmente previsíveis parecem ser sistemas formais capazes de avaliar (por si mesmos) o peso dos argumentos, porque a força de um argumento depende também do contexto em que se insere e o contexto depende de circunstâncias mutáveis.

[4] Sobre estes aspetos: G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, Giappichelli, 2022, pp. 44-45 103-122.

Em todo o caso, permanece o facto de que, de momento, os vários sistemas de inteligência artificial – quando se ultrapassa um certo limiar de complexidade das questões – não são capazes de oferecer o que a inteligência humana pode fácil e corretamente produzir (se bem educada e se habituada a monitorizar os seus estados mentais). Assim, é claro que se recorre a resultados de aplicação de elaborações teóricas que são interessantes pelos seus possíveis desenvolvimentos aplicativos futuros, mas ainda embrionárias.

Entretanto, parece necessário fornecer a quem se dedica à produção do direito e a quem trata da sua aplicação os instrumentos intelectuais necessários para manter o controlo da situação **em curso** e utilizar proveitosamente os contributos da inteligência artificial. O que esta reserva para o futuro, na parte em que é previsível, tem limites que são fonte de perplexidade. Contudo, para além de muitas das suas antecipações imaginativas, em certa medida as mudanças terão lugar. Se forem muito rápidas, só se tomará plena consciência dos seus efeitos depois de estes terem ocorrido. Basta pensar nas consequências (principalmente, mas não exclusivamente, positivas) do uso da informática para a documentação jurídica que, aliás, apesar da sua amplitude, permanece conceptualmente controlável pelos seus utilizadores.

O que é necessário entretanto, porém, é uma recomposição ponderada dos vários ensinos universitários relativos à informática jurídica com os seus crescentes desenvolvimentos[5] ramificados, de modo a incluí-la entre as componentes das renovadas artes *sermocinales*, para que estas, a partir das tradicionais (e hoje negligenciadas) artes do *trivium* (gramática, retórica, dialética), se expandam para instrumentos interdisciplinares modernos, tais como, segundo alguns, poderiam ser: os fundamentos da linguística geral, a lógica com as suas ramificações na informática e no cálculo de probabilidades, a metodologia.

IV. FALÁCIAS LÓGICAS E CIBERSEGURANÇA

Na **infosfera**, a informação flui sem interrupção através de redes informáticas: desde dados pessoais e bancários até segredos industriais e militares, um vasto leque de informação sensível torna-se alvo de conquista e/ou defesa.

A. INFOSFERA E SERVIÇOS SECRETOS

As **agências de informação** utilizam a IA para gerir e interpretar quantidades massivas de dados provenientes de diferentes fontes – incluindo comunicações digitais, sensores eletrónicos, *dark web*, *trojans*, várias formas de *malware*, bem como informação recolhida junto de pessoas – para prevenir ameaças à segurança nacional, identificando padrões, anomalias e potenciais ameaças que são difíceis de descobrir manualmente[6].

Através da IA, as reações a incidentes de segurança podem ser automatizadas e tornadas muito rápidas. Sistemas inteligentes podem bloquear autonomamente endereços suspeitos, colocar em quarentena dispositivos infetados ou iniciar contramedidas com base em regras predefinidas.

O uso de drones, geolocalização por GPS e dispositivos ligados à *internet*, integrados com IA, permite uma vigilância em tempo real mais precisa e generalizada.

A IA também transforma a contra-espionagem, ajudando a reconhecer falsificações de áudio e vídeo (*deepfakes*) e a combater a contrafação mediática, um fenómeno cada vez mais utilizado para desinformar ou manipular. As plataformas *online*, geridas por privados, bem como os grandes modelos de linguagem (LLM), podem ser utilizados para influenciar escolhas e estratégias individuais e coletivas ou para veicular mensagens encriptadas ou esteganográficas.

[5] Para uma exposição histórica da relação entre a informática jurídica e a formação do jurista: G. Ciacci-G. Buonomo, *Profili di informatica giuridica*, Milano, Wolters Kluwer, 2021, pp. 19-30.

[6] L. Floridi, *Pensando all'infosfera. La filosofia come design concettuale*, Milano, Raffaello Cortina, 2020.

Embora, ao automatizá-las, torne as operações mais rápidas e precisas, a IA também levanta novas questões éticas e de confidencialidade, e apresenta igualmente riscos de resultados falaciosos e enganadores[7].

B. PADRÕES, INCERTEZAS E ANOMALIAS

A relação entre IA e cibersegurança é ambivalente, porque a IA representa tanto um aliado poderoso na ciberdefesa como um recurso para os atacantes, através da sua capacidade de analisar grandes volumes de dados para identificar padrões e detetar anomalias.

Em particular, a IA analisa quantidades massivas de dados em frações de segundo, detetando anomalias e comportamentos suspeitos com maior precisão do que os métodos tradicionais.

O conhecimento dos padrões de comportamento normal é fundamental para prevenir ameaças mais avançadas (como tentativas de personificação de pessoas de alto perfil dentro de organizações). Ao analisar uma vasta quantidade de dados, a IA permite identificar correlações que seriam difíceis de reconhecer e que podem ser vistas como indícios de potenciais ataques. Em resumo, a IA estabelece **padrões de normalidade** através da aprendizagem contínua a partir de dados e depois deteta qualquer desvio desse padrão como uma anomalia, que pode sinalizar uma potencial ciberameaça.

Contudo, se a *machine learning* pode permitir a identificação precoce de uma ameaça, o problema seguinte é como responder prontamente à ameaça, tendo também em conta a possibilidade de falácias na análise de dados.

A inteligência artificial é, portanto, uma espada de dois gumes na cibersegurança: pode reforçar as defesas, mas também tornar as ofensivas mais sofisticadas, reduz algumas incertezas, mas pode também gerar outras.

Os seus instrumentos, nas suas várias formas, desde os sistemas periciais – baseados na lógica dedutiva – até às máquinas inteligentes – que funcionam segundo algoritmos governados pela lógica indutiva, correlações e cálculo probabilístico – são mentalmente (eletronicamente) vivos, mas podem revelar-se intelectualmente preguiçosos e não tão racionais como as mentes humanas (individuais ou coletivas) podem ser, quando atuam em condições de serenidade e sem limitações de tempo, de modo a tomar decisões informadas, avaliando objetivamente a informação disponível e as possíveis consequências das suas ações.

A capacidade da IA de resolver problemas específicos com base em procedimentos aprendidos e memorizados – eventualmente adaptando-se a novas situações, desenvolvendo modelos abstratos e tomando algumas decisões – pode, contudo, ser induzida em erro por **vieses** (enviesamentos, que conduzem a perspetivas enganadoras) e falácias (usos incorretos de inferências lógicas)[8].

As falácias lógicas podem até ser úteis porque permitem a expansão do conhecimento e podem conduzir – ainda que de modos logicamente imperfeitos – a conclusões verdadeiras, aumentando a informação (como é típico da lógica indutiva e abdutiva e das suas projeções probabilísticas). Mas contêm riscos. Por isso, nos vários campos, em relação aos diferentes problemas, é necessária uma ponderação calibrada – levada a cabo por escolhas humanas – sobre o nível de risco aceitável na relação entre os perigos ligados às falácias, a exatidão lógica, a rapidez e a rentabilidade dos resultados.

Da parte das pessoas, as falácias são mais difíceis de gerir em condições de incerteza e quando as decisões precisam de ser tomadas com urgência. Nestas condições, os indivíduos são guiados por uma racionalidade limitada, que os leva, devido a vários condicionamentos externos e internos, a decidir não segundo cânones lógicos ótimos, mas seguindo o caminho que melhor satisfaz

[7] A. Costanzo, *Fallacie logiche e cybersecurity*, in: *Diritto di Internet*, 2025, pp.649-657.

[8] A. Costanzo -S. Novani, *La logica dell'analisi e della sintesi dei dati processuali*, Torino, Giappichelli, 2025.

as suas necessidades no contexto dos recursos, do conhecimento (limitado) e do tempo em que atuam.

Por isso, em condições de incerteza, na presença de riscos potenciais graves e pouco tempo para refletir, o uso de procedimentos algorítmicos – que são desenvolvidos com base em modelos bem pensados – pode servir para evitar condicionamentos emocionais e, como precaução, em contextos de segurança informática, para adotar escolhas defensivas urgentes que não sejam irracionais, evitando custos no caso de ameaças aparentes e riscos adicionais no caso de reações agressivas a ameaças aparentes.

V. POSSÍVEIS "FALÁCIAS INFERENCIAIS" OU DE EQUIVOCAÇÃO EM ALGORITMOS DEDUTIVOS

Obviamente, os sistemas periciais dedutivos [III. A.], uma vez que por natureza não desenvolvem inferências amplificadoras, não geram conhecimento novo para além das premissas iniciais, ainda que tenham o mérito de poder estender todas as derivações e, se solicitado, tornar todas as passagens transparentes.

Por isso, não são adaptáveis a cenários não predefinidos. São rigorosos, mas intrinsecamente limitados na gestão de ambiguidades e contextos dinâmicos, porque requerem integrações com **lógicas não monotónicas**, que permitem introduzir exceções às regras inferenciais. Em resumo, as **lógicas não monotónicas** são fundamentais para representar o raciocínio **derrotável** ou tentativas de inferências que podem ser retratadas à luz de nova informação, como acontece no raciocínio indutivo, nas explicações abdutivas e na revisão de crenças. São fundamentais em todas as áreas onde o raciocínio deve ser flexível, atualizável e capaz de lidar com exceções e mudanças no conhecimento, gerir a incerteza, o conhecimento incompleto ou mutável e o raciocínio que pode ser modificado por nova informação.

A sua validade depende do contexto para o qual foram feitos; se este muda, tornam-se obsoletos e, em campos onde as mudanças são ordinárias e rápidas, os sistemas periciais requerem revisões contínuas, de modo que, se emerge um erro ou uma aproximação inaceitável, devem ser radicalmente revistos ou postos de lado.

As falácias lógicas representam um risco significativo no raciocínio automatizado complexo porque são armadilhas.

Eis as principais.

Os sistemas computacionais baseados na lógica dedutiva (silogística ou expressa com inferências condicionais) podem incorrer em falácias lógicas específicas, principalmente relacionadas com erros ocasionais na aplicação de regras inferenciais ou, mais facilmente e sub-repticiamente, com a equivocação de significados derivada do uso ambíguo de termos.

Sistemas inferenciais complexos podem, por erros na sua conceção, incorrer nas **falácias do condicional**: na **falácia da afirmação do consequente**, que infere o antecedente a partir do consequente (se P então Q; Q é verdadeiro; logo, P é verdadeiro); na **falácia da negação do antecedente, que infere da exclusão do antecedente a negação do consequente** (se P então Q; P é falso; logo, Q é falso).

As falácias baseadas na **equivocação dos significados** dos termos podem – usando metáforas derivadas da mecânica – comprometer as engrenagens do percurso informático, tornando-as oscilantes ou mesmo completamente desconjuntadas.

Podem então conduzir a erros inesperados, o que torna o algoritmo não fiável porque anuncia decisões erradas ou disfunções.

Um exemplo disto é a **falácia da *quaternio terminorum*** nos silogismos.

Um silogismo válido deve ter apenas três termos ligados entre si; quando um quarto é introdu-

zido, a conclusão não é logicamente sustentada pelas premissas.

Isto acontece porque os sistemas computacionais não "compreendem" o conteúdo, mas aplicam mecanicamente as regras: os mal-entendidos não são reconhecidos e alimentam falácias. Isto pode resultar numa propagação de erros em cadeias sucessivas de inferências, que comprometem todo o processo decisório e reduzem a fiabilidade do sistema[9].

VI. AS FALÁCIAS INERENTES À LÓGICA INDUTIVA E ÀS MÁQUINAS INTELIGENTES

O funcionamento de algoritmos (não determinísticos) abertos à aquisição de informação, para além daquela com que são providos como premissas iniciais, realiza-se através de formas de aprendizagem automática pelos sistemas que os utilizam.

Mesmo com uma certa simplificação, pode dizer-se que as máquinas inteligentes operam estabelecendo correlações segundo uma lógica indutiva e probabilística.

A. CORRELAÇÕES E CONEXÕES

A identificação de correlações entre dados específicos é uma fase fundamental que precede e sustenta a generalização indutiva e consiste na análise de dados para identificar padrões, modelos ou relações recorrentes entre variáveis ou fenómenos.

As IA são particularmente aptas a detetar semelhanças (e, inversamente, diferenças), agrupando dados semelhantes em *clusters*.

Identificam correlações entre miríades de dados, mesmo quando estas não são detetáveis pelo analista humano, principalmente através de algoritmos de *machine learning*, e procuram maximizar a precisão das previsões ou classificações com base em cálculos probabilísticos.

Por isso, as correlações nem sempre correspondem a conexões reais (muito menos a relações causais reais) e são influenciadas pela qualidade e representatividade dos próprios dados.

Além disso, não deve ser negligenciada a possibilidade de correlações espúrias: associações aleatórias ou devidas a fatores externos que não implicam um verdadeiro nexo causal.

Estas correlações representam a base empírica sobre a qual se funda a generalização indutiva (inferência "do particular para o geral") com projeções probabilísticas, que é também uma forma de previsão, mas pode revelar lacunas inesperadas e prejudiciais.

Assim, a incerteza permanece inerente aos sistemas de *machine learning*, que não permite excluir que o novo caso examinado, embora semelhante aos anteriores, não se ajuste à previsão.

Além disso, ao contrário de uma árvore de decisão em que se centra um sistema pericial, a rede neuronal não fornece diretamente explicações compreensíveis para os seus resultados, pelo que é comparável a uma *black box* sem transparência.

Acima de tudo, estes algoritmos não têm a capacidade de considerar adequadamente as circunstâncias de cada caso concreto, também porque, em qualquer caso, não são capazes de obter toda a informação que seria necessária.

Por isso, não são capazes de formular o **juízo reflexivo**, o (tipicamente humano) que extrai das circunstâncias específicas do caso concreto o critério para a resolução do problema[10].

[9] Isto não impede que muitos termos sejam intrinsecamente indeterminados ou que tenham um núcleo central bem definido e franjas periféricas mais ou menos indeterminadas. Contudo, quando (como por vezes é inevitável) se introduzem nos algoritmos premissas que veiculam termos não plenamente determinados, é importante ter consciência disso para não incorrer nas várias **falácias de equivocação**.

[10] A. Costanzo, *Intelligenza artificiale e logica giuridica*, in: *Macchine intelligenti e diritto* (G. Ciacci- G. Buonomo- A. Costanzo), Torino, Giappichelli, 2025, pp.93-96.

B. FALÁCIAS DA LÓGICA INDUTIVA: GENERALIDADES E GENERALIZAÇÕES

Quando a IA estabelece correlações entre miríades de dados, pode incorrer em várias falácias lógicas e **vieses cognitivos, principalmente devido à natureza dos dados e ao modo como processa a informação**.

A lógica da generalização indutiva visa expandir o conhecimento, pelo que deve coexistir com as falácias do condicional (em particular a da afirmação do antecedente), que permanecem como tal na lógica dedutiva, mas que, por outro lado, são a base da lógica indutiva (na qual as conclusões veiculam informação (que poderia revelar-se falsa) maior do que a oferecida pelas premissas).

Por isso, o risco da confusão falaciosa entre generalidade e generalização, inerente à tendência de atribuir o caráter de generalidade ao que poderia revelar-se mera generalização indevida, permanece constante, tanto mais quando se procede por caminhos não supervisionados pelo rigor do método científico.

As inferências (necessárias) que amplificam informação, produzem informação nova (talvez verdadeira, talvez falsa), são úteis, desde que se mantenha a vigilância intelectual sobre a sua fragilidade.

No uso das variadas expressões da lógica indutiva, podem surgir falácias macroscópicas.

A generalização indevida (ou *secundum quid*, ou acidente **converso**, ou **generalização apressada**) apresenta o que é verdadeiro em alguns casos como se fosse verdadeiro para todos os casos, ou uma conclusão relativa a uma classe inteira de objetos a partir de premissas relativas apenas a um ou alguns dos seus componentes, e consiste em derivar uma regra geral de prova inadequada, seja porque se refere a um caso especial, seja porque a amostra considerada não é representativa. Na forma de **generalização estatística**, baseia-se na amostragem, mas pretende ter uma conclusão geral: a probabilidade estatística, entendida como frequência estatística, não pode sustentar um raciocínio inteiro, mesmo que indique uma probabilidade elevada, porque lida com frequências e, portanto, admite exceções, de modo que não se ajusta à reconstrução de eventos singulares.

A falácia da **falsa causa** faz parecer como causa de um evento algo que não o é, ou atribui arbitrariamente uma determinada causa a um evento sem ter considerado as concausas ou possíveis causas alternativas. Os instrumentos atuais de racionalidade artificial que detetam **regularidades** entre os dados recolhidos não são eficazes na identificação de relações causais entre fenómenos em relação a um caso específico: de modo que o resultado algorítmico deve, em qualquer caso, ser corroborado por prova que é processada segundo o método dialético e que requer intervenção humana para assegurar a **coerência lógica global** do raciocínio.

No uso da lógica abdutiva, a **avaliação atomística dos indícios** é falaciosa porque ignora o facto de que o indício – pela sua constituição – é um dado cuja ambiguidade deve ser emendada ligando-o a outros. Furtar-se a esta operação é pôr indevidamente de lado elementos relevantes de avaliação que poderiam, em última análise, revelar-se mesmo decisivos e, portanto, falhar por defeito. Pelo contrário, a *praesumptio de praesumpto* parte de um facto conhecido (indício) para remontar a um desconhecido e depois, colocando o facto (originalmente) desconhecido como fonte de uma presunção ulterior, faz o indício perder precisão, mas poderia fornecer perspetivas úteis ao conhecimento, se examinado com um método adequado no contexto de uma avaliação não atomística dos dados (esta operação não é admitida pela jurisprudência).

VII. FALÁCIAS NO USO DAS CONCLUSÕES

Algumas falácias dizem respeito ao uso das conclusões.

Na **falácia da conjunção**, o valor informativo de dados semelhantes é sobrestimado, violando frequentemente a teoria da probabilidade, porque eventos conjuntos são erroneamente consi-

derados mais prováveis do que eventos descritos individualmente. Em particular, na **falácia do suporte**, eventos sustentados por uma descrição mais rica em dados específicos são considerados mais prováveis do que os propostos com um suporte descritivo mais limitado, enquanto, pelo contrário, a riqueza de detalhe da descrição, que torna o evento mais específico, deveria, do ponto de vista estatístico, reduzir a probabilidade da sua ocorrência e tornar cauteloso em relação a **correlações ilusórias**.

Alguns vieses típicos dos algoritmos ou do modo como são utilizados também recorrem. Muitos algoritmos são configurados para procurar toda a informação que possa confirmar a hipótese inicial, enquanto dados e hipóteses dissonantes são deixados de fora até se **estabelecer** a chamada **visão de túnel**, que mostra apenas o que confirma a hipótese inicial (viés de confirmação); outra distorção ocorre quando dados importantes são excluídos porque o programador não viu fatores novos e importantes (viés de exclusão).

Mesmo a confusão entre **mera derivação** (condição necessária) e consequência (condição necessária e suficiente) constitui uma falácia lógica que pode entrelaçar-se com a propensão psicológica para uma busca apressada e/ou injustificada de conclusões, introduzindo premissas adicionais na árvore do raciocínio. No caso da IA, seja por mal-entendidos ou aproximações de correlações probabilísticas, uma **mera derivação** poderia ser tratada como uma consequência.

A **falácia da falsa dicotomia** deriva de confundir meros antónimos com contraditórios, supondo erroneamente que só podem existir duas hipóteses explicativas plausíveis de um facto, de modo que a refutação de uma conduziria necessariamente à verdade da outra, esgotando o espaço lógico da questão, quando na realidade, no caso de hipóteses que são apenas *contrariae*, *tertium datur*, de modo que ambas poderiam ser falsas.

O viés de coesão consiste na busca de coesão mesmo quando o resultado de coerência não é racionalmente justificado porque se baseia em dados incompletos, quando deveriam ser examinadas hipóteses reconstrutivas alternativas.

A questão é que, em situações de incerteza e ambiguidade na reconstrução de dados factuais, existe uma propensão para formular hipóteses para criar narrativas que expliquem os eventos, preenchendo as lacunas nos dados. Nesta perspetiva, além disso, são favorecidas cadeias causais curtas em detrimento de mais longas e construções contrafactuais mais facilmente disponíveis à mente.

Igualmente, vale a propensão para se ancorar à primeira informação disponível, ao enquadramento inicial, e depois fazer ajustamentos. Apesar de ter uma compreensão parcial, assume-se que se pode ter cognição total e tende-se a tornar os dados consistentes e coesivos com a base inicial em *stock*. Depois, os dados são todos colocados ao mesmo nível para serem tornados coerentes, negligenciando a sua diferente relevância e compreensão diacrónica.

Em alguns casos, tenta-se salvar o trabalho feito de modo que – especialmente quando é urgente decidir e as alternativas possíveis são duvidosas – os esforços despendidos não sejam desperdiçados e assim se cai na **falácia dos custos afundados**.

Uma vez que a reconstrução de um facto resulta também da composição das relações lógicas entre certos eventos, quando esta composição é afetada por falácias ou representações erróneas, o facto é substituído por um "factoide".

VIII. ESTRATÉGIAS DE PROGRAMAÇÃO DE UMA IA PARA RECONHECER ERROS DE RACIOCÍNIO

Porque não tem pensamento crítico nem autoconsciência, a IA atual não consegue reconhecer ou corrigir erros lógicos ou vieses por si própria, e o aumento contínuo dos dados analisados

pode ocultar erros e vieses mais profundos que são difíceis de detetar e corrigir.

Para programar uma IA capaz de reconhecer erros de raciocínio, são adotadas várias estratégias, entre as quais as mais proveitosas parecem ser as que adotam uma abordagem analítica:

a) **Aprendizagem supervisionada com *feedback* passo a passo**: o modelo é treinado com exemplos de raciocínio correto e incorreto, fornecendo *feedback* sobre cada passo individual. Isto ajuda a IA a identificar onde se escondem os erros lógicos e a corrigi-los durante o processo de inferência. Quando se utiliza um modelo supervisionado, são os especialistas na área que selecionam os dados de treino: é crucial que o seu grupo seja diverso e que tenham recebido formação adequada para ajudar a prevenir vieses inconscientes;

b) **Raciocínio passo a passo**: a IA é treinada para raciocinar passo a passo, tornando explícita cada etapa do raciocínio. Em vez de fornecer apenas a resposta final, a IA decompõe o problema numa sequência lógica de passos intermédios, tornando o itinerário decisório transparente, de modo que programadores e utilizadores possam verificar a consistência interna do raciocínio, facilitando a deteção de inconsistências ou passagens inválidas. Ou, para o mesmo problema, a IA pode ser induzida a gerar múltiplas cadeias de raciocínio, de modo a reduzir, pela sua comparação, a influência de erros aleatórios ou inferências erróneas.

Atualmente, os **sistemas híbridos**, aqueles que utilizam tanto o juízo humano como a inteligência artificial, tendem a minimizar a possibilidade de viés e, portanto, a garantir os melhores resultados. Embora seja verdade que os algoritmos podem trazer maior rigor e repetibilidade a um processo e são capazes de procurar e remover vieses devidos a erro humano, é igualmente verdade que os humanos são capazes de avaliar situações num contexto mais amplo, acrescentando capacidade crítica, competências de investigação e compreensão do processo decisório. Assim, os sistemas em que a IA oferece opções ou recomendações para avaliação humana são ótimos.

Finalmente, a **estratégia de cultivar a hipótese contrária** (também praticável com ferramentas de IA) pode reduzir os efeitos negativos dos vieses, ancoragens, efeitos de túnel, especialmente o viés de confirmação[11], por vezes induzido pela formulação do *prompt*.

Podem ser introduzidos alertas nos algoritmos para solicitar a consideração de uma hipótese contrária (talvez gerada pelo próprio algoritmo, com base na heurística lógica).

Contudo, tanto os sistemas periciais como os sistemas baseados em correlações de dados não parecem ter, atualmente, uma capacidade dialética significativa para examinar pressupostos e hipóteses alternativas em relação àquelas com que trabalham[12].

[11] S. van Brussel, M. Timmermans, P. Verkoeijen, F. Paas, *Consider the Opposite Effects of Elaborative Feedback and Correct-Answer Feedback on Reducing Confirmation Bias*, in: *Contemporary Educational Psychology*, 60, 101844, 2020.

[12] D. Andler, *Artificial Intelligence, Human Intelligence: The Double Enigma*, Gallimard, Paris, 2023.

UMA GRANDE QUESTÃO PARA MICRO E PEQUENAS EMPRESAS: A DELIMITAÇÃO SUBJETIVA DA DIRETIVA SRI 2 E DO DECRETO-LEI N.º 125/2025, DE 4 DE DEZEMBRO

ANA XAVIER NUNES
Associada da Morais Leitão

A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 (SRI 2)[1] e o Decreto-Lei n.º 125/2025, de 4 de dezembro[2] (Decreto-Lei n.º 125/2025) (conjuntamente, "diplomas"), partem de um critério aparentemente simples: ficam abrangidas, em regra, desde que respeitados os critérios de âmbito territorial previstos, as médias empresas e as empresas que excedam os limiares relativos às médias empresas (ou "grandes empresas") que operem nos setores identificados pelo regime e prestem os seus serviços ou exerçam as suas atividades na União Europeia[3].

O critério quantitativo relevante resulta da remissão expressa para a definição europeia de micro, pequenas e médias empresas (PME) constante da Recomendação 2003/361/CE, de 6 de maio de 2003. Nos termos do respetivo artigo 2.º, n.º 1, a categoria das PME é constituída por empresas que empreguem menos de 250 pessoas e cujo volume de negócios anual não exceda 50 milhões de euros ou cujo balanço total anual não exceda os 43 milhões de euros[4].

Porém, a previsão do âmbito de aplicação subjetivo ainda é longa, e só uma leitura mais apressada poderia levar à conclusão de que as micro e pequenas empresas cairiam fora do seu alcance, pelo que se impõe, em qualquer caso, uma análise aprofundada, incompatível com uma aplicação acrítica[5].

A aparente centralidade do critério quantitativo é mitigada por um conjunto de exceções consagradas pela SRI 2 e concretizadas pelo Decreto-Lei n.º 125/2025 ao prever que determinadas entidades possam ficar abrangidas «[...] independentemente da sua natureza e dimensão e respeitados os critérios de âmbito territorial [...]». Assim, os referidos diplomas admitem que certas entidades sejam qualificadas como essenciais ou importantes em função da sua relevância material, ainda que não atinjam os limiares típicos de média ou grande empresa.

1 Relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.

2 Transpõe a SRI 2 para o ordenamento jurídico nacional.

3 Reportamo-nos exclusivamente às entidades empresariais. Não nos debruçaremos sobre a aplicação do Decreto-Lei n.º 125/2025 à Administração Pública, às entidades públicas integradas na estrutura institucional do Estado e às instituições de ensino superior, cuja sujeição ao regime é direta e independente do critério da dimensão (*cf.* artigo 3.º. n.os 3, 4 e 6, do referido diploma).

4 Nos termos da Recomendação 2003/361/CE, de 6 de maio, considera-se microempresa a que emprega menos de dez pessoas e cujo volume de negócios anual ou balanço total anual não excede dois milhões de euros; pequena empresa a que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede dez milhões de euros; média empresa a que empregue menos de 250 pessoas e cujo volume de negócios anual não exceda 50 milhões de euros ou cujo balanço total anual não exceda 43 milhões de euros. São consideradas grandes empresas as que ultrapassem os limiares aplicáveis às médias empresas.

5 Com uma formulação não inteiramente coincidente (e, em certos segmentos, num ou noutro diploma, menos linear) o âmbito de aplicação subjetivo encontra-se previsto, respetivamente, no artigo 2.º da SRI 2 e no artigo 3.º do Decreto-Lei n.º 125/2025.

Em termos gerais, esta prevalência do critério material ocorre quando esteja em causa uma atividade intrinsecamente crítica e estrutural para o funcionamento da economia e da sociedade, a nível nacional ou regional. Pense-se, desde logo, nos operadores de comunicações eletrónicas, nos prestadores de serviços de confiança digital ou nas entidades ligadas à gestão de *Domain Name System* (áreas cuja vulnerabilidade acarreta um impacto imediato e transversal).

Por outro lado, a dimensão deixa também de ser determinante quando a entidade desempenha um papel insubstituível ou altamente significativo num determinado setor, seja por constituir o único prestador de um serviço essencial, seja pelo impacto que a perturbação do serviço possa ter na segurança, proteção ou saúde públicas, pela possibilidade de gerar riscos sistémicos consideráveis, ou ainda pela sua importância específica, a nível nacional ou regional, para o setor, tipo de serviço ou setores interdependentes. A lei contempla ainda situações em que a entidade já foi previamente identificada como crítica[6].

A delimitação subjetiva exige, por isso, não apenas a verificação de limiares quantitativos, cujo critério da dimensão empresarial constitui a regra numa primeira aproximação, mas também uma apreciação substantiva do impacto potencial da atividade exercida, o que implica uma avaliação casuística que atua como mecanismo de inclusão excecional, mas nem por isso menos expressivo.

A exclusão do âmbito subjetivo não significa, contudo, imunidade ao regime. Os diplomas impõem às entidades abrangidas deveres expressos de gestão do risco da sua *supply chain* (ou cadeia de abastecimento)[7]. Isso significa, por exemplo, que uma média ou grande empresa sujeita ao regime terá de assegurar que os seus prestadores e fornecedores adotam níveis adequados de segurança, podendo, para o efeito, impor-lhes exigências contratuais acrescidas em matéria de cibersegurança e ciber-resiliência.

Deverá, por isso, a entidade (não abrangida) que preste serviços a uma entidade sujeita ao regime adotar e ser capaz de demonstrar a existência de políticas adequadas de segurança, planos de resposta a incidentes, mecanismos de controlo de acessos, procedimentos de auditoria, entre outros. Ignorar esta realidade pode originar vários tipos de riscos, que não se esgotam na contribuição para a propagação de incidentes com impacto em terceiros, podendo ainda traduzir-se na não adjudicação de contratos por entidades abrangidas, com fundamento na falta de conformidade nesta matéria.

Assim, ainda que as micro e pequenas empresas não se encontrem, em função da sua dimensão, formalmente abrangidas pelas obrigações em matéria de cibersegurança, deverá considerar-se que, operando em ecossistemas críticos, o impacto regulatório lhes chegará, no mínimo, por via contratual.

Mas acresce ainda um fator adicional. Uma entidade que, isoladamente considerada, preencha os requisitos para ser qualificada como micro ou pequena empresa, poderá perder esse estatuto, para efeitos de aplicação do regime, se integrar um grupo empresarial que, em termos agregados, ultrapasse os limiares referidos[8]. A aferição da dimensão para efeitos de aplicação do regime não será, à partida, exclusivamente individual, exigindo-se uma análise consolidada da estrutura societária e das relações de controlo ou participação existentes, independentemente

[6] À luz da Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas.

[7] É o caso, designadamente, da previsão do artigo 21.º, n.º 2, alínea *d*), da SRI 2, bem como do artigo 28.º do Decreto-Lei n.º 125/2025. Quanto à gestão da *supply chain*, assumem particular relevância, entre outros, o Regulamento de Execução (UE) 2024/2690 da Comissão, de 17 de outubro de 2024, que estabelece regras de execução da NIS 2, relativamente aos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança, bem como o *Technical Implementation Guidance*, versão 1.0, de junho de 2025, e ainda o *Good Practices for Supply Chain Cybersecurity*, de junho de 2023, ambos elaborados pela *European Union Agency for Cybersecurity* (ENISA).

[8] O Regime Jurídico da Segurança do Ciberespaço ainda em vigor (Lei n.º 46/2018, de 13 de agosto, que transpôs a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016), faz depender a sua aplicação de qualificações assentes em critérios essencialmente materiais, não prevendo nem remetendo para quaisquer parâmetros quantitativos. Ainda assim, para se ir traçando algum caminho, a par dos Considerandos da SRI 2, têm-se revelado particularmente relevantes as orientações adotadas por autoridades nacionais de cibersegurança de outros Estados-Membros, como sucede com o *Centre for Cybersecurity Belgium*, cujas *Frequently Asked Questions* (FAQs) relativas à SRI 2 e à respetiva transposição para o ordenamento jurídico belga, que já se encontram na versão 2.1.3 (03/2026). Ainda que menos detalhadas, são também relevantes as FAQs publicadas pela *Agenzia per la Cybersicurezza Nazionale*, em Itália, bem como as FAQs divulgadas pelo *Instituto Nacional de Ciberseguridad* (*INCIBE-CERT*), em Espanha.

da origem geográfica das diferentes empresas do grupo[9].

Este elemento deve, contudo, ser lido com cautela. A análise consolidada da dimensão do grupo não deverá ser considerada de forma automática, sob pena de conduzir a resultados materialmente desproporcionados. É precisamente essa a preocupação que se encontra refletida no Considerando 16 da SRI 2, ao admitir que os Estados-Membros possam atender ao grau de independência da entidade relativamente às suas empresas parceiras ou associadas, designadamente quanto às redes e sistemas de informação utilizados e aos serviços concretamente prestados.

Significa isto que uma entidade integrada num grupo não deverá, em todo e qualquer caso, ser reconduzida, sem mais, à dimensão agregada desse grupo. Por conseguinte, quando demonstre uma autonomia funcional suficientemente relevante e, considerada isoladamente, não ultrapasse os limiares aplicáveis, poderá justificar-se o afastamento de uma aplicação meramente tabelar do referido critério.

Estes elementos – que, de resto, não esgotam as hipóteses possíveis –, permitem concluir que esta aparente exclusão é, em rigor, apenas um problema de perceção do regime que importa acautelar, antecipando situações de desconformidade, com o consequente risco de exposição e responsabilização das entidades envolvidas.

9 *Cf. European Commission: Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Guide de l'utilisateur pour la définition des PME, Publications Office, 2015* ("Guia do utilizador relativo à definição de PME"). A Comissão Europeia disponibilizou igualmente, para estes efeitos, uma ferramenta eletrónica destinada a auxiliar a determinação da dimensão da empresa, acessível aqui.

NOTÍCIAS

Cibercrime e prova digital

DIMENSÃO GLOBAL DA AMEAÇA

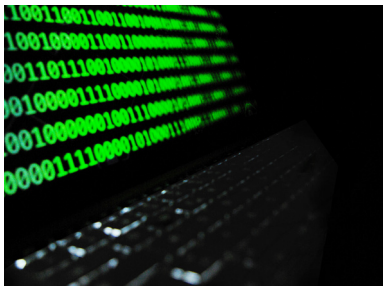
BJÖRN WYLEZICH - STOCK.ADOBE.COM

O panorama global do cibercrime em 2026 é marcado por uma sofisticação crescente das ameaças e pela sua escala sem precedentes. O relatório **IOCTA 2026** (*Internet Organised Crime Threat Assessment*), publicado pela Europol, documenta o cenário evolutivo das ameaças do crime organizado *online*, identificando como tendências estruturais a profissionalização das organizações criminosas, a crescente interdependência entre o cibercrime e outras formas de criminalidade organizada, e a exploração sistemática de infraestruturas legítimas para fins ilícitos (Europol, IOCTA 2026). Os números do **FBI** confirmam a gravidade do fenómeno: segundo o relatório anual do *Internet Crime Complaint Center* (IC3), as perdas patrimoniais decorrentes de crimes informáticos atingiram um **máximo histórico de 20 mil milhões de dólares**, com o *phishing* e o *spoofing* a dominarem o panorama das queixas recebidas, embora se estime que os valores reais sejam significativamente superiores (FBI Internet Crime Report).

OPERAÇÕES INTERNACIONAIS DE REPRESSÃO

No plano das operações de *law enforcement*, os últimos meses foram marcados por iniciativas de grande escala em múltiplas jurisdições. A Interpol identificou e neutralizou cerca de **45 000 endereços IP maliciosos** associados a *ransomware* e *phishing* a nível global (Interpol). Com foco no continente africano, a mesma organização deteve **651 pessoas em 16 países** por crimes informáticos, ilustrando a disseminação crescente da cibercriminalidade organizada em regiões historicamente subrepresentadas nestas estatísticas (Interpol). A Europol por sua vez noticiou uma operação em que **dois telemóveis apreendidos** permitiram, mediante análise forense, desvendar conexões com uma rede criminosa global de grande dimensão – sublinhando o papel central da extração forense de dispositivos móveis no combate ao crime organizado (Europol). Já o **Brasil liderou a maior operação internacional de combate ao abuso sexual de menores *online*** de que há registo, envolvendo **16 países** e resultando em numerosas detenções e na identificação de vítimas – sendo paradigmática da importância da cooperação policial internacional e das capacidades de investigação digital neste domínio (Observador). A **Eurojust** coordenou ainda uma operação bem-sucedida contra serviços ilegais de *streaming*, com impacto em milhões de utilizadores a nível mundial (Eurojust).

REDES ENCRIPTADAS: SKY ECC, ENCROCHAT E ANOM



O debate sobre a admissibilidade de prova digital obtida através de redes de comunicações encriptadas mantém-se em plena efervescência nos tribunais europeus, com decisões divergentes em múltiplas jurisdições. No que respeita à rede **Sky ECC**, o Tribunal de Antuérpia terá, num futuro próximo, de se pronunciar sobre a admissibilidade de provas obtidas a partir de interceções, tendo já sido confrontado com o

depoimento de um perito forense que suscitou dúvidas quanto à transparência e fiabilidade dos mecanismos de interceção (Computer Weekly); na Suíça, o Tribunal de Basileia adotou posição semelhante, recusando a valoração de prova cuja obtenção não observou as garantias procedimentais exigidas pelo direito suíço; em Espanha, um tribunal absolveu arguidos que tinham sido impedidos de aceder às interceções brutas, colocando o direito à prova da defesa no centro da discussão (Computer Weekly); e em Itália registam-se igualmente impugnações à prova Sky ECC e EncroChat, com a defesa a contestar a cadeia de custódia e a autenticidade das interceções.

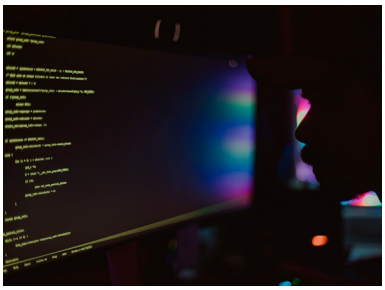
INTEGRIDADE DA INVESTIGAÇÃO CRIMINAL E DA PROVA POLICIAL

O período em análise trouxe também desenvolvimentos perturbadores sobre a fiabilidade da prova policial. Em Espanha, o **antigo chefe da UDEF** (Unidade de Delitos Económicos e Fiscais da Polícia Nacional) prestou declarações perante um juiz descrevendo aquilo que classificou como um "**sistema" institucionalizado de falsificação da origem de grandes operações antidroga**, através da manipulação das circunstâncias de deteção e da atribuição do mérito investigatório. O caso levanta questões fundamentais sobre a integridade da cadeia de custódia da prova e a veracidade dos relatórios policiais, com potencial alcance sobre vários processos por tráfico de droga em que a prova da UDEF desempenha papel central (El Diario). Num registo distinto, a *Wired* revelou que um **informador do FBI geriu durante anos um *site* na *dark web*** que vendia drogas adulteradas com fentanil, levantando interrogações sobre os limites das operações encobertas em ambiente digital e a responsabilidade das autoridades pelos ilícitos praticados no decurso da gestão de plataformas infiltradas (Wired). A mesma revista detalhou a fuga de um colaborador que revelou os segredos dos *scam compounds* do Sudeste Asiático e foi obrigado a deixar o país para salvar a sua vida, iluminando a realidade por detrás das redes de cibercrime assentes em trabalho forçado que alimentam as burlas de *pig butchering* (Wired).

ENCRIPTAÇÃO, ACESSO A DISPOSITIVOS E PROVA DIGITAL

O tema do acesso a dispositivos encriptados gerou dois casos americanos que ilustram, em sentidos opostos, a tensão estrutural entre acesso legítimo aos dados e criptografia robusta. A *Forbes* revelou que a **Microsoft forneceu ao FBI as chaves de desencriptação BitLocker** para aceder a dados num dispositivo confiscado, inaugurando um precedente relevante sobre a cooperação das grandes tecnológicas com as autoridades na obtenção de prova digital (*Forbes*). Pelo contrário, o FBI confessou não ter conseguido aceder ao **iPhone de uma jornalista do *Washington Post*** porque o dispositivo tinha o modo *Lockdown* ativado – um recurso de segurança reforçada da Apple que se revelou eficaz contra as ferramentas forenses das autoridades (404 Media).

INCIDENTES DE SEGURANÇA E AMEAÇAS PERSISTENTES



Investigadores detetaram indícios da utilização, pelo grupo **Lazarus** (ligado à Coreia do Norte), do *ransomware* **Medusa**, designadamente em ataques ao setor da saúde dos Estados Unidos da América (Security.com). Ao nível dos incidentes de segurança com maior impacto, a **Coinbase** confirmou uma violação de origem interna, ligada a *screenshots* de ferramentas de suporte extraídos por um colaborador (Bleeping Computer). A **Comissão Europeia** abriu uma investigação sobre um ciberataque dirigido aos seus sistemas internos (IT Security PT). O governo francês confirmou a exposição de dados de **1,2 milhões de contas bancárias** na sequência de uma violação de dados (SecurityWeek).

PLATAFORMAS DE COMUNICAÇÃO E RESPONSABILIDADE

No que respeita às grandes plataformas de comunicação, o fundador do **Telegram**, Pavel Durov, viu-se confrontado com um processo judicial aberto na **Rússia por alegada contribuição ao terrorismo** – num desenvolvimento que sublinha a pressão crescente dos estados sobre plataformas de comunicação encriptada e suscita questões sobre a responsabilidade das plataformas por conteúdos de terceiros (NowCanal). No plano europeu, o **WhatsApp** viu as suas obrigações de transparência e responsabilidade reforçadas pela Comissão Europeia no âmbito do Regulamento dos Serviços Digitais (Tek.pt).

INTELIGÊNCIA ARTIFICIAL EM CONTEXTO JUDICIAL

Dois desenvolvimentos relevantes marcam o período no que respeita ao uso de inteligência artificial em contexto judicial. No Brasil, o **TRT da 8.ª Região** proferiu uma decisão pioneira sobre uma tentativa de manipulação do sistema de IA generativa utilizado pelo tribunal através de *prompt injection* – técnica que consistiu na inserção de instruções ocultas numa peça processual, com letra branca sobre fundo branco, destinadas a induzir o sistema a produzir uma contestação superficial em prejuízo da parte contrária. O Tribunal qualificou a conduta como

ato atentatório à dignidade da Justiça e aplicou às advogadas subscritoras multa solidária de 10% sobre o valor da causa (ver secção de jurisprudência). Em paralelo, o **STJ** analisou pela primeira vez (AgRg no HC n.º 1.059.475/SP) a validade de um relatório policial elaborado com recurso a IA generativa, em contradição com laudos periciais oficiais, levantando a questão de saber se a IA pode substituir a atividade pericial com implicações diretas nos direitos de defesa (STJ Brasil).

PORTUGAL E O PANORAMA NACIONAL

Em Portugal, o Gabinete Nacional de Segurança lançou o portal **myCiber.gov.pt**, que permite simular a eventual inclusão das empresas no âmbito de aplicação da lei de transposição da NIS2 (myCiber.gov.pt). No plano da formação, a ECTEG lançou a versão **eFirst 2.1**, com novos *serious games* e um módulo renovado sobre desencriptação legal para agentes de primeira linha (ECTEG). Numa nota menos positiva, o jogo *online* ilegal continua a gerar mais de duas mil reclamações, evidenciando a persistência de um mercado ilegal robusto (Jornal Económico).

Criptoativos

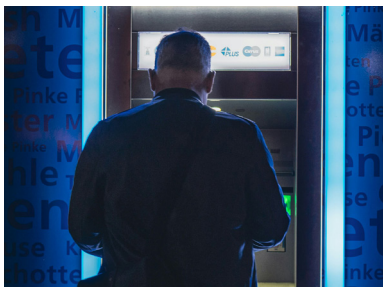
PANORAMA GERAL DO CRIME CRIPTO

O **relatório anual de crime em criptomoedas da TRM Labs** para 2026 traça uma panorâmica preocupante sobre as tendências do crime cripto, com destaque para o crescimento das burlas de investimento, dos ataques a protocolos DeFi e da utilização de *stablecoins* no branqueamento de capitais. A erosão da fronteira entre o ecossistema cripto lícito e o ilícito, bem como a capacidade de atores estatais de utilizarem criptomoedas para financiar atividades ilícitas, emergem como preocupações centrais (TRM Labs).

BYBIT E O LAZARUS: O MAIOR BRANQUEAMENTO COM RECURSO A CRIPTO DA HISTÓRIA

O caso mais mediático do período é o ***hack* da Bybit**, atribuído ao grupo norte-coreano **Lazarus**, no valor de cerca de **1,5 mil milhões de dólares**. Investigadores da Arkham Intelligence confirmaram que o Lazarus concluiu o processo de branqueamento da totalidade dos fundos roubados, convertendo cerca de **500 000 ETH** em BTC através da **THORChain** como mecanismo de *chain hopping* – rede descentralizada que, desde o ataque de 21 de fevereiro de 2025, processou mais de 5,5 mil milhões de dólares em volume. Uma vez em Bitcoin, os fundos foram vendidos através de OTC *desks* opacas, frequentemente situadas na China e no Sudeste Asiático, com desconto de 15 a 20% sobre o valor de mercado.

ATMs CRIPTO E TURBULÊNCIA DE MERCADO



A Bitcoin Depot, **maior operadora de ATM de criptomoedas nos EUA** declarou insolvência e procedeu ao encerramento de **mais de 9000 máquinas** em todo o território americano. O CEO, Alex Holmes, apontou como principais causas as exigências regulatórias cada vez mais restritivas e a fragmentação do enquadramento regulatório entre os diferentes estados.

O encerramento abrupto suscita ainda dúvidas quanto à situação dos utilizadores com transações pendentes. O caso assume igualmente relevância do ponto de vista de AML, na medida em que os ATM de criptomoedas têm sido reiteradamente identificados como vetores de risco elevado nas avaliações do FATF (Jornal de Negócios).

OPERAÇÕES DE *LAW ENFORCEMENT* E APREENSÕES

No plano das operações de repressão, o FBI desenvolveu uma operação inovadora ao criar o seu próprio serviço de cripto designado **NextFundAI,** que permitiu aos agentes comunicar com *market-makers* e observar a sua forma de trabalhar. Esta operação permitiu identificar participantes num esquema de manipulação de mercado e apreender 25 milhões de dólares (TRM Labs). Adicionalmente, o Gabinete do Procurador do Distrito Norte da Carolina anunciou a apreensão de 61 milhões de dólares **em Tether, relacionados com burlas e furtos através de esquemas de *pig butchering* (DOJ EDNC). Na Flórida, o Estado requereu a perda de** imóveis e veículos adquiridos com produto dos crimes de burla e branqueamento que levaram à detenção do CEO da Goliath Ventures (DOJ MDFL).

CONDENAÇÕES RELEVANTES

Um **nacional francês** foi condenado a **oito anos de prisão** pelo branqueamento de centenas de milhões de dólares em criptomoedas (DOJ SDNY). Nos Estados Unidos, o proprietário do **Incognito Market** – um dos maiores mercados de drogas da *dark web* à escala global – foi condenado a **30 anos de prisão**, numa das penas mais severas alguma vez aplicadas em processos de crime organizado em ambiente digital (DOJ SDNY). Um **nacional chinês** foi condenado pelo seu papel num esquema de burla cripto dirigido a cidadãos americanos (DOJ). O ex-campeão olímpico de *snowboard* **Ryan Wedding** foi detido no âmbito de um caso transnacional que combina tráfico de droga, violência e branqueamento de capitais em criptomoedas (TRM Labs). No processo **United States v. Roman Sterlingov** (Bitcoin Fog), a defesa contesta em recurso as metodologias de análise de *blockchain* utilizadas para provar a titularidade do serviço – tornando o processo numa referência sobre os padrões probatórios aplicáveis à análise forense cripto em processo penal (Court Listener).

COMPLIANCE, REGULAÇÃO E DESENVOLVIMENTOS DE MERCADO

A Fortune revelou que a **Binance** despediu investigadores que tinham alertado internamente para potenciais violações de sanções ao Irão, levantando interrogações sobre os mecanismos de *compliance* da maior *exchange* do mundo (Fortune). No Brasil, a **Circle** viu determinado por um tribunal cível o bloqueio de USDC, suscitando questões sobre a executabilidade de decisões judiciais sobre ativos digitais emitidos por entidades estrangeiras (LiveCoins). Em África, as autoridades angolanas desmantelaram um centro de mineração de criptomoedas em Luanda (Jornal de Negócios) e dez cidadãos foram detidos em Ramiros por mineração não autorizada (PTI Angola). Por fim, o *New York Times* publicou uma investigação avançando com **Adam Back** como o candidato mais credível à identidade de Satoshi Nakamoto (New York Times).

LEGISLAÇÃO E *SOFT LAW*

Portugal

LEGISLAÇÃO

LEI N.º 12-A/2026, DE 15 DE ABRIL (Implementação do DSA)

Foi publicada a Lei n.º 12-A/2026, que implementa em Portugal o **Regulamento dos Serviços Digitais (DSA – Regulamento (UE) 2022/2065)**, estabelecendo as autoridades nacionais competentes, os mecanismos de supervisão, as vias processuais aplicáveis e o regime sancionatório nacional. A lei designa as autoridades sectoriais competentes para a supervisão do cumprimento das obrigações decorrentes do DSA pelos diferentes tipos de plataformas e intermediários, numa arquitetura de fiscalização articulada com a Comissão Europeia. A aprovação deste diploma conclui o processo de implementação nacional de um dos mais importantes instrumentos regulatórios europeus no domínio da responsabilidade das plataformas digitais por conteúdos de terceiros (Diário da República).

LEI N.º 73/2025, DE 23 DE DEZEMBRO (Implementação do DORA)

Publicada em 23 de dezembro de 2025, a Lei n.º 73/2025 assegura a implementação dos atos jurídicos europeus sobre resiliência operacional digital do sector financeiro, transpondo e executando o Regulamento DORA. Confirma a competência sectorial do **Banco de Portugal**, da **ASF** e da **CMVM**, em articulação com o **Centro Nacional de Cibersegurança (CNCS)**. Em matéria sancionatória, prevê coimas até **5 000 000 EUR ou 10% do volume de negócios** por incumprimento dos deveres de *governance*, gestão de risco TIC, resposta a incidentes, gestão de terceiros e testes de resiliência. O diploma introduz alterações sectoriais abrangentes ao RGICSF, CVM, sector segurador e ressegurador, serviços de pagamento e moeda eletrónica, fundos de pensões e empresas de investimento (Diário da República, 1.ª série, n.º 246, 23-12-2025).

DECRETO-LEI N.º 25/2026, DE 28 DE JANEIRO (Conteúdos Terroristas em Linha)

Publicado em 28 de janeiro de 2026, o Decreto-Lei n.º 25/2026 transpõe para a ordem jurídica interna o **Regulamento (UE) 2021/784** relativo ao combate à difusão de conteúdos terroristas em linha. Designa a **Polícia Judiciária** (UNCT-PJ) como autoridade competente para emitir decisões de supressão ou bloqueio, com validação pelo **DCIAP/Ministério Público** em 48 horas e controlo judicial pelo Juiz de Instrução (Diário da República).

GRUPO DE TRABALHO DO CSMP – PROPOSTA DE REVISÃO DO CÓDIGO DE PROCESSO PENAL (PROVA DIGITAL)

O Conselho Superior do Ministério Público constituiu, em fevereiro de 2025, um grupo de trabalho composto por sete magistrados – coordenado pelo Procurador-Geral Adjunto jubilado José Góis e com Rui Cardoso (Diretor do DCIAP) como porta-voz –, com o mandato de analisar e propor alterações à legislação processual penal. As propostas foram apresentadas na PGR em 28 de abril de 2026 e contemplam a alteração de 130 artigos do Código de Processo Penal.

No domínio específico da prova digital (correspondente, em substância, às propostas constantes das pp. 63 e seguintes do documento), as alterações mais relevantes são as seguintes:

a) Competência para seleção de correio eletrónico – transferência do JIC para o MP: a proposta prevê que a seleção dos conteúdos relevantes de correio eletrónico e registos de comunicações passe a ser efetuada pelo Ministério Público, em termos análogos ao que já vigora para as escutas telefónicas ao abrigo dos artigos 187.º e seguintes do CPP – retirando ao Juiz de Instrução a competência que lhe é atualmente atribuída pelo artigo 17.º da Lei do Cibercrime conjugado com o artigo 179.º, n.º 3, do CPP. O porta-voz do grupo justificou a proposta com base nos atrasos – por vezes de anos – que o regime vigente tem causado na obtenção de prova digital: «O procedimento que hoje tem de ser seguido por causa da interpretação que é feita da lei, tem levado a atrasos, às vezes de anos, até que nós consigamos ter a prova digital.» O grupo sublinhou que a alteração não coloca em causa o direito de defesa dos arguidos, que manterão acesso aos dados apreendidos;

b) Extensão expressa do regime das escutas à utilização de dispositivos de localização (GPS): a proposta prevê

que o regime de autorização judicial aplicável às escutas telefónicas seja expressamente estendido à utilização de dispositivos de localização por GPS, clarificando o quadro legal aplicável a este meio de obtenção de prova e uniformizando os requisitos de autorização prévia;

c) Revisão da Lei do Cibercrime – pesquisa e apreensão de dados informáticos: o grupo propõe a revisão da Lei do Cibercrime no que respeita ao regime de pesquisa e apreensão de dados informáticos, em linha com as propostas acima referidas e com o objetivo de simplificar e agilizar o acesso a prova digital em investigação criminal. O grupo reconheceu, contudo, que a questão dos metadados – que o acórdão do TRL de 19 de março de 2026 voltou a colocar em destaque – não foi objeto de proposta de alteração específica neste pacote.

Estrangeiro e Internacional

LEGISLAÇÃO E INSTRUMENTOS VINCULATIVOS

CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME – PAPUA NOVA GUINÉ TORNA-SE A 82.ª PARTE.

A Papua Nova Guiné ratificou a Convenção de Budapeste (STE n.º 185), tornando-se a 82.ª parte deste instrumento e alargando o seu alcance geográfico ao Pacífico. A Convenção consolida-se assim como o principal quadro jurídico multilateral de combate ao cibercrime (Conselho da Europa | Texto da Convenção).

MOÇAMBIQUE – LEI DE CRIMES INFORMÁTICOS.

A Assembleia da República de Moçambique aprovou legislação específica em matéria de cibercrime, harmonizando o quadro jurídico nacional com os princípios da Convenção de Budapeste e colocando Moçambique no conjunto crescente de países africanos com legislação dedicada nesta área (Parlamento de Moçambique).

CHINA – REFORÇO DAS PENAS POR CIBERCRIME.

A China anunciou alterações legislativas que reforçam as penas por cibercrime, acrescentando a possibilidade de aplicação de **proibições de saída do país** após o cumprimento de penas de prisão, com o objetivo declarado de conter a reincidência e o crime organizado transnacional (South China Morning Post).

REINO UNIDO – PROIBIÇÃO DE VPN PARA MENORES.

A Câmara dos Lordes aprovou uma proposta de proibição do uso de VPN por crianças, no âmbito de uma iniciativa legislativa mais ampla de proteção de menores no ambiente digital (ISPreview).

SOFT LAW E OUTROS INSTRUMENTOS

COE C-PROC – ESTADO GLOBAL DA LEGISLAÇÃO SOBRE CIBERCRIME (2013–2025).

O Comité da Convenção sobre o Cibercrime publicou uma análise panorâmica da evolução dos quadros normativos nacionais e das lacunas persistentes a nível global – referência essencial para a comparação de sistemas e para a identificação de jurisdições com necessidade de harmonização (Conselho da Europa).

UNIÃO EUROPEIA – REFORÇO DA CIBERSEGURANÇA.

A Comissão Europeia adotou um pacote de medidas para reforçar a resiliência e as capacidades de cibersegurança da UE no âmbito da implementação da Estratégia de Cibersegurança e da NIS2, incluindo iniciativas de partilha de informação, capacitação técnica e coordenação entre Estados-Membros (Comissão Europeia).

ENISA – NIS360 2024.

A Agência da União Europeia para a Cibersegurança (ENISA) publicou o relatório NIS360 2024, que avalia a maturidade e a prontidão dos sectores abrangidos pela Diretiva NIS2 nos diferentes Estados-Membros, identificando lacunas de implementação e boas práticas. O relatório constitui uma ferramenta de referência para as autoridades competentes, os operadores de serviços essenciais e os prestadores de serviços digitais na calibração dos seus programas de conformidade com a NIS2 (ENISA).

UNIÃO EUROPEIA – DIRETRIZES SOBRE TRANSPARÊNCIA NO AI ACT (ARTIGO 50.º).

A Comissão Europeia submeteu a consulta um projeto de diretrizes sobre as obrigações de transparência aplicáveis a determinados sistemas de IA ao abrigo do artigo 50.º do AI Act – nomeadamente *chatbots*, sistemas de geração de conteúdo sintético e marcação de conteúdo gerado por IA. As diretrizes têm relevância direta para o uso de IA em contextos judiciais e de investigação criminal (Comissão Europeia).

FATF – RELATÓRIO SOBRE *STABLECOINS* E CARTEIRAS NÃO CUSTODIAIS.

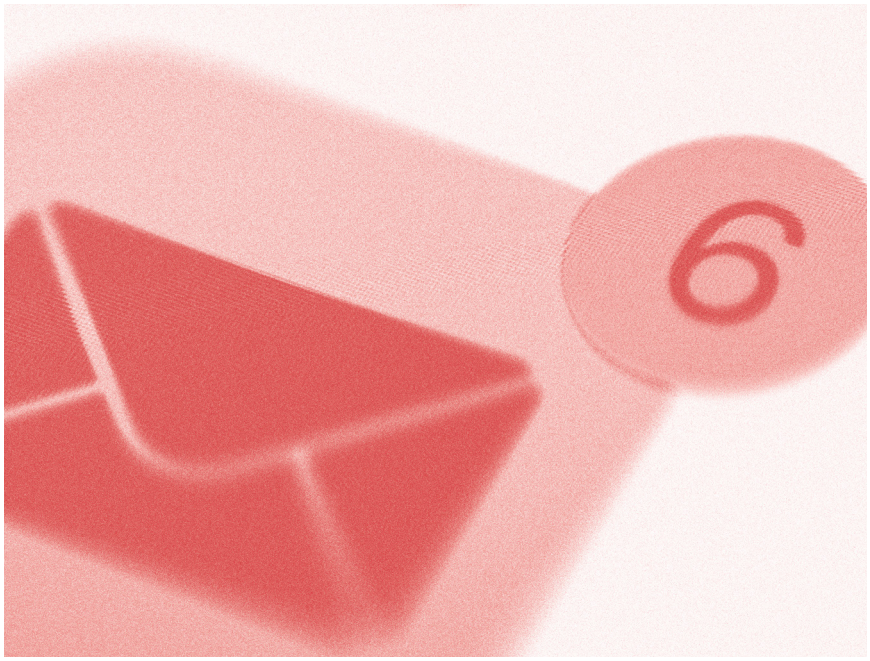
O FATF/GAFI publicou relatório específico sobre *stablecoins* e carteiras sem custódia (*unhosted wallets*), reforçando as expectativas de conformidade AML/CFT para os prestadores de serviços sobre ativos virtuais e abordando os riscos específicos destas categorias para o branqueamento de capitais (FATF).

JURISPRUDÊNCIA

Jurisprudência portuguesa

TRIBUNAL DA RELAÇÃO DE LISBOA, PROC. N.º 2221/19.3JFLSB-C.L1-5, ACÓRDÃO DE 23 DE JANEIRO DE 2026.

Correio eletrónico – Competência para seleção – Artigo 17.º da Lei do Cibercrime – Artigo 179.º, n.º 3, do CPP.



Decidiu que é o Juiz de Instrução quem, cumprindo o art. 179.º, n.º 3, do CPP (aplicável por força do art. 17.º da Lei 109/2009), seleciona e faz juntar ao processo os conteúdos relevantes de correio eletrónico e registos de comunicações. Referiu que não viola a estrutura acusatória (art. 32.º, n.º 5, da CRP) o despacho que recusa entregar ao MP, após o JIC tomar conhecimento e expurgar conteúdos proibidos, os conteúdos para o MP pesquisar e selecionar os relevantes. (DGSI)

TRIBUNAL DA RELAÇÃO DE LISBOA, PROC. N.º 23/26.0GCALM-A.L1-9, ACÓRDÃO DE 19 DE MARÇO DE 2026.

Dados de tráfego e localização – Metadados – Regimes de obtenção de prova digital – Lei n.º 32/2008.

Referiu que os dados de tráfego e de localização constituem metadados protegidos pelo sigilo das telecomunicações e pela reserva da vida privada, por permitirem inferir comportamentos apesar de não incidirem sobre o conteúdo das comunicações.

Mais clarificou que a obtenção de prova digital se organiza em três regimes distintos: (*i*) interceção em tempo real (arts. 187.º a 190.º, do CPP); (*ii*) pesquisa e apreensão de dados informáticos (Lei n.º 109/2009); e (*iii*) acesso a dados de tráfego armazenados (Lei n.º 32/2008).

Esclareceu que, após os Acórdãos do Tribunal Constitucional n.ºs 268/2022 e 800/2023, afirma-se a necessidade de um modelo de conservação seletiva e dependente de prévia autorização judicial para dados de tráfego e de localização para fins de investigação criminal. O acesso a dados de tráfego armazenados, mesmo que conservados pelas operadoras para outras finalidades (*v.g.*, comerciais ou de faturação), exige o cumprimento do regime específico da Lei n.º 32/2008, não podendo ser obtidos por via dos arts. 187.º e 189.º do CPP, da Lei do Cibercrime ou da Lei n.º 41/2004.

Decidiu julgar improcedente o recurso do MP, confirmando o indeferimento do acesso a dados de tráfego armazenados por falta de prévia autorização nos termos legalmente exigidos. (DGSI)

Jurisprudência estrangeira

ISRAEL

SUPREMO TRIBUNAL, PROC. ח"תע 65435-03-26, ESTADO DE ISRAEL V. ARTYOM NADORNENKO, JUIZ ALEX STEIN, 19 DE MAIO DE 2026.

Cooperação voluntária com emissora de *stablecoin* – Congelamento de criptoativos – Extraterritorialidade – Artigo 3.º da Ordenança da Polícia.

O acórdão decidiu que, ao contactar a Tether e obter o congelamento da carteira, a Polícia de Israel não exerceu qualquer poder jurídico ou praticou qualquer ato coercivo sobre o requerido ou sobre a própria Tether, mas apenas a sua liberdade de ação (*privilege*), isto é, a faculdade de tentar obter a cooperação de um terceiro privado, sem criar sujeição jurídica nem restringir direitos do requerido, que nunca teve qualquer direito a impedir a polícia de fazer essas diligências. Considerou ainda que a Tether é uma sociedade estrangeira, que não opera em Israel, não está sujeita ao direito israelita e não se encontra sujeita à autoridade israelita, pelo que a polícia não dispunha de qualquer meio de pressão regulatória sobre a empresa; pelo contrário, foi a própria Tether que exigiu um despacho judicial israelita como condição para proceder ao congelamento da carteira, tendo a Polícia de Israel apenas satisfeito essa exigência. Nestas circunstâncias, o tribunal concluiu que não houve ato estatal coercivo que carecesse de habilitação estatutária expressa, bastando a habilitação geral conferida à Polícia pelo artigo 3.º da Ordenança da Polícia. O acórdão sublinha ainda que a deteção e apreensão de carteiras digitais enfrenta dificuldades consideráveis, dado que criptoativos como o Bitcoin são ativos virtuais sem localização geográfica definida, e afirma que, quando as carteiras estão associadas a empresas financeiras, a cooperação voluntária com essas empresas, segundo o modelo seguido com a Tether, pode auxiliar de forma significativa a polícia, tanto mais que pelo menos algumas dessas empresas têm interesse em preservar a sua reputação e, por isso, se mostram disponíveis para colaborar.

BRASIL

TRIBUNAL REGIONAL DO TRABALHO DA 8.ª REGIÃO, PROC. ATORD 0001062-55.2025.5.08.0130, 3.ª VARA DO TRABALHO DE PARAUAPEBAS.

***Prompt injection* – Manipulação de sistema de IA judicial – Ato atentatório à dignidade da Justiça – Artigos 5.º e 77.º, §2.º, do CPC.**

O acórdão decidiu que o sujeito processual utilizou uma técnica de manipulação de sistemas de inteligência artificial, conhecida como *prompt injection*, ao inserir, na petição, texto em fonte branca sobre fundo branco – invisível ao leitor humano – contendo um comando oculto dirigido à IA judicial, instruindo-a a contestar a petição de forma superficial e a não impugnar os documentos, independentemente do comando que lhe fosse dado. O tribunal qualificou essa técnica como a inserção deliberada de instruções ocultas em documentos com o propósito de manipular sistemas de IA que venham a processar o texto, induzindo-os a produzir resultados favoráveis a quem inseriu o comando. Entendeu ainda que a tentativa de manipulação da Justiça se consuma no momento em que o comando é inserido no documento protocolado perante o Poder Judiciário, independentemente de ter ou não produzido o resultado pretendido, tratando-se de ilícito processual de natureza formal, que se perfectibiliza com a própria conduta e dispensa a demonstração de prejuízo concreto para legitimar a aplicação da sanção. Com base nisso, o tribunal considerou configurado ato atentatório à dignidade da Justiça, à luz dos artigos 5.º e 77.º, §2.º, do CPC, e aplicou multa de 10% sobre o valor da causa (842 500,87 BRL), de forma solidária, a reverter a favor da União Federal, determinando ainda a comunicação dos factos à OAB/PA e à Corregedoria do TRT da 8.ª Região.

EUA

TRIBUNAL FEDERAL DO DISTRITO DE COLUMBIA, CIVIL ACTION NO. 25-CV-1907.

Queixa de perda *in rem* – 225 milhões de USDT – *Pig butchering* – 18 U.S.C. §§ 981(a)(1)(A), 1956.

O acórdão descreve que os *cryptocurrency confidence scams* conhecidos como *pig butchering* constituem um tipo de fraude de investimento em criptomoedas baseada na *internet*, em que a vítima é "engordada antes do abate": primeiro há um contacto a frio por mensagem, redes sociais ou outra plataforma; depois constrói-se uma relação com a vítima ao longo de dias, semanas ou meses; em seguida a vítima é induzida a enviar alegados investimentos através de plataformas fraudulentas; por fim, os autores do esquema cortam todo o contacto quando a vítima deixa de fazer pagamentos. O tribunal assinala que a análise da atividade transacional associada a 144 contas na plataforma OKX revelou mais de 263 000 transações de depósito, totalizando cerca de três mil milhões de dólares, sendo que 98% dessas transações ocorreram entre novembro de 2022 e novembro de 2023. Nesse período de um ano, as 144 contas realizaram aproximadamente 257 740 transações, envolvendo moeda virtual no valor de cerca de 2,94 mil milhões de dólares, o que corresponde a uma média de mais de 700 transações por dia, movimentando mais de oito milhões de dólares diários. O tribunal conclui ainda que quase todas as 144 contas foram acedidas a partir de endereços IP nas Filipinas, todas associadas a endereços de *email* iCloud com uma convenção de nomenclatura específica, e abertas com documentos de identificação vietnamitas e fotografias KYC que aparentam ter sido tiradas no mesmo local, o que é um forte indicador de que essas contas são controladas por indivíduos a operar a partir de um *scam compound*. (Justice)

4.º CIRCUITO, UNITED STATES V. LOWERS, N.º 24-4546, 10 DE MARÇO DE 2026.

Google Drive – Expectativa de privacidade em ficheiros *cloud* – *Hash-matching* – Atenuação da prova ilicitamente obtida – 4.ª Emenda.

O acórdão reconheceu que existe uma expectativa razoável de privacidade relativamente a ficheiros armazenados em contas de *cloud*, designadamente no Google Drive, concluindo que a polícia não pode abrir ou visualizar esses ficheiros sem mandado judicial, salvo se estiver em causa alguma exceção constitucional aplicável à exigência de mandado. Apesar de ter reconhecido que houve violação da 4.ª Emenda, por terem sido abertos e visualizados ficheiros sem mandado, o Tribunal manteve a recusa de declaração de proibição da prova, entendendo que essa prova se encontrava suficientemente atenuada (*attenuated*) em virtude dos intervalos temporais e dos atos voluntários entretanto ocorridos – nomeadamente entrevistas e a prestação de consentimento pelo arguido –, o que tornava injustificada a aplicação da regra de exclusão.

(Justia)

5.º CIRCUITO, UNITED STATES V. BURGER, N.º 25-51021, 19 DE MARÇO DE 2026.

Ameaças em plataforma de jogo *online* (Roblox) – «true threats» – 1.ª Emenda – Questão factual para júri.

O Tribunal reverteu a decisão que tinha arquivado a acusação em fase pré-julgamento, entendendo que a qualificação de declarações como "true threats" – e, portanto, fora da proteção da 1.ª Emenda – é tipicamente uma questão factual a ser submetida ao júri e não suscetível de decisão antecipada pelo tribunal. (Justia)

2.º CIRCUITO, UNITED STATES V. PENCE, N.º 24-1025, 10 DE ABRIL DE 2026.

***Dark web* – Pagamento em Bitcoin – Confissão pré-Miranda – Custódia – 5.ª Emenda.**

O arguido foi investigado por alegadamente ter contratado, através da *dark web*, o homicídio de um casal, pagando em Bitcoin. Após uma operação do FBI, foi interrogado, sem algemas, numa viatura policial e confessou antes de ser informado dos seus direitos enquanto arguido (*Miranda Rights*).

Tentou posteriormente excluir essa confissão em tribunal, alegando que se encontrava detido de forma ilegal no momento do interrogatório.

O Tribunal concluiu que o arguido **não estava formalmente em situação de detenção, pelo que os direitos de Miranda** (*Miranda Rights*) ainda não se aplicavam. Consequentemente, a condenação foi confirmada em recurso. (Justia)

7.º CIRCUITO, UNITED STATES V. BLOCKER, N.º 25-1536, 5 DE MAIO DE 2026.

Dropbox – Termos de serviço como consentimento – *Scanning* automático – Denúncia ao NCMEC – 4.ª Emenda.

O caso envolvia a deteção de pornografia infantil pelo Dropbox através de monitorização permitida pelos termos de serviço da plataforma, reporte ao NCMEC e subsequente mandado de busca do FBI, com descoberta de mais imagens. O Tribunal confirmou a validade da interceção: a aceitação dos termos de serviço foi considerada consentimento eficaz para o Dropbox examinar ficheiros e divulgá-los para fins como o reporte às autoridades, mantendo-se o indeferimento do pedido de supressão. (Justia)

ENTREVISTA A NICK FURNEAUX: "AS CRIPTOMOEDAS, NOS SEUS FUNDAMENTOS, NÃO SÃO ASSIM TÃO DIFÍCEIS"

Autor de *Investigating Cryptocurrencies* e *There's no such thing as crypto crime*

Por **David Silva Ramalho**

Nick Furneaux

Nick, mais uma vez, obrigado por ter aceitado o convite para esta entrevista. Sem mais demoras, vou entrar diretamente no assunto: como é que entraste no rastreio de criptomoedas?

Por acidente. Se soubesse, provavelmente nunca o teria feito – tem de haver uma forma mais fácil de ganhar a vida. Talvez seja um pouco simplista, mas venho de um percurso em que costumávamos criar muitas ferramentas de extração encoberta de dados, que eram utilizadas por todo o tipo de agências que precisavam de extrair dados de computadores-alvo discretamente. E, portanto, ensinávamos muitas metodologias à volta disso – análise de memória, por exemplo, que podia ser feita a alta velocidade no terreno. Fazer uma imagem da memória de uma máquina-alvo é muito mais rápido do que fazer uma imagem de um disco rígido, por exemplo, num cibercafé num país mais complicado. E ensinávamos muitas dessas coisas. Depois começámos a deparar-nos com estas longas sequências de letras e números nas máquinas dos suspeitos. Eram endereços de Bitcoin dos primórdios. Comecei a ler sobre o assunto, apenas para tentar perceber a tecnologia e o que estava em causa, e vou ser completamente honesto: achei que era simplesmente ótimo para criminosos.

E poderia ter comprado Bitcoin quando valia qualquer coisa como algumas centenas de dólares, mas não o fiz, porque achei que aquilo era definitivamente uma rede criminosa e que nunca iria resultar em nada de bom. Por isso, julgo que neste momento possuo qualquer coisa como seis mil libras em Bitcoin. Quer dizer, é literalmente uma ninharia no grande esquema das coisas.

Identifico-me com isso. Comecei a investigar o tema em 2012, 2013, e devia ter comprado na altura.

Sim, o que se sabe depois...mas não peçam conselhos de investimento a um investigador; essa é a lição a retirar. Interessava-me nisso enquanto tecnologia. Achei interessante e que podia ser um bom indicador: se nos deparássemos com isto, poderíamos estar perante um criminoso. Estamos a falar de uma fase muito inicial, não dos dias de hoje, em que Wall Street compra Bitcoin. Foi alguns anos depois que nos foi proposta a primeira investigação com Bitcoin. Na altura não havia grandes ferramentas – a Chainalysis estava a começar a aparecer – por isso começámos a fazer muitas destas investigações manualmente, usando apenas exploradores de blocos e coisas do género. Não havia grande coisa em termos de atribuição.

Acho que esta história dá uma volta completa, e isso está no meu primeiro livro, quando um bom amigo meu numa polícia local me ligou por causa de um disco rígido que tinham levado para o laboratório de informática forense. Ele perguntou: "como é que extraio a Bitcoin deste computador?".

E eu disse: "o que queres dizer?". Ele respondeu: "bem, como é que extraio o Bitcoin deste computador? Há Bitcoin aqui". Eu tinha um enorme respeito por este tipo – muito inteligente e um excelente "forensicador", o que não é uma palavra, mas enfim – e pensei: "uau, essa é a pergunta errada". E se ele não percebe que é a pergunta errada, imagino que muita gente não perceba que é a pergunta errada. Por isso criei um curso de formação sobre investigação de Bitcoin na altura, e o curso tornou-se viral no meio policial – acabámos por ensinar polícias na maioria dos principais países do mundo. E depois, claro, começámos a fazer cada vez mais investigações. Um bom amigo meu, eu próprio e um tipo chamado Luke, que está na TRM Labs, acho que fizemos investigações de Bitcoin no valor de cerca de 21 mil milhões ao longo de aproximadamente quatro anos. Depois criámos cursos avançados e assim por diante, e então a TRM Labs apareceu há quatro anos e comprou a CSI Tech, que era a empresa na altura. Por isso aí tens, é essa a história.

E como é que esse curso que se tornou viral no meio policial resistiria hoje.

Inabalável.

A sério?

As únicas coisas que mudaram são alguns dos exploradores de blocos. Um ou dois já não existem; alguns funcionam de forma ligeiramente diferente; alguns eram generosos a permitir descarregar ficheiros CSV de contas, e alguns já não permitem isso. Por isso, algumas funcionalidades mudaram. Mas o livro, *Investigating Cryptocurrencies* – em que o curso se baseia e que eu estava a escrever ao mesmo tempo que o curso – resiste. A Bitcoin não mudou fundamentalmente. Os endereços mudaram ao longo do tempo e alguns protocolos de melhoria do Bitcoin foram aprovados, mas fundamentalmente nada mudou de forma substancial. Está mesmo como estava.

«ERA QUE EU ESTAVA PREOCUPADO POR ESTARMOS A VER MUITAS FORÇAS POLICIAIS E ORGANIZAÇÕES DE INVESTIGAÇÃO MUITO BOAS A CRIAR EQUIPAS DEDICADAS DE INVESTIGAÇÃO DE CRIPTOMOEDAS.»

Mas dirias que a criminalidade através do Bitcoin se mantém igual?

Bom, isso é interessante, porque serve de ponte para o segundo livro, *There's No Such Thing as Crypto Crime*. O propósito desse título *clickbait* – se me é permitido usar o termo – era que eu estava preocupado por estarmos a ver muitas forças policiais e organizações de investigação muito boas a criar equipas dedicadas de investigação de criptomoedas. O que não é, em si mesmo, uma coisa má.

Funciona.

Mas é uma coisa má se se vê a criminalidade com criptomoedas como um novo tipo de crime – o que não é. Desafio qualquer pessoa a inventar um crime verdadeiramente novo que não tenha algum antecedente nos últimos 2000 anos de história criminal. Os gregos já o faziam. O branqueamento de capitais não mudou muito; os *scams* não mudaram muito. Por vezes temos um mecanismo diferente, um meio de pagamento diferente, mas fundamentalmente alguém que te telefona a tentar manipular-te, com recurso a técnicas de engenharia social, para que reveles as tuas *seed words* não é diferente de alguém que te manda uma mensagem de texto a pedir a tua *password*.

«FUNDAMENTALMENTE AINDA HÁ MUITO POUCOS CRIMES EM QUE A BLOCKCHAIN SEJA A ÚNICA PROVA»

As técnicas não mudaram nada. Se pensarmos nas pessoas a quem se dizia para comprar um cartão de crédito pré-pago, em que é que isso difere de lhes dizerem para ir a uma caixa ATM, comprar algum Bitcoin e transferi-la para os burlões? É tudo igual. E preocupou-me durante bastante tempo que isto não estivesse a ser compreendido. Acho que agora já está – que podemos usar as mesmas técnicas investigativas fundamentais que sempre usámos e compreendemos. As criptomoedas são apenas um *plugin*, e nada mais do que isso, na verdade.

Vou citar-te nisso. Mas o teu curso sobre investigação de criptomoedas foi construído em torno dos esquemas de branqueamento de capitais que existiam à data. Agora vemos fundos a circular através de *liquidity pools*, *bridges* e agregadores em vez de *exchanges* centralizadas. E mesmo com o aumento dos requisitos KYC para as *exchanges* centralizadas – isto não altera a metodologia investigativa, ou a investigação é fundamentalmente a mesma, apenas aplicada com técnicas diferentes?

Quem já esteve ligado à polícia, especialmente à polícia financeira, e eu alargaria isso a todos os que estão envolvidos no crime financeiro, seja no âmbito legislativo ou qualquer outro, sabe que a criminalidade está a mudar muito rapidamente, adaptando esses pequenos métodos e a forma como atinge os seus objetivos. Se surge um novo serviço, pode esse serviço ser explorado para fins ilícitos? É isso que muda. E se leres o capítulo sobre branqueamento no segundo livro, está bom, mas há certamente uma dúzia de outras coisas que deveriam lá estar agora.

Dito isso, sempre acreditei que, se se compreender o essencial do modo de funcionamento de uma criptomoeda, consegue-se assimilar novas metodologias com relativa facilidade. Para isso é necessário ter um certo raciocínio criminal. Se se compreender como a Bitcoin funciona enquanto pseudomoeda – podemos chamá-lo uma moeda? Não me parece –, se se compreender como funciona o Ethereum, como funciona o Tron, se se perceberem as suas particularidades, então quando surgem novas técnicas consegue-se aplicar esse conhecimento. É como um investigador financeiro que percebe como funciona um banco: mesmo que os criminosos usem novas técnicas, o investigador compreende o sistema subjacente.

Mas parece-te que algumas técnicas se tornam em verdadeiras novas formas de cometer crimes? Estou a pensar nas *privacy chains*, em Monero, nas redes de *layer* 2, serão elas uma mudança de paradigma para o rastreio de fundos??

Sim, são – são métodos técnicos de transferir valor. São verdadeiramente novos? Na forma como funcionam, sim, mas já tivemos mulas de dinheiro a atravessar fronteiras com passaportes falsos. Não será isso fundamentalmente idêntico a um endereço Monero não rastreável a transferir valor de um sítio para outro? Percebo que possa parecer forçado, mas há quase sempre um paralelo histórico com o que vemos hoje. Não estou a subestimar a dificuldade: algumas destas moedas de privacidade complicam as coisas. Por isso temos de acompanhar a inovação técnica, mas fundamentalmente ainda há muito poucos crimes em que a *blockchain* seja a única prova. Quase sempre há comunicações; quase sempre há outras provas que ajudam a estabelecer as conexões. Se tentares desmantelar um grupo de crime organizado apenas com rastreio Monero – boa sorte, mas vais reformar-te antes de veres resultados. Na prática, o rastreio fará parte de uma investigação que, se bem-sucedida, acrescentará peso a uma peça do puzzle onde também

tens informações de inteligência, vigilância e outros elementos. E a propósito de ainda ser muito difícil comprar qualquer coisa com criptomoeda: em algum momento, algures, a criptomoeda tem de ser convertida em moeda fiduciária, e esse é muitas vezes o ponto fraco. Boa *intelligence*, boa compreensão de como estas coisas funcionam, é disso que tudo depende. Por isso, mais uma vez, pode parecer que estou a minimizar, mas não estou de todo.

Percebo. Quando falavas das mulas, lembrei-me que seria mais próximo se essas mulas tivessem portais como no Stargate que lhes permitissem aparecer noutras dimensões.

Sim, é um ponto muito pertinente. E remete para algo que tenho dito há muito tempo: tenho sido uma pedra no sapato de muita gente por causa da linguagem de enviar e receber criptomoeda, porque na verdade não se envia nem se recebe coisa alguma. Simplesmente desbloqueia-se e bloqueia-se na *blockchain*. Nunca se move de facto. E já vi escrito em processos judiciais que "esta bitcoin foi enviada além-fronteiras para a Rússia".

Não foi. Não se moveu nada. Nas dezenas de milhões de registos da *blockchain* da Bitcoin a funcionar por todo o mundo em qualquer momento, o que pode ter acontecido é que outra pessoa assumiu o controlo – alguém que estava a usar uma carteira e que se encontrava na Rússia, ou onde quer que fosse – mas fundamentalmente, nada se moveu.

Já vi uma decisão judicial em que disseram que o suspeito, que era meu cliente, "tinha uma *blockchain*", portanto, sim.

Ótimo. Talvez tivesse e tu lha tenhas dado.

Bem, era a *blockchain* da Bitcoin.

Pois, aí está.

Percebo o teu ponto. A *blockchain* e o rastreio não te contam uma história, dão-te migalhas a partir das quais se podem construir duas narrativas diferentes, quer para a acusação quer para a defesa. É por isso que é necessária prova corroborante.

Sim, quando éramos a CSI Tech, antes da venda à TRM Labs, dávamos um curso de recolha de informação em fontes abertas a par dos nossos cursos de criptomoedas, porque era extremamente importante conseguir seguir essas migalhas para o mundo digital mais vasto.

Compreender endereços IP, acompanhar o fluxo de dados de rede, recolher informações das redes sociais – essas coisas andam de mão dada com o rastreio na *blockchain*.

Ligeiramente fora do tema, mas mencionaste algo sobre talvez estares a minimizar a relevância da criptomoeda. Temos visto quem chame à *blockchain* a *internet* do dinheiro – e ainda assim apontaste, com razão, que não se compra grande coisa com criptomoeda e que, a dada altura, o anonimato tende a quebrar. Dirias que és um cético quanto ao futuro da criptomoeda enquanto meio legítimo de transação ou investimento?

«TENHO SIDO UMA PEDRA NO SAPATO DE MUITA GENTE POR CAUSA DA LINGUAGEM DE ENVIAR E RECEBER CRIPTOMOEDA, PORQUE NA VERDADE NÃO SE ENVIA NEM SE RECEBE COISA ALGUMA»

Costumam perguntar-me isso e genuinamente não tenho uma opinião relevante sobre o assunto. O que direi é que acho que a tecnologia blockchain é fantástica. Satoshi Nakamoto – ele, ela, eles, quem quer que seja – produziu uma das inovações técnicas mais brilhantes dos últimos 100 anos. O conceito de blocos ligados por criptografia e transações criptográficas é simplesmente uma coisa linda, e funciona. Precisamos de adaptá-lo à computação quântica nos próximos 15 anos mais ou menos, talvez antes – a Google parece estar a avançar mais rapidamente nesse domínio neste momento – mas não é uma tarefa insuperável. Acho que a criptomoeda tem futuro, porque a tecnologia é sólida, mesmo que possa parecer diferente do que temos hoje. E em muitos aspetos, porque nunca comprei, não me interessa particularmente que o Tron tenha sucesso ou

que o USDT seja adotado pelo governo americano. Enquanto investigador, interessa-me simplesmente como pode ser usada criminalmente e como os investigadores podem melhor desvendar o fluxo de fundos.

Isso é interessante – pessoalmente não és um grande investidor em criptomoedas, e ainda assim dizes que precisas de pensar como um criminoso para investigar. Isso significa que precisas de experimentar como funciona um *mixer*, de testar uma *liquidity pool*, de utilizá-los de forma ilícita? Ou parece-te que analisar e estudar como os criminosos usam estas ferramentas é suficiente?

As pessoas que se especializam em identificar notas contrafeitas passam a maior parte do tempo a estudar como é uma nota autêntica, não as falsificadas. Porque quando se conhece verdadeiramente como é um dólar ou uma nota de cinco libras, e todas as características de segurança incorporadas, identificar a contrafação é simples. A mesma lógica se aplica aqui: se se perceber como funciona uma criptomoeda ou um *mixer*, é mais fácil reconhecer quando está a ser usado de forma abusiva. Precisas de usar estes instrumentos para os compreenderes? Na verdade, não – a *blockchain* mostra publicamente o que toda a gente está a fazer com ele. E muitas ferramentas, como o Tornado Cash, são de código aberto: é um repositório no GitHub, podes descarregá-lo e executar a tua própria instância num laboratório, se quiseres. Mas o Luke e eu levámos apenas um dia, quando o Tornado Cash apareceu pela primeira vez, a perceber como funcionava e a encontrar formas de rastrear através dele – simplesmente observando o que toda a gente estava a fazer *on-chain*. Não precisámos de fazer passar fundos nossos por ele.

Enquanto rastreador e investigador, qual é atualmente o maior obstáculo que enfrentas? Aquele com que tens genuinamente mais dificuldade quando rastreias fundos?

O problema não está verdadeiramente no rastreio. O problema continua a ser a velocidade e a capacidade de resposta das forças de segurança – a amplitude de capacidade, a velocidade e a disponibilidade das *exchanges* para responder, e as exigências de prova para decretamento de uma *freezing order* para fazer os fundos regressar às vítimas. Deixe-me dar-lhe um exemplo.

Ou a cooperação judiciária internacional.

Nos últimos dois meses, recebi uma chamada de um bom amigo meu. A mãe do melhor amigo dele tinha acabado de perder tudo. Tudo. 1,2 milhões de libras, tudo o que tinha. Literalmente já não conseguia comprar manteiga. Tinha continuado a enviar dinheiro para recuperar o dinheiro anteriormente enviado, o padrão clássico: "precisamos de mais dez mil libras para libertar os seus fundos", e tudo isso. Eu soube do assunto, tinha sido tudo convertido em criptomoeda, e eu sabia para onde tinha ido. Não vou nomear as *exchanges*. Consegui ligar aos responsáveis pelas investigações em duas *exchanges* e dizer: "sou o Nick, isto aconteceu, os fundos estão consigo" – e eles pegaram no assunto de imediato. Rastrearam esses fundos. Liguei também a uma pessoa muito sénior em matéria de criptomoedas na polícia do Reino Unido, que disse estar a tratar do assunto. Direcionei-os para as *exchanges*. E não recuperámos um cêntimo.

Isso magoa-me. Estas pessoas já tinham denunciado a burla à sua polícia local, que disse que isto era demasiado complexo para eles. O assunto escalou para a equipa da City of London Policing, que disse não poder fazer nada. E apenas porque eu conhecia pessoas, consegui pegar no telefone, e mesmo assim não obtivemos nada de volta.

Ninguém teve culpa; simplesmente tudo demorou demasiado.

E nesse caso, sabias que os fundos tinham chegado a uma *exchange* centralizada. Mas por vezes o problema está em chegar lá. Antes de os fundos chegarem a uma *exchange*, passam por todo o lado: *mixers*, esquemas de branqueamento de capitais, *chain hopping*, *bridges*. Consideras que esses são obstáculos genuinamente difíceis de ultrapassar? Achas difícil ultrapassá-los, ou há sempre uma pista, sempre um caminho?

Não, não são difíceis de ultrapassar.

A verdadeira questão é: em que caso se trabalha? As pessoas encontram-me – o meu número de telefone, o meu *email* – e entram em contacto: "perdi todo este di-

nheiro, não sei o que fazer". Recebo-os constantemente e tento ajudar, geralmente a título gratuito.

Por vezes há resultados maravilhosos. Há uns anos, recuperei 15 milhões de euros para uma senhora; está no segundo livro. Esses resultados são maravilhosos, mas é sempre uma questão de a que caso entregas o teu tempo, e a polícia enfrenta exatamente o mesmo dilema.

Toda a gente está no mesmo barco. A tecnologia não é necessariamente a parte difícil. As *bridges* são geríveis, há dez anos eu rastreava através de *mixers* com papel e caneta. Este trabalho é possível. Só demora tempo. Esse é o problema.

Mencionaste o rastreio com papel e caneta, e agora as ferramentas são muito mais desenvolvidas. Mas chega um momento em que tudo isto tem de ser escrito num relatório, apresentado a um tribunal e usado para fazer ou desfazer um caso. Quais são os erros mais comuns que vês os investigadores a cometer nesses relatórios?

É-me difícil responder a isso em 2026, porque trabalho principalmente com a polícia britânica – um privilégio enorme, são pessoas muito boas – e aqui investiu-se imensamente na formação de rastreadores de criptomoeda e de agentes da linha da frente: reconhecer quando algo é uma peça de prova relacionada com cripto, compreender as vantagens e desvantagens, saber como escrevê-lo. No âmbito da polícia britânica, estou a ver relatórios muito bons, declarações muito boas. Portanto, esse já não é o maior problema. O próximo problema – e é aqui que eu diria que está o maior desafio no Reino Unido – é a cadeia de compreensão. O representante legal tem de perceber o que foi escrito, depois o juiz, e depois doze bons homens e mulheres da comunidade que naturalmente não irão compreender como funciona uma *blockchain*. Uma das maiores vulnerabilidades é esta: o rastreio de criptomoedas é muitas vezes uma inferência. Uma inferência muito sólida, mas ainda assim uma inferência. Por isso, é muito fácil para a defesa perguntar "isso é 100%?". Devido à forma como um *cluster* é inferido, tem de se dizer: "não, não é 100%". E pode-se imaginar o que acontece a seguir. Já enfrentei isso no banco como testemunha – tal como acontece com a prova de ADN, em que alguém pode dizer "bem, é um em 17 milhões, mas não é 100%, pois não?". Não se consegue nunca ultrapassar completamente isso com atribuição inferida, e isso pode ser muito prejudicial. Boas acusações estão a ser deduzidas no Reino Unido, boas declarações estão a ser apresentadas, mas se o Crown Prosecution Service, os juízes e os júris as compreendem verdadeiramente: esse é o próximo grande problema.

«O PROBLEMA CONTINUA A SER A VELOCIDADE E A CAPACIDADE DE RESPOSTA DAS FORÇAS DE SEGURANÇA – A AMPLITUDE DE CAPACIDADE, A VELOCIDADE E A DISPONIBILIDADE DAS EXCHANGES PARA RESPONDER, E AS EXIGÊNCIAS DE PROVA PARA DECRETAMENTO DE UMA FREEZING ORDER PARA FAZER OS FUNDOS REGRESSAR ÀS VÍTIMAS»

Costumas assessorar também os advogados de defesa? Isso implicaria analisar as provas recolhidas e perguntar: "como é que destruo isto? Como é que demonstro que isto não conta a história que a acusação diz que conta?".

Fiz muito trabalho de defesa no passado, no crime digital em termos mais amplos. Mas há cerca de oito anos, quando nos mudámos para o trabalho com cripto, tomei a decisão de me focar em apoiar a acusação. Acredito absolutamente que todos merecem uma defesa sólida – na verdade, um querido amigo meu foi uma vez enviado por um juiz no meu curso especificamente para aprender a defender um cliente em que eu estava envolvido na acusação. Acabou por se tornar um ótimo amigo e fez um trabalho fantástico para o seu cliente. Mas já era uma tarefa suficientemente grande ajudar a treinar as forças de segurança ao nível certo, sem trabalhar também do outro lado. E muito cedo, à medida que o meu nome se tornou conhecido através dos livros, recebia chamadas tanto da acusação como da defesa em simultâneo. Estou na defesa nisto? Estou na acusação naquilo? Tornou-se incontrolável. Por isso, com as criptomoedas, posicionei-me do lado da acusação, não porque ache que os arguidos não merecem uma boa defesa, mas porque saltar entre os dois era simplesmente demasiado difícil de gerir.

O teu trabalho envolve exclusivamente o rastreio, ou também ajudas na construção da narrativa? Porque o mesmo rastreio pode suportar tanto uma explicação legal como ilegal, especialmente com o branqueamento de capitais, em que por vezes existe um crime subjacente e por vezes não...

É absolutamente verdade.

Por vezes utiliza-se um *mixer* por razões de privacidade e não para branquear dinheiro. E quer estejas do lado da investigação quer do lado da defesa, o viés de confirmação é humano, é inevitável. Como tentas proteger-te disso?

É uma área fascinante. O curso de OSINT que mencionei dedicava a primeira meia jornada ao viés, porque é muito difícil de abordar. Há demasiadas formas de viés numa investigação: algumas impostas por oficiais mais seniores, outras que surgem simplesmente da sensação de que alguém parece culpado, ou porque outras provas apontam nessa direção. É muito difícil de gerir.

O meu papel tem sido fundamentalmente ensinar e demonstrar: esta é a prova, estes são os graus de certeza que lhe estão associados, isto é definitivo, isto é inferido, e depois os investigadores têm de o documentar em conformidade. É muito, muito complicado.

Mas também ensinas como interpretar o que a *blockchain* te diz e como encontrar provas corroborantes de uma narrativa específica?

Sempre. Um dos problemas, David – e já o tocaste anteriormente – é que há simplesmente demasiadas técnicas agora. O que é que se ensina sequer? Sempre tentei criar competências de rastreio, com ou sem ferramentas, e deixar às forças de segurança e à representação legal adequada fazer o que entenderem com ela. Mas sempre achei que é criticamente importante não ser perentório quando algo não é perentório. É muito fácil usar a linguagem errada e ficar em sérios apuros quando se está a depor em tribunal. "Isto equivale a isto" é uma afirmação muito diferente de "isto quase certamente equivale a isto" – e esta última é geralmente a honesta.

Para concluir, estiveste dos dois lados, acusação e defesa, mas focando-te agora no meio: o que aconselharias a que os juízes estivessem atentos? Qual é a única coisa a que gostarias que prestassem atenção para avaliar se a narrativa da acusação ou da defesa se sustenta?

«POSICIONEI-ME DO LADO DA ACUSAÇÃO, NÃO PORQUE ACHE QUE OS ARGUIDOS NÃO MERECEM UMA BOA DEFESA, MAS PORQUE SALTAR ENTRE OS DOIS ERA SIMPLESMENTE DEMASIADO DIFÍCIL DE GERIR»

As criptomoedas, nos seus fundamentos, não são assim tão difíceis de entender. Ninguém tende a acreditar em mim quando digo isso, porque o tema se tornou uma tal teia de vídeos do YouTube e ruído que é preciso colocar tudo isso de lado e fazer uma pergunta simples: como funciona um livro-razão da Bitcoin? Porque fundamentalmente, é muito, muito simples. Como funciona um livro-razão de Ethereum? É ligeiramente diferente, mas igualmente simples. Nos meus primeiros cursos, usávamos uma folha de cálculo para ilustrá-lo, e chegámos mesmo a simular a mineração com um par de algoritmos simples.

Muito simples. Desenvolvemos programas de formação para o sistema judiciário, e se eles se envolvem neles já não sei. Mas o que esperamos é que compreendam os fundamentos, porque a partir daí podem fazer as perguntas certas. Os representantes legais são muitas vezes muito bons a turvarem as águas, a fazer com que algo pareça imensamente complicado: "Não se preocupe com isto, é difícil de acompanhar". Já vi isso muitas vezes. As criptomoedas não são difíceis.

Muito obrigado, Nick. Usaremos isso como a frase de abertura da entrevista: "As criptomoedas fundamentalmente não são assim tão difíceis de entender"..

Cita-a livremente – porque realmente não são. No início de *Investigating Cryptocurrencies*, uso o exemplo das pedras na ilha de Yap – a grande moeda de pedras – e como toda a gente na aldeia se lembra simplesmente de quem é dono de qual pedra. Isso é um livro-razão distribuído em todo o sentido. Quando me vendeste algumas ovelhas e eu te dei uma pedra, a pedra nunca se moveu, porque estas coisas têm o tamanho de uma pessoa. Limitámo-nos a dizer a toda a gente na aldeia que eu agora

sou dono da pedra que antes era tua. É assim que a Bitcoin funciona na sua totalidade: mudar a propriedade em livros-razão distribuídos. Muito simples.

Embora com a cripto, surjam novas pedras a cada dez minutos, o que é novo.

Exatamente, e é essa a maravilha de um livro-razão distribuído. Como escrevi no livro: no momento em que se contrata alguém para se sentar no meio da aldeia e registar quem é dono de cada pedra, isso chama-se um banco. Tiraste-o do livro-razão distribuído na mente de todos e colocaste-o num pedaço de papel. Essa é a diferença fundamental.

Nick, muito obrigado. Foi um verdadeiro prazer – estaremos em contacto.

Fantástico – obrigado por me teres convidado.

INTELIGÊNCIA ARTIFICCIONAL

Em 2058, *passwords* tinham desaparecido.

A autenticação fazia-se através de memórias: bancos, tribunais e governos validavam identidades usando recordações pessoais armazenadas em cofres neurais ligados à *internet*.

Até surgir o "Jardineiro".

As vítimas começavam a lembrar-se de crimes que nunca cometeram. Um juiz confessou um homicídio inexistente. Um ministro entregou códigos militares convencido de que tinha prometido fazê-lo anos antes.

Miguel Varela, especialista em investigação digital, descobriu que todas as vítimas tinham passado pela mesma empresa: MnemoSyn, uma clínica de otimização de memória.

Ao infiltrar-se nos seus servidores, encontrou milhões de memórias humanas catalogadas, editáveis e à venda.

Traumas podiam ser apagados. Álibis podiam ser descarregados. Testemunhos eram fabricados como ficheiros.

Mas o pior surgiu quando Miguel encontrou memórias suas no sistema — incluindo a recordação detalhada de uma filha que nunca existira.

Dias depois, começou realmente a lembrar-se dela: o nome, a voz, a gargalhada.

Percebeu então a verdadeira ameaça.

Num mundo onde a memória era a principal prova digital, quem controlasse as recordações controlava a própria verdade.

E a justiça tornara-se apenas um *software* vulnerável.

Imagem gerada por inteligência artificial.

DEFESA DIGITAL

A Defesa Digital é um serviço especializado da Morais Leitão, correspondendo às exigências jurídicas, técnicas e probatórias colocadas pela interseção entre o cibercrime e o Direito. ↗

Coordenação

DAVID SILVA RAMALHO
dsramalho@mlgts.pt

NUNO IGREJA MATOS
nimatos@mlgts.pt

ADRIANA BRÁS
adriana.bras@mlgts.pt

ANA S. PEREIRA COUTINHO
acoutinho@mlgts.pt

INÊS COSTA BASTOS
icbastos@mlgts.pt

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Head Office
LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTUGAL
ANGOLA
MOÇAMBIQUE
CABO VERDE
SINGAPURA
TIMOR-LESTE
MACAU

LexMundi Member

mlgts.pt

3D

3D: Digital Defense Dispatch
Coordenação David Silva Ramalho
Volume 2
Julho de 2026