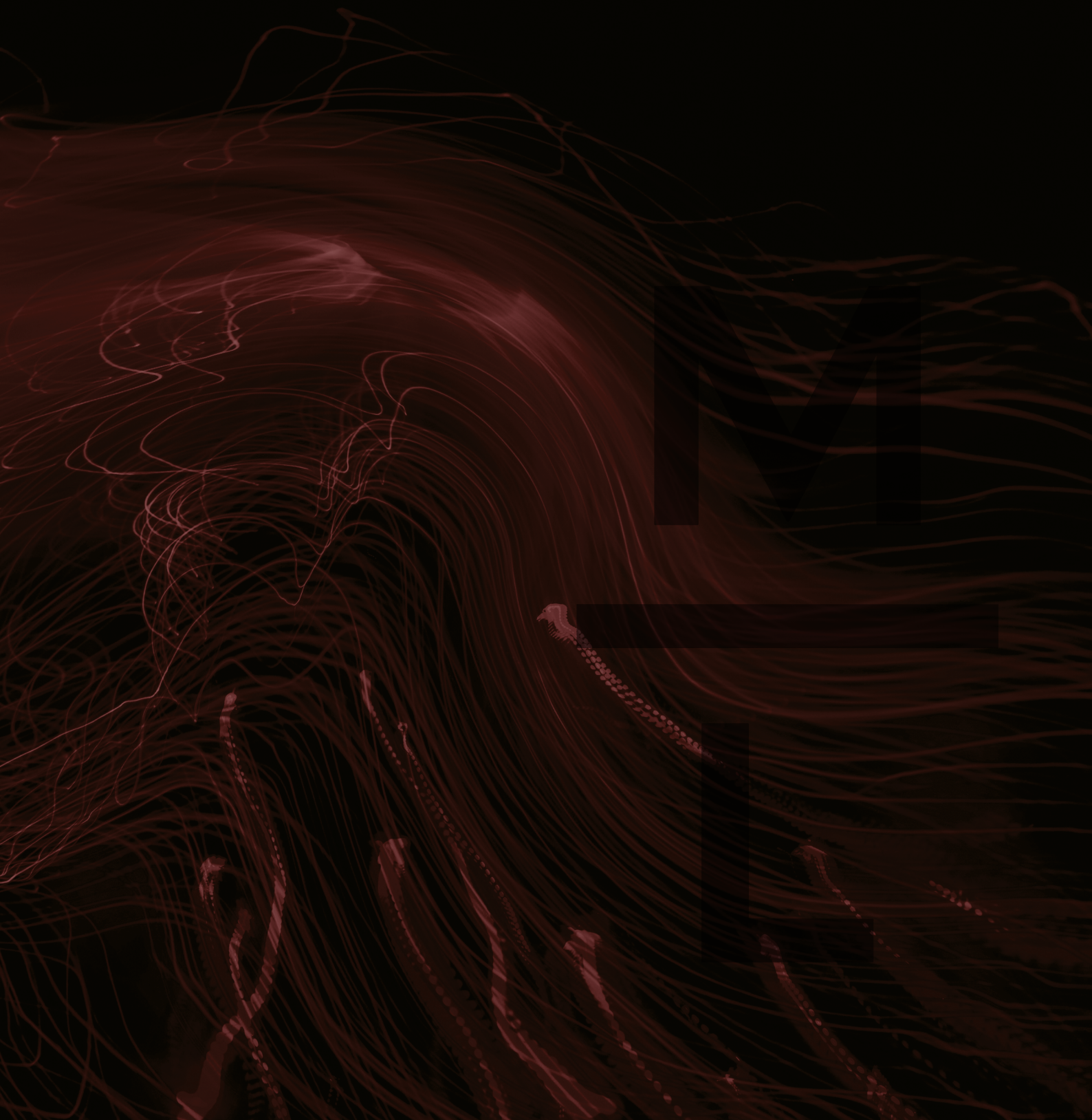
Vol. 2 July 2026

3D DIGITAL DEFENSE DISPATCH



DAVID SILVA RAMALHO

In December 2025, we launched the first issue of 3D. When we began preparing it, almost a year earlier, the idea was to create a newsletter condensing a roundup of news, legislation, and case law on cybercrime and digital evidence. We completed the first version of the newsletter, but the result felt incomplete, of little use, and lacking distinctive content. We then decided to try a different model. A model in which we could count on leading specialists in the field, willing to contribute freely and informally with their views on the topics they deal with on a daily basis.

That is how, sometime in January 2025, I spoke with Jan Kerkhofs, Head of the Cyber Unit of the Belgian Federal Prosecutor's Office, and asked him whether he would be willing to contribute an article on Sky ECC, the case that changed the paradigm of criminal investigation in Europe, and which Jan himself led. The answer was yes, and the project took on a whole new dimension.

At the end of January 2025, I spoke with Alexandre Senra, Federal Prosecutor of Brazil, an enthusiast and unparalleled expert in everything with crypto in its name, whom I had met approximately a year earlier during a Council of Europe course in São Paulo, and extended the invitation for him to give us an interview. Alexandre accepted, and the newsletter turned into a review.

Finally, I was fortunate that Nuno Igreja Matos and Inês Costa Bastos, office colleagues and friends, wanted to share the preparation of the first issue with me, and were even willing to contribute two texts of outstanding quality. The result was a first issue that would be hard to surpass.

As soon as we published it, we began preparing the next issue. Now under the pressure of what we had released in December, we decided to take as long as necessary to produce a second issue that would be no less than the first. Seven months later, here we are.

The idea for the opening of the second issue had existed since the first. When we decided to begin the Review with an article on the Sky ECC case, focused almost exclusively on the enforcement perspective and the need for investigative tools, we thought it would make sense to include in the second issue an article focusing on the other side – defence rights. That is how, in January 2026, shortly after the launch of 3D, I spoke with Maša Galič, Professor at *Vrije Universiteit Amsterdam* and an essential Author in the field, whom I had the pleasure of meeting in Kraków back in 2022, and presented her with the idea of writing an article on the subject. The result is a brilliant article, in which the Author questions the means used in the case and their outcomes, both as regards the reliability and authenticity of the evidence, and as regards the compatibility of the case's coordinates with the defence rights of those targeted.

Also in January, in conversation with Cláudia Pina, who had just returned to the judiciary from the European Judicial Cybercrime Network, I suggested she write a text on a topic of her choosing, drawing on the knowledge and experience accumulated during her time there. Cláudia chose a topic on which very little has been written and whose relevance is beyond question – hybrid threats. And she wrote it, as in her recent book, using the case method, in a style that makes it impossible to stop reading.

But since it is impossible to speak of new technologies without speaking of Artificial Intelligence, and given that this was a notable omission in the first issue, we decided to include an article specifically on that topic. I contacted Angelo Costanzo, Judge of the Italian Supreme Court (the *Corte Suprema di Cassazione*), with whom I had the pleasure of sharing a panel in Syracuse sometime in February 2023, and who has devoted extensive study to this and other matters, and he prepared a text, as complex as it is interesting, on the intersection between logic, legal reasoning, and artificial intelligence.

Lastly, Ana Xavier Nunes was generous enough to accept the invitation to contribute a text on cybersecurity, and with that text, also of outstanding quality, we closed all the written contributions.

There was still, however, an interview missing, in order to maintain the structure of the first issue. I took the liberty of contacting Nick Furneaux. Unlike all the other authors of both issues, I did not know him personally, but I had already read his books *Investigating Cryptocurrencies and There's no such thing as crypto crime*, and I knew he is one of the world's leading authorities on crypto-asset tracing, so I decided to take the chance. With Nick's affirmative reply, we closed the list of external guests (with an interview that, to Nick's credit, is excellent).

What remained was the most time-consuming part – compiling news, legislation, soft law, and case law from all corners of the globe – which is why this issue has only come out now. I am well aware that in the age of Artificial Intelligence this task should be easier, but there are things that, for now, cannot do without human supervision. If there were any doubts, one need only read the fiction story with which we close this issue, written by Artificial Intelligence, whose (low) quality leads to the conclusion that there is still room for human imagination.

And so, another issue of 3D is complete.

ARTICLES

What's access to the raw data set got to do with it? 4
Maša Galič
Assistant Professor Privacy and Criminal (Procedure) Law
Vrije Universiteit Amsterdam

Hybrid warfare in cyberspace – from Operation Eastwood to the Stânca-Costești Dam: when cyberspace becomes a battlefield 7
Cláudia Pina
Investigating Judge

From the preconscious to cybersecurity 13
Angelo Costanzo
Judge of the Italian Supreme Court

A big question for micro and small enterprises: the criteria for the application of the NIS 2 Directive and Decree-Law No 125/2025 of 4 December 24
Ana Xavier Nunes
Morais Leitão's Associate

NEWS

CYBERCRIME AND DIGITAL EVIDENCE 27

CRYPTO-ASSETS 29

LEGISLATION AND SOFT LAW 31

CASE LAW 33

Interview with Nick Furneaux: "Cryptocurrencies fundamentally are not that hard" 36
Author of *Investigating Cryptocurrencies* and *There's no such thing as crypto crime*
By David Silva Ramalho

ARTIFICTIONAL INTELLIGENCE 44

FIND OUT ABOUT OUR DIGITAL DEFENSE SERVICE 45

WHAT'S ACCESS TO THE RAW DATA SET GOT TO DO WITH IT?

MAŠA GALIČ
Assistant Professor Privacy and Criminal (Procedure) Law
Vrije Universiteit Amsterdam

On 21 January 2026, a Spanish first-instance court in Valencia acquitted multiple defendants charged with drug trafficking in one of the many Sky ECC cryptophone prosecutions currently pending across Europe. The judgment is remarkable because it falls into a very small group of European court decisions, where the reliability of digital evidence obtained through large-scale cross-border hacking operations was not accepted at face value. Instead, the court engaged with one of the foundational questions concerning the sharing of digital evidence obtained via a European Investigation Order (EIO): how should the authenticity and reliability of crypto-communications obtained through EIO-based cooperation be assessed? In this contribution, I briefly address this question by situating the Spanish court's reasoning within the broader discussion on reliability of digital evidence.

I. RELIABILITY AS MULTI-LAYERED CONCEPT

Questions concerning the authenticity and reliability of the intercepted crypto-communications, relate to broader issues of reliability of digital evidence, issues which are far too complex to answer in a short contribution, such as this one. In the context of digital evidence, the mere terms themselves – authenticity and reliability – are multi-layered and are oftentimes used in an inconsistent manner both in legal scholarship and by courts. In fact, discerning the exact distinctions between authenticity, validity, integrity and reliability in the digital context, all of which are also used in the Spanish judgment, is no easy task.

Furthermore, the processing of digital material in criminal investigations usually unfolds in several stages: (1) collection and securing of data; (2) extraction, storage, selection and analysis; (3) translation of digital material into written reports (as still required by many national legal systems); and (4) assessment of the written reports at trial.[1] Each stage raises distinct reliability concerns and therefore requires distinct safeguards.

In the initial stage of collecting and securing the data, the central issue is the chain of custody: where, how, and by whom were the data obtained, and how were they processed? The chain of custody therefore requires **authenticity** of the data (relating to their origin and identity) and **integrity** of the data (referring to the state of the data, which need to be intact and unchanged).[2] In practice, this is ordinarily achieved through forensic imaging, hashing,[3] and detailed logging. Even where such steps are followed, however, Sky ECC cases raise structural difficulties. The hacking method and tools used by French authorities remain classified. While such secrecy is legally permissible under French, Dutch and seemingly also Spanish law, it leaves receiving states largely dependent on assurances from the

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

2 ibid.

3 A hash value is a condensed representation of the binary (digitised) content of digital material, which is calculated for the purpose of an integrity check of digital material and efficient identification and classification of files. See Netherlands Forensic Institute (2021), "Technical Supplement – Forensic Use of Hash Values and Associated Hash Algorithms", available at https://www.forensicinstitute.nl/documents/2018/02/13/forensic-use-of-hash-values-and-associated-hash-algorithms.

executing authority regarding the integrity and authenticity of the data.

II. FROM CHAIN OF CUSTODY TO CHAIN OF EVIDENCE

During the second stage, whereby data are extracted, filtered, stored and analysed, the chain of custody remains an essential requirement, since the collected data need to remain intact during their processing too. This stage, however, introduces an additional requirement: the chain of evidence. The chain of evidence asks, which choices were made during the processing of data, including which interpretations? This stage of the processing is therefore concerned not only with the preservation of data, but also the validity of the tools and interpretative choices applied to it. Which datasets were selected? Which filters were used? Are the results consistent and reproducible? These questions go to methodological validity rather than mere integrity.

It is during this stage, specifically relating to the chain of evidence, that things have gone awry in the Spanish case. According to the judgment, French authorities filtered the dataset at least twice before sharing it with Spain. The Spanish police received a link to download a zip file, copied it onto two USB memory sticks (one deposited with a court, one for operational use), and proceeded with their investigation. Crucially, the Spanish agents acknowledged that the files received from the French were not accompanied by hash values or digital signatures. Their only assurance was that the USB stick delivered to the court contained everything they had downloaded.

This means that the chain of custody during this phase was not technically established. Moreover, the judgment contains no examination of the chain of evidence: no information about the filtering criteria used by the French authorities (or Europol), no validation of analytical tools, and no assessment of reproducibility.

Despite these deficiencies, the Spanish court initially held that reliability could nevertheless be sufficiently established from the statements made by the Spanish officers who downloaded the file and the French documentation attached to the European Investigation Order.

III. SOLE EVIDENCE AND ARTICLE 6 ECHR

The decisive turn in the Spanish judgment came from a different direction. The court ultimately acquitted because the Sky ECC communication constituted the sole evidence against the defendants. The Spanish court concluded that in order for the right to a fair trial in Article 6 ECHR to be guaranteed, the defence would have needed to be allowed access to the "raw data" obtained from the interception ordered on the servers used by the company SKY ECC.

This reasoning aligns, at least in spirit, with Strasbourg doctrine: equality of arms and the accusatorial principle require that the defence be placed in a position to test the prosecution's evidence effectively. Yet, the judgment is conceptually imprecise. Access to raw data, by itself, cannot repair defects in the chain of custody.[4] Nor can it retroactively establish the integrity of files transferred. [Just as statements by officers who downloaded the file cannot be a substitute for the absence of any technical guarantees]. At most, raw data combined with information on the filtering tools and methods might allow the defence to assess the consistency and reproducibility of the filtering, relating to the chain of evidence. But that was not called into question in the case at hand.

[4] See my discussion on the levels and types of access to the various types of data sets in the case law of the European Court of Human Rights: M. Galič (2021), "De rechten van de verdediging in the context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken", *2 Boom Strafblad*; draft in English available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3838680.

IV. A MODEST BUT IMPORTANT STEP

For all its shortcomings, the Valencia judgment represents an important departure from the largely deferential approach adopted by courts in several other Sky ECC jurisdictions. While the Spanish court's focus on raw data access does not properly address the underlying digital forensic problems, the judgment nevertheless marks a first judicial attempt acknowledging that large-scale cross-border hacking operations create evidentiary black boxes that cannot be reconciled with Article 6 merely through an abstract principle of mutual trust.

HYBRID WARFARE IN CYBERSPACE – FROM OPERATION EASTWOOD TO THE STÂNCA-COSTEȘTI DAM: WHEN CYBERSPACE BECOMES A BATTLEFIELD

CLÁUDIA PINA
Investigating Judge

I. THE UNDECLARED THREAT

Hybrid warfare has no front line. There is no formal declaration of hostilities, no uniforms, no clearly identifiable enemy. What exists is a calculated orchestration of economic, cyber, informational and sabotage instruments, designed to pressure, destabilise and weaken a State without that State, or its allies, being able to legitimately invoke the classical mechanisms of military response.

This is its strength and its legal perversity. Hybrid threats deliberately operate below the formal threshold of war, occupying a grey zone, a space between armed conflict and peace. It is precisely in this zone that the law faces its greatest difficulties: the rules of International Humanitarian Law apply to armed conflicts; national Criminal Law has limited response capacity when agents operate from non-cooperating jurisdictions; and Public International Law lacks rapid-response mechanisms for acts that, individually, may appear minor, but which together constitute a systematic aggression.

However, this grey zone is not a normative vacuum. Existing law – domestic, European and international Criminal Law – already provides us with instruments to classify, prosecute and deter these acts. What is lacking is not rules. What is lacking is evidentiary capacity, institutional coordination and political will. The two cases that follow illustrate this argument: the first, a real case, shows what the justice system can already do; the second, a hypothetical case but grounded in real data, shows what it may be called upon to address.

Advanced Persistent Threat groups, referred to in the technical literature as APTs, are the operational arm of this strategy. They are not solitary hackers driven by curiosity or immediate greed. They are organised structures, frequently funded or tolerated by States, that follow methodical operational cycles: reconnaissance, infiltration, expansion and exploitation.

II. OPERATION EASTWOOD: CYBERCRIME, TERRORISM AND THE LIMITS OF LEGAL CLASSIFICATION

It was spring in Central Europe. On the screens of dozens of ministries, parliaments and public bodies, access was becoming impossible – not due to technical failure, but by design. Somewhere, on a server whose location was deliberately opaque, a group called NoName057(16) was unleashing its routine of silent destruction.

The pro-Russian group NoName057(16) had been operating for months in a disciplined manner, combining distributed denial-of-service (DDoS) attacks with a gamified recruitment

structure. Approximately 4,000 users were mobilised through messaging applications such as Telegram, receiving cryptocurrency rewards for each successful attack. Targets were carefully selected: critical infrastructure and government bodies in European countries that supported Ukraine or expressed alignment with NATO. The attacks were timed to coincide with politically sensitive moments – summits, parliamentary votes, announcements of military support – amplifying their media impact.

The response to this threat was coordinated. Under the aegis of Eurojust and Europol, twelve countries participated in an operation that dismantled the group's central infrastructure, issued seven international arrest warrants and disrupted more than one hundred servers worldwide. Participants recruited through social media were notified of their criminal liability. The face of one of the alleged leaders, a Russian national, was placed on the European Union's most wanted list – an act of public naming that carries both deterrent and symbolic value.

DDoS **attacks are an example of cyber-dependent crime**: offences that exist only in cyberspace and depend entirely on digital means for their commission. Operation Eastwood classified the conduct of NoName057(16) as organised crime and cybercrime. It is a legally sound option but one that leaves more severe sanctions unexplored.

The objective and teleological elements of the group may lead to the conclusion that its activity falls within the definition of a terrorist offence for the purposes of Article 3(2) of Directive (EU) 2017/541 and Article 2(3) of Law 52/2003, of 22 August: acts likely to seriously intimidate a population, compel governments to change policies and destabilise the fundamental political, economic or social structures of a State. Both the Directive and Law 52/2003 expressly refer to attacks on critical infrastructure as an autonomous category. In the case of APT NoName, the intention behind the attacks was not a financial one, but political and intimidatory, and their timing confirms this, allowing their integration within the concept.

Classification as terrorism could have allowed, in some jurisdictions, access to reserved investigative measures, extended pre-trial detention periods, asset freezing and facilitated access to data held by private entities. In the legal systems of the countries participating in the operation, this avenue was available. That it was not used reflects an understandable hesitation, for classifying as terrorism an attack tolerated or funded by a sovereign State entails a position of considerable diplomatic weight. This ambiguity in classification, this hesitation in moving from the designation of a mere criminal organisation to that of a terrorist group, is itself a problem that requires better coordination in transnational cases of this nature.

Even without the classification of NoName as a terrorist group, its principal members, even if resident in non-cooperating jurisdictions such as the Russian Federation, are not immune from the domestic criminal law of the targeted States. The conduct in question, described in Article 5 of the Budapest Convention and the national legislation of the targeted States, may allow, in accordance with the Criminal Procedure Law of each State, the institution of proceedings *in absentia* and the issuance of international warrants for the moment when conditions change and it becomes possible to bring each perpetrator before a court, given that the plausible deniability of the sponsoring State does not extinguish the individual criminal liability of the identified operators.

III. THE NIGHT THE PRUT BECAME A WEAPON: A DIGITAL WAR CRIME?

The Stânca-Costești Dam, built between 1974 and 1978 as a joint project between Romania and the former USSR, stands on the river Prut, the border between Romania and the Republic of Moldova. Its location is special: the Prut rises in Ukraine, in the Carpathians, serves as the natural border between Romania and Moldova along 711 kilometres, and flows into the Danube, making the dam a point of confluence of three

sovereignties and one of the most sensitive cross-border infrastructures in Eastern Europe.

The reservoir has a total capacity of 1,285 million cubic meters and an area of 59 km². The dam measures 48 meters in height and 740 meters in length. Its primary function is the protection of the Prut floodplains: it was built to prevent a recurrence of the catastrophic floods of 1970. In 2008, with the dam in controlled mode releasing water at 845 m³/s, the authorities classified the situation as a threat to the 15,000 people in the 13 downstream localities and proceeded with a partial evacuation. Even so, more than 300 dwellings were affected and approximately 180 completely destroyed.

In the early hours of 24 April, it was raining heavily. The waters of the Prut were running high. The Stânca-Costești reservoir was at 91% capacity. Despite this, it was a normal spring scenario for the operators on duty; what they did not know was that for months they had not been alone in the systems.

In November, members of an APT with documented links to military intelligence services of an Adversary State had obtained remote access to the dam's SCADA management system through an unpatched vulnerability in an industrial control module. The entry vector was a phishing attack directed at a maintenance engineer subcontracted for systems maintenance. Once the malware was infiltrated, it remained in "living off the land" mode, hibernating silently until the trigger of 90% reservoir capacity was reached.

As programmed, at 03:33 AM, with strong winds, heavy rain, high inflow and maintenance crews reduced to the minimum night shift, the discharge gates were opened suddenly and in an uncontrolled manner. In the first minutes, the operators thought it was a system failure. They attempted to restore the commands digitally, without success.

While the operators desperately attempted to activate the physical redundancies, rescue teams were dispatched to a riverbed that had already become a deadly torrent. Precisely one hour later, on the Ukrainian side, surgical explosions destroyed the protective dykes, releasing a wall of water that travelled like a hydraulic piston over the already full flow, striking the dam with an unstoppable kinetic force.

The decision became impossible: close the gates and risk total structural collapse, or keep them open and let the flow run towards Moldova. Due to the low geography of the left bank, the catastrophe was brutally asymmetric, resulting in more than six thousand Moldovan dead and the annihilation of their rescue teams, compared to approximately one thousand Romanian victims. On social media, the disproportion of resources, with Romania mobilising EU emergency assets while Moldova sought to recover from the catastrophe with scarce resources, was used to fuel the narrative that Bucharest had known about the attack and sacrificed the "brother country" to save itself, sealing a definitive and traumatic geopolitical rupture.

No State declared war. A spokesperson for the Adversary denied any involvement, suggesting that the Ukrainian secret services had been involved in the sabotage of infrastructure in their own country in order to lay the blame on it.

IV. LEGAL FRAMEWORK

For a cyberattack to be classified as a war crime under Article 8 of the Rome Statute, three cumulative elements are required: the existence of a sufficient nexus with an ongoing armed conflict, serious effects on the civilian population, and intentionality within the meaning of Article 30 of the same Statute. In the scenario described, all three elements are present.

The first element, the so-called "war nexus", requires that the act be sufficiently linked to an ongoing armed conflict. The international armed conflict between Russia and Ukraine provides this anchor. The link is geographical, doctrinal and strategic. The River Prut rises in the Ukrainian Carpathians, and the upper watershed of the Stânca-Costești Dam includes Ukrainian territory. A catastrophic discharge

would directly affect the Moldovan districts that today constitute a critical logistical and humanitarian corridor for the Ukrainian war effort, namely the Ungheni infrastructure and the Iași–Chișinău railway corridor.

Moldova, a candidate State for European Union membership with a Russian military presence in Transnistria, is itself a fragile actor whose institutional or humanitarian collapse would serve identified Russian strategic objectives. The destruction of water infrastructure as an instrument of strategic pressure is, moreover, a documented feature of conduct in the Ukrainian conflict: the collapse of the Kakhovka Dam in June 2023 deprived hundreds of thousands of people in southern Ukraine of drinking water, and the International Criminal Court's investigation into that event analyses precisely Articles 8(2)(b)(ii) and (iv), of the Rome Statute, relating to the intentional attack on civilian objects and excessive harm to the civilian population.

The Tallinn Manual, a non-binding but authoritative guide produced by the NATO CCDCOE, establishes that a cyber operation constitutes an attack within the meaning of International Humanitarian Law when it can reasonably be expected to cause damage, destruction, death or injury. The criterion is the effect, not the means employed. Malware that opens the gates of a dam is legally equivalent, for the purposes of International Humanitarian Law, to the hand of a saboteur who opens them manually.

Dams further benefit from enhanced protection under Article 56 of Additional Protocol I to the Geneva Conventions, which classifies them as installations containing dangerous forces. Their attack is prohibited even when they constitute military objectives, if the foreseeable effects would be the release of forces causing severe losses among the civilian population. This enhanced protection is mirrored in Rule 42 of the Tallinn Manual. In the scenario of the Stânca-Costești Dam, there is not even a military advantage to be gained: the nocturnal discharge of water upon sleeping civilian populations serves no identifiable combat objective.

Article 30 of the Rome Statute requires that the agent have knowledge of the circumstances and foresee the consequences in the ordinary course of events. In the scenario described, the deliberate choice of timing – night, reservoir at 91% capacity, maximum inflow – evidences precisely the knowledge and foresight that the discharge would cause civilian casualties. The Pre-Trial Chamber of the International Criminal Court has recognised that this pattern of intentionality may be inferred from the operational circumstances, regardless of confession or direct documentary evidence.

The greatest procedural obstacle is evidentiary, not normative. The attribution of a cyberattack to a specific agent, with the degree of certainty required by criminal proceedings, is technically complex: APTs operate through deliberately fragmented infrastructures, with servers in multiple jurisdictions, masked IP addresses and shared code designed to create attribution confusion. However, the principle of superior responsibility, provided for in Article 28 of the Rome Statute, partially circumvents this obstacle: a superior, whether military or civilian, may be held criminally liable for crimes committed by subordinates if he or she knew or should have known that they were being committed, and failed to take reasonable measures to prevent or punish them. Applied to the cyber operations of a State, this principle allows the chain of command to be ascended beyond the individual operator, even if that operator is in Russian territory. Plausible deniability is not an absolute legal shield.

In December 2025, the International Criminal Court published its Policy on Cyber-Enabled Crimes under the Rome Statute, confirming for the first time in an express and systematic manner its intention to investigate and prosecute international crimes facilitated by cyber means. The document does not create new rules; it applies the Rome Statute to cyberspace, confirming that the digital form does not alter the criminal substance of the acts. An attack on the Stânca-Costești Dam, committed in association with the ongoing armed conflict in Ukraine, satisfies the criteria of this Policy in three dimen-

sions: it is an act perpetrated by cyber means, it causes serious physical effects on civilian populations, and it occurs in a geopolitical context with a sufficient nexus to an international armed conflict.

V. WHAT CAN THE JUSTICE SYSTEM DO?

The justice system's response to hybrid threats of cyber origin must be structurally honest about its limits. Retaliation against the sponsoring State, sanctions, coercive diplomacy and cybercounter-attack measures belong to the toolbox of diplomacy and national security, not to the justice system. Its role is the production of evidence and the attribution of individual criminal liability, even when effective prosecution remains frustrated by the borders of non-cooperating States. Four best practices emerge from the experience of Operation Eastwood and recent developments in international criminal law.

The first is public naming and judicial prosecution. Through European or international arrest warrants, wanted lists and public criminal proceedings, the justice system creates mechanisms of pressure and deterrence that transcend mere individual sanction: they increase the reputational and operational cost for the adversary and for the proxy recruitment market. The act of making the face and name of an APT operator public, even if he or she resides in Moscow, constrains their future mobility and signals to the criminal ecosystem that impunity has limits.

The second is international judicial cooperation. European Investigation Orders and mutual legal assistance instruments in criminal matters allow the consolidation of attribution evidence with procedural value across multiple jurisdictions simultaneously. Operation Eastwood demonstrated that twelve countries can coordinate joint action, including searches, seizures and digital notifications, **on a single Action Day**. This coordination should be the norm in similar cases.

The third is coordination with the intelligence, defence and private sector ecosystem. The investigation of complex cyberattack cases requires technical information from sources that the justice system does not produce autonomously, namely signals intelligence, digital forensic analysis of equipment, and data from cybersecurity companies. The procedural integration of this information, to the extent possible that it may serve as evidence, is a necessary condition for attribution proceedings with criminal value.

The fourth is the preservation of evidence for the future. Even when immediate prosecution is unfeasible, the rigorous documentation of cyberattacks with humanitarian impact constitutes the basis for national courts or, subsidiarily, the International Criminal Court, to act when the political window opens.

VI. CONCLUSION

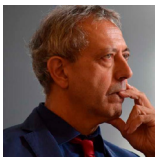
The Stânca-Costești Dam is not a metaphor. It is a real infrastructure, with published capacity data, with 15,000 people documented in its downstream risk zones, with a history of catastrophic floods and with digital control systems that share the structural vulnerabilities of any legacy SCADA system. The scenario described in this article is framing fiction, but it is built upon real hydrological facts, documented operational precedents and an analysis of consequences that the official records of the 2008 floods themselves allow us to project.

Hybrid warfare in cyberspace dissolves the boundaries between crime and war, between the digital and the kinetic, between State responsibility and individual responsibility. Existing law already offers a response on two complementary planes: on the plane of domestic and European law, state-sponsored hybrid attacks must be classified, according to their nature and gravity, as cybercrimes, organised crime or terrorist offences under Directive 2017/541 and Law 52/2003, with all the procedural instruments that each classification makes available, regardless of the location of the operators. On the plane of international law, where the nexus

with an ongoing armed conflict is established, together with the existence of serious effects on the civilian population and the intentionality required by the Rome Statute, the path of war crimes before the International Criminal Court ensures reach over the principal instigators and institutional memory of the act.

The challenge is not one of normative gaps. It is one of evidentiary capacity, international coordination and institutional will. Operation Eastwood showed that it is possible to act on the criminal plane against state proxies in hybrid warfare. The scenario of the Prut dam shows that the potential scale of the next step requires that the justice system, both national and international, be properly coordinated before the wave arrives.

FROM THE PRECONSCIOUS TO CYBERSECURITY



ANGELO COSTANZO
Judge of the Italian Supreme Court

I. BI-LOGIC

The logic of the twentieth century has provided two powerful tools for refining the idea that reasoning is a verbal process, but, at the same time, it is an internal action of the psyche.[1]

The first is constituted by **non-classical logics**, which have legitimised deviations from logical principles (non-contradiction, third excluded) that tradition has understood as fundamental but which in arguments are ordinarily relativised.

The second is offered by bi-logic, which gives shape to a broader perspective, in which informal arguments and formal demonstrations can be understood as forms of reasoning stationed at the same level as emergence from the prelogical foundations of thought.[2]

The central ideas of bi-logic are as follows. When conscious, the mind can approach its objects in two ways: one analytical (distinguishing, dividing) and the other analogical (assimilating, unifying). The first way connects the objects it has distinguished through logical relations. The second way treats the set of its objects as a homogeneous totality: it reveals aspects of the observed field that are sometimes not otherwise accessible, but, because it is rooted in the soil of the preconscious, it can mislead the discursive thought. Bi-logic accesses the levels of thought behind the two modes, interpreting states of mind as interactions between the tendency to follow symmetrical relationships and the propensity to establish asymmetrical relationships.

The **symmetrising logical principle** treats objects and their classes as components of larger classes, propagates unconscious assimilations, not moved by discernment. They are governed by **symmetrical relationships**: dream activity, fantasies, drives, the most intense emotions, creativity (which, however, requires that the ability to distinguish objects that are unified in the meantime not be lost, because, as *ex contradictione quodlibet sequitur* so *ex indistinctione quodlibet sequitur*).

The **asymmetrical logical principle** proliferates distinctions, treats a particular object as a component of a class (following the scheme of conceptual ramifications of the classical "Porphyry tree") and while the products of **symmetrisation** tend to become indistinguishable, those of **genericisation** are clearly distinguishable from each other, so that they are treatable by a logic with two truth values (**true, false**). The total application of the **symmetrising principle** would lead to the absence of negation and to the

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

2 The author of bi-logic is I. Matte-Blanco, to whose main works we must refer: *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.

total identifiability (indiscernibility) between objects. On the other hand, since it interacts with the **asymmetrical principle**, it is possible to regiment – in different ways and degrees – disorder thus avoiding logical chaos. The result is a bi-logic, which however can only be described through its asymmetrical component: **classical logic** (a bulwark against the disintegrating force of emotions and impulses).

II. ARGUMENTATION AND *ARS DISTINGUENDI*

Much of the data and its correlations is lost in the transition from the pre-conscious to the conscious elaboration of an argument expressed in the forms of a discourse, but this passage is indispensable for communication and useful for controlling its contents.

In any case, the bi-logical reading of an argument (of the individual arguments and their connection in a reasoning) is not always possible, it is never simple, it involves the risk of serious misunderstandings or mere inferences and, in any case, it is inevitably destined to remain incomplete.

However, even taking just a few steps in its direction can clarify some psychological roots of reasoning, its degrees of **cogency** and the fallacies that can vitiate it: manifest reasoning takes place against the background of extensive bases, destined to remain enthymematic, of inexplicit assumptions and subtleties not always shared between those who express themselves and those who read or listen.

The argumentation with which the treatment of a theme is developed can evoke, organise and intertwine in different ways a varied multitude of relationships, each characterised by its own proportion between symmetrical and asymmetrical relationships.

The persuasive power of an argument is influenced by the combination of asymmetrisation and symmetrisation, between logic (of identity, which supports deductive inferences) and analogical logic (of similarity, which supports inductive inferences and abduction). This interweaving is effective if it respects a fundamental canon: logical cogency has (if recognised) a persuasive efficacy in itself, to which the (psychagogenic) force of the various forms of symmetrisation can be added but not replaced.

The logical relationships between the data used connect the vertices of complex structures, which incorporate myriads of latent associations between data and evaluations that usually remain unexpressed but sometimes re-emerge and, in various ways and for various reasons, surreptitiously insert themselves into the articulations of explicit discourse.

This reservoir of information and connections provides the necessary material for the exercise of the *ars distinguendi*, a natural art, because it is linked to the spontaneous attitude of the mind to associate and dissociate notions and judgments, which is refined with experience in the various fields of knowledge and practice.

The *ars distinguendi* has value in all areas of knowledge but in law, in particular, it constitutes a necessary constant exercise to grasp the specificity of cases and avoid the inconsistencies that derive from treating dissimilar situations in a similar way, *i.e.* differentiable on the basis of a legal principle that is relevant to the case or on the basis of a different hypothesis of reconstruction of the events.

The search for reasons to exclude what was admitted as a similarity and turn it into an essential diversity may depend on the different levels of analysis: two objects may appear similar at one level but at another they may differ.

In reality, "Porphyry's tree" (the one of conceptual branches) can develop in different ways and in different ways you can climb or perch on its branches. The intellectual spring that leads to associating or dissociating notions arises from an option within the psychology and cultural training of the interpreter that can be translated into a legally relevant datum if it is anchored to significant factual circumstances in relation to

the normative data (especially the principles) offered by the legal system.

The *ars distinguendi* is the basis of the most important arguments that develop in the legal field: to resolve the incompatibilities between normative data (when the legislative criteria for resolving antinomies do not help), to reject a previous interpretation, to find an exception, to set aside a maxim of common experience. Accurate interpretation can increase legal uncertainty, because it raises new problems by revealing unexpected complexities, but it benefits Justice.[3]

III. ARTIFICIAL RATIONALITY AND LEGAL REASONING

Just as the transition from the pre-conscious to discursive thinking involves a reduction in the data and correlations that can be consciously used, so the transition from argumentation to crystallisations of the meanings of terms and inferences that is achieved with the methods of artificial intelligence involves a further impoverishment of reasoning, due to simplifications and mechanisations that can be useful as long as those who use them remain vigilant on the limits of the tools they use.

In particular, algorithms with artificial rationality lend themselves to being used in various areas of interest for legally relevant decisions, but (at the current state of their development) they cannot follow paths that go beyond the guidelines of formal logic to enter the field of argumentation.

Artificial intelligence cannot replace the jurist but it can provide him with aids.

A. RELIABLE DEDUCTIVE EXPERT SYSTEMS

Algorithms offer the best and least problematic results when they produce expert systems – those that operate according to a logic that is fully controlled by those who design them and by the user who (by studying and updating) is able to understand how they work, so as to use them as tools to support operations that they could also complete on their own.

The logical models that govern expert systems are based on rules focused on the inferential connection between antecedent and consequence (if... → then...). For years there have been useful practical applications to speed up operations based on a deductive logic, such as, for example, among the simplest: the calculation of the statute of limitations for crimes or the quantification of compensation or compensation for damage on the basis of predetermined criteria.

In addition, legal informatics can help to discover pseudological procedures: by introducing into the legal itinerary canons of correctness or at least transparency of impropriety. This applies both to the analysis of legislative texts (to their drafting and to the inferences that can be drawn from them) and to the analysis of judgments and administrative measures (for their contents and for the inferences that can be drawn from them). The different interpretative and inferential criteria can lead to a plurality of plausible results, but not all of these results derive from intellectual operations that respect the principles of formal logic.

Computational law can be used for this purpose, which concerns the representation of facts and rules through formal logic and the use of mechanical reasoning techniques to derive the consequences of facts and rules as represented through formalised propositions. The major current limitation of **computational law** is the same as that of general computational logic: it does not go beyond **propositional calculus**, *i.e.* **logical calculus** in which the analysis of inferences is conducted at the level of propositions without investigating the internal structure of the propositions themselves.

Even with this limitation, some algorithms could be profitably used to verify the logical correctness of a part of the arguments concerning the

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

proof of facts, identifying formal fallacies in the reasoning and, first of all, its manifest illogic.

To this end, however, a purification of the language with which the evidentiary arguments are expressed is required in order to adequately take care of their logical form and make them treatable by programs that use **expert logical systems** and this involves a cultural evolution in the training of jurists to enable them to exploit this potential.

B. INEXPERIENCED INTELLIGENT MACHINES AND PITFALLS OF INDUCTIVE LOGIC

The operation of algorithms open to the acquisition of information, in addition to those with which they are equipped as initial premises, through forms of machine learning by the systems themselves. It is based on extracted generalisations of (evaluated as) similar cases.

These algorithms do not have the ability to adequately consider the circumstances of each concrete case also because, in any case, they are not able to obtain all the information that would be necessary.

Neural networks aim to overcome these limitations by means of flexible adaptation strategies to the environment, with a parody of the animal neural system. But the uncertainty remains inherent in systems based on machine learning that does not allow us to exclude that the new case examined, although similar to the previous ones in terms of characteristics considered by the network, does not fit the prediction. This condition is not resolved, indeed it could be aggravated, by the possibility of such systems (which, therefore, turn out to be **inexperienced**) to use large masses of data as examples from which to extract correlations and generalisations. Moreover, unlike a **decision tree** on which an expert system is centred, the neural network does not directly provide comprehensible explanations for its **outputs**, so it is comparable to **a black box** devoid, by definition, of transparency.

C. ARTIFICIAL INTELLIGENCE AND DIALECTICAL RATIONALISM

The model of argumentation traced for evidentiary reasoning in trials is inspired by dialectical rationalism and in this direction, the *Charter of Ethics on the use of artificial intelligence in judicial systems and their environment*, adopted on 3 December 2018 by the European Commission for the Efficiency of Justice Systems (CEPEJ) requires **logical** coherence algorithmic calculations in a decision-making process in accordance with the principles of procedural law. In other words, the algorithmic result must be corroborated by evidence that is elaborated according to the dialectical method and that requires human intervention.

In some time, it will also be possible to develop a new formal logic (broader than traditional deductive models) to package models of legal reasoning (not reducible to mere syllogisms), and to design expert systems capable of grasping the dialectic of opposing arguments and using techniques to attack and refute them. It is a matter of formalising the so-called **defeasible reasoning**, *i.e.* the reasoning that is convincing but that is not deductively valid because it could be disavowed by specific exceptions and, therefore, subject to refutation.[4]

Less easily predictable seem to be formal systems capable of evaluating (by themselves) the weight of arguments, because the strength of an argument also depends on the context in which it is placed and the context depends on changing circumstances.

In any case, the fact remains that at the moment the various artificial intelligence systems – when a certain threshold of complexity of the issues is exceeded – are not able to offer what human intelligence can easily and correctly produce (if well educated and if accustomed to monitoring its mental states). So, it is clear that resorting to the application results of theoretical elaborations that are interesting for their possible

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

further application developments, but still embryonic.

In the meantime, it seems necessary to provide those who engage in the production of law and those who deal with its application with the intellectual tools necessary to maintain control of the situation **in progress** and profitably use the contributions of artificial intelligence. What this reserves for the future, in the part in which it is predictable, has limits that are sources of perplexity. However, beyond many of their imaginative anticipations, to some extent the changes will take place. If they are very fast, you will only become fully aware of their effects after they have occurred. Just think of the consequences (mainly but not exclusively positive) of the use of information technology for legal documentation which, moreover, despite its breadth, remains conceptually controllable by its users.

What is needed in the meantime, however, is a thoughtful recomposition of the various university teachings concerning legal informatics with its growing ramified developments,[5] so as to include it among the components of the renewed *artes sermocinales* so that these, from the traditional (and now neglected) arts of the *trivium* (grammar, rhetoric, dialectics) expand to modern interdisciplinary tools, such as: the basics of general linguistics, logic with its ramifications in computer science and probability calculus, methodology.

IV. LOGICAL FALLACIES AND CYBERSECURITY

In **the infosphere**, information flows seamlessly through computer networks: from personal and banking data to industrial and military secrets, a wide range of sensitive information becomes a target of conquest and/or defence.

A. INFOSPHERE AND SECRET SERVICES

Intelligence agencies use AI to manage and interpret massive amounts of data from different sources – including digital communications, electronic sensors, dark web, trojans, various forms of malware, as well as information collected from people – to prevent threats to national security by identifying patterns, anomalies, and potential threats that are difficult to discover manually.[6]

Through AI, reactions to security incidents can be automated and made very fast. Smart systems can autonomously block suspicious addresses, quarantine infected devices, or initiate countermeasures based on predefined rules.

The use of drones, GPS geolocation and internet-connected devices, integrated with AI, allows for more precise and widespread real-time surveillance.

AI also changes counter-espionage, helping to recognise audio and video falsifications (deepfakes) and to counter media counterfeiting, a phenomenon increasingly used to misinform or manipulate. Online platforms, managed by private individuals, as well as **large language models** (LLMs), can be used to influence individual and collective choices and strategies or to convey encrypted or steganographic messages.

While, by automating them, it makes operations faster and more precise. AI also raises new ethical and confidentiality issues, and also presents risks of fallacious and misleading outcomes.[7]

B. PATTERNS, UNCERTAINTIES AND ANOMALIES

The relationship between AI and **cybersecurity** is ambivalent, because AI represents both a powerful ally in cyber defence and an asset for attackers through its ability to analyse large vo-

[5] For a historical exposition of the relationship between legal informatics and the training of the jurist: 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.

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

lumes of data to identify patterns and detect anomalies.

In particular, AI analyses massive amounts of data in fractions of a second, detecting anomalies and suspicious behaviour with greater accuracy than traditional methods.

Knowledge of normal behaviour patterns is critical to preventing more advanced threats (such as attempts to impersonate high-profile people within organisations). By analysing a vast amount of data, AI makes it possible to identify correlations that would be difficult to recognise and that can be seen as clues to potential attacks. In summary, AI establishes **patterns of normalcy** through continuous learning from data and then detects any deviation from this pattern as an anomaly, which can signal a potential cyber threat.

However, if **machine learning** can allow the early identification of a threat, the next problem is how to respond promptly to the threat, even taking into account the possibility of fallacies in data analysis.

Artificial intelligence is therefore a double-edged sword in cybersecurity: it can strengthen defences but also make offensives more sophisticated, it reduces some uncertainties but can also generate others.

Its tools, in their various forms, from expert systems – based on deductive logic – to intelligent machines – which work according to algorithms governed by inductive logic, correlations and probabilistic calculation – are mentally (electronically) lively but can turn out to be intellectually lazy and not as rational as human minds (individual or collective) can be, when they act in conditions of serenity and without time limitations, so as to make informed decisions, objectively evaluating the available information and the possible consequences of their actions.

AI's ability to solve specific problems based on learned and memorised procedures – possibly adapting to new situations, to develop abstract models and to make some decisions – but can be misled by **biases** (biases, which lead to misleading perspectives), fallacies (incorrect uses of logical inferences).[8]

Logical fallacies can even be useful because they allow the expansion of knowledge and can lead – albeit in logically imperfect ways – to true conclusions by increasing information (as is typical of inductive and abductive logic and its probabilistic projections). But they contain risks. Therefore, in the various fields, in relation to the different problems, a calibrated weighting is needed – carried out by human choices – on the level of risk acceptable in the relationship between the hazards connected with fallacies, the logical exactness, the speed and the profitability of the results.

On the part of people, fallacies are more difficult to manage in conditions of uncertainty and when decisions need to be made urgently. In these conditions, individuals are guided by a limited rationality, which leads them, due to various external and internal conditionings, to decide not according to optimal logical canons, but following the path that best satisfies their needs in the context of resources, (limited) knowledge and the time in which they act.

Therefore, in conditions of uncertainty, in the presence of serious potential risks and little time to reflect, the use of algorithmic procedures – which are developed on the basis of well-thought-out models – can serve to avoid emotional conditioning and, as a precaution, in IT security contexts, to adopt urgent defensive choices that are not irrational, avoiding costs in the case of apparent threats and further risks in the case of aggressive reactions to apparent threats.

V. POSSIBLE INFERENTIAL OR EQUIVOCATION FALLACIES IN DEDUCTIVE ALGORITHMS

Obviously, expert deductive systems [III.A.], since by their nature they do not develop am-

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

plifying inferences, do not generate new knowledge beyond the initial premises, even if they have the merit of being able to extend all the derivations and, if required, to make all the passages transparent.

Therefore, they are not adaptable to non-predefined scenarios. They are rigorous, but intrinsically limited in the management of ambiguities and dynamic contexts, because they require integrations with **non-monotonic logics**, which allow exceptions to the inferential rules to be introduced. In summary, **non-monotonic logics** are fundamental to represent **defectible reasoning** or attempts at inferences that can be retracted in the light of new information, as happens in inductive reasoning, abductive explanations and the revision of beliefs. They are fundamental in all those areas where reasoning must be flexible, updatable and able to handle exceptions and changes in knowledge, manage uncertainty, incomplete or changing knowledge and reasoning that can be modified by new information.

Their validity depends on the context for which they were made; if this changes, they become obsolete and, in fields where changes are ordinary and fast, expert systems require continuous revisions, so that if an error or an unacceptable approximation emerges, they must be radically revised or set aside.

Logical fallacies pose a significant risk in complex automated reasoning because they are pitfalls.

Here are the main ones.

Computational systems based on deductive logic (syllogistic or expressed with conditional inferences) can incur specific logical fallacies, mainly related to occasional errors in the application of inferential rules or, more easily and surreptitiously, to the **equivocation** of meanings deriving from the ambiguous use of terms.

Complex inferential systems can, due to errors in their design, run into the **fallacies of the conditional**: in the **fallacy of the affirmation of the consequential**, which infers the antecedent from the consequent (if P then Q; Q is true; thus, P is true); in the **fallacy of the negation of the antecedent, which infers from the exclusion of the antecedent the negation of the consequent** (if P then Q; P is false; therefore Q is false).

Fallacies based on **the equivocation of the meanings** of terms can – using metaphors deriving from mechanics – compromise the gears of the computer path making them tilt or even completely ramshackle.

Then they can lead to unexpected errors and this makes the algorithm unreliable because it heralds wrong decisions or malfunctions.

An example of this is the ***quaternio terminorum*** **fallacy** in the syllogisms.

A valid syllogism must have only three terms connected to each other; when a fourth is introduced, the conclusion is not logically supported by the premises.

This happens because computational systems do not "understand" the content but mechanically apply the rules: misunderstandings are not recognised and feed fallacies. This can result in a propagation of errors in successive chains of inferences, which compromise the entire decision-making process and reduce the reliability of the system.[9]

VI. THE FALLACIES INHERENT IN INDUCTIVE LOGIC AND INTELLIGENT MACHINES

The operation of (non-deterministic) algorithms open to the acquisition of information, in addition to those with which they are provided as initial premises, takes place through forms of machine learning by the systems that use them.

[9] This does not prevent many terms from being intrinsically indeterminate or from having a well-defined central core and more or less indeterminate peripheral fringes. However, when (as is sometimes inevitable) premises are introduced into algorithms that convey terms that are not fully determined, it is important to be aware of this in order not to fall into the various **fallacies of misunderstanding**.

Even with a certain simplification, it can be said that intelligent machines operate by establishing correlations according to an inductive and probabilistic logic.

A. CORRELATIONS AND CONNECTIONS

The identification of correlations between specific data is a fundamental phase that precedes and supports inductive generalisation and consists of the analysis of data to identify patterns, or recurring relationships between variables or phenomena.

AIs are particularly adept at spotting similarities (and, **conversely**, differences) by grouping similar data into clusters.

They identify correlations between myriads of data, even when these are not detectable by the human analyst, mainly through **machine learning** algorithms, and try to maximise the accuracy of predictions or classifications based on probabilistic calculations.

Therefore, correlations do not always correspond to actual connections (much less to real causal relationships) and are influenced by the quality and representativeness of the data themselves.

Furthermore, the possibility of spurious correlations should not be overlooked: random associations or due to external factors that do not imply a true causal link.

These correlations represent the empirical basis on which inductive generalisation ("detail-to--general" inference) with probabilistic projections is based, which is also a form of prediction, but can reveal unexpected and harmful gaps.

So the uncertainty remains inherent in **machine learning** systems that does not allow us to exclude that the new case examined, although similar to the previous ones, does not fit the prediction.

Moreover, unlike a decision tree on which an expert system is centred, the neural network does not directly provide comprehensible explanations for its outcomes, so it is comparable to a **black box** without transparency.

Above all, these algorithms do not have the ability to adequately consider the circumstances of each concrete case, also because, in any case, they are not able to obtain all the information that would be necessary.

Therefore, they are not able to formulate the **reflective judgment**, the (typically human) one that draws from the specific circumstances of the concrete case, the criterion for solving the problem.[10]

B. FALLACIES OF INDUCTIVE LOGIC: GENERALITIES AND GENERALISATIONS

When AI establishes correlations between myriads of data, it can fall into various logical fallacies and **cognitive biases, mainly due to the nature of the data and the way it processes information.**

The logic of inductive generalisation aims to expand the knowledge for which it must coexist with the fallacies of the conditional (in particular that of the affirmation of the antecedent), which remain such in the deductive logic but which, on the other hand, are the basis of inductive logic (in which the conclusions convey information (which could turn out to be false) greater than those offered by the premises).

Therefore, the risk of the fallacious confusion between **generality** and **generalisation** inherent in the tendency to attribute the character of generality to what could turn out to be mere undue generalisations remains constant, all the more so when one proceeds along paths not supervised by the rigor of the scientific method.

[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.

The (necessary) inferences that amplify information, produce new (perhaps true, perhaps false) information are useful, provided that intellectual vigilance over their fragility is maintained.

In the use of the variegated expressions of inductive logic, macroscopic fallacies can arise.

Undue generalisation (or *secundum quid*, or onverse accident or hasty generalisation) presents what is true in some cases as if it were true for every case, or a conclusion concerning an entire class of objects starting from premises concerning only one or some of its components and consists in deriving a general rule from inadequate evidence, either because it relates to a special case, or because the sample considered is not representative. In the form of statistical generalisation, it is based on sampling but claims to have a general conclusion: statistical probability, understood as statistical frequency, cannot support an entire reasoning, even if it indicates a high probability, because it deals with frequencies and, therefore, admits exceptions, so that it does not fit the reconstruction of single events.

The fallacy of the **false cause** makes something appear as the cause of an event that is not or arbitrarily attributes a certain cause to an event without having considered the concauses or possible alternative causes. The current tools of artificial rationality that detect **regularities** among the collected data are not effective in identifying causal relationships between phenomena in relation to a specific case: so that the algorithmic result must in any case be corroborated by evidence that is processed according to the dialectical method and that requires human intervention to ensure the **overall logical coherence** of the reasoning.

In the use of abductive logic, the **atomistic evaluation of clues** is fallacious because it overlooks the fact that the clue – by its constitution – is a datum whose ambiguity must be amended by linking it to others. To shy away from this operation is to unduly set aside relevant elements of assessment that could ultimately prove to be even decisive and, therefore, fail by default. On the contrary, the *praesumptio de praesumpto* starts from a known fact (clue) to go back to an unknown one and then placing the (originally) unknown fact as the source of a further presumption makes the clue lose precision, but it could provide useful insights into knowledge, if examined with an appropriate method in the context of a non-atomistic evaluation of the data (this operation is not allowed by the jurisprudence).

VII. FALLACIES IN THE USE OF CONCLUSIONS

Some fallacies concern the use of conclusions.

In the **conjunction fallacy**, the informative value of similar data is overestimated, often violating probability theory, because joint events are mistakenly considered more likely than events described individually. In particular, in **the fallacy of the support** events supported by a description richer in specific data are considered more probable than those proposed with a more limited descriptive support, while, on the contrary, the richness of detail of the description, which makes the event more specific, should, from a statistical point of view, reduce the probability of its occurrence and make one cautious with respect to **illusory correlations**.

Some **biases** typical of algorithms or the way in which they are used also recur. Many algorithms are set up to look for all the information that can confirm the initial hypothesis, while dissonant data and hypotheses are left out until the so-called **tunnel vision is established**, which shows only what confirms the initial hypothesis (**bias** of confirmation); another distortion occurs when important data is excluded because the programmer failed to see new and important factors (exclusion bias).

Even the confusion between **mere derivation** (necessary condition) and consequence (necessary and sufficient condition) constitutes a logical fallacy that can be intertwined with the psychological propensity towards a hasty and/or

unjustified search for conclusions, introducing additional premises into the tree of reasoning. In the case of AI, either due to misunderstandings or approximations of probabilistic correlations, a **mere derivation** could be treated as a **consequence**.

The **fallacy of the false dichotomy** derives from mistaking mere antonyms for contradictory ones, so erroneously supposing that there can be only two plausible explanatory hypotheses of a fact, so that the refutation of one would necessarily lead to the truth of the other, exhausting the logical space of the question, while in reality, in the case of hypotheses that are only *contrarie tertium datur,* so that they could both be false.

The **bias** of cohesion consists of the search for cohesion even if the result of coherence is not rationally justified because it is based on incomplete data, while alternative reconstructive hypotheses should be examined.

The point is that in situations of uncertainty and ambiguity in the reconstruction of factual data, there is a propensity to formulate hypotheses to create narratives that explain the events, filling the gaps in the data. In this perspective, moreover, short causal chains are favoured over longer ones and counterfactual constructions more easily available to the mind.

Again, the propensity to anchor oneself to the first available information, to the initial framework, and then make adjustments, is valid. Despite having a partial understanding, it is assumed that we can have total cognition and tend to make the data consistent and cohesive with the initial base on the stock. Then, the data are all placed on the same level to be made coherent, neglecting their different relevance and diachronic understanding.

In some cases, an attempt is made to save the work done so that – especially when it is urgent to decide and the possible alternatives are doubtful – the efforts spent are not wasted and so we fall into **the fallacy of sunken costs**.

Since the reconstruction of a fact also results from the composition of the logical relations between certain events, when this composition is affected by fallacies or misrepresentations, the **fact** is surrogate by a **factoid**.

VIII. PROGRAMMING STRATEGIES OF AN AI TO RECOGNISE REASONING ERRORS

Because it has no critical thinking or self-awareness, current AI cannot recognise or correct logical errors or **biases** on its own, and the continuous increase in analysed data can hide deeper errors and biases that are difficult to detect and correct.

To program an AI capable of recognising reasoning errors, several strategies are adopted, among which the most profitable seem to be those that adopt an analytical approach:

a) **Supervised learning with step-by-step feedback**: the model is trained on examples of correct and incorrect reasoning, providing feedback on each individual step. This helps the AI identify where logical errors lurk and correct them during the inference process. When using a supervised model, it is the experts in the field who select the training data: it is crucial that their group is diverse and that they have received adequate training to help prevent unconscious bias.

b) **Step-by-step reasoning**: the AI is trained to reason step by step, making each stage of reasoning explicit. Instead of just providing the final answer, AI breaks down the problem into a logical sequence of intermediate steps, making the decision itinerary transparent, so that programmers and users can verify the internal consistency of the reasoning, making it easier to detect inconsistencies or invalid passages. Or, for the same problem, AI can be induced to generate multiple chains of reasoning, so as to reduce, by comparing them, the influence of random errors or erroneous inferences.

At present, **hybrid systems**, those that use both human judgment and artificial intelligence, tend to minimise the possibility of bias and therefore guarantee the best results. While it is true that algorithms can bring greater rigor and repeatability to a process and are able to look for and remove biases due to human error, it is also true that humans are able to evaluate situations in a broader context, adding critical capacity, research skills and understanding of the decision-making process**.** Then systems in which AI offers options or recommendations for human evaluation are optimal.

Finally, the **strategy of cultivating the opposite hypothesis** (also practicable with AI tools) can reduce the negative effects of **biases**, anchors, tunnel effects, especially **confirmation bias**[11], sometimes induced by the formulation of the **prompt**.

Alerts can be introduced in the algorithms to solicit the consideration of a contrary hypothesis (perhaps generated by the algorithm itself, based on the logical heuristic).

However, both expert systems and systems based on data correlations do not appear to have, at present, a significant dialectical ability to examine alternative assumptions and hypotheses with respect to those with which they work.[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.

A BIG QUESTION FOR MICRO AND SMALL ENTERPRISES: THE CRITERIA FOR THE APPLICATION OF THE NIS 2 DIRECTIVE AND DECREE-LAW NO 125/2025 OF 4 DECEMBER

ANA XAVIER NUNES
Morais Leitão's Associate

Directive (EU) 2022/2555 of the European Parliament and of the Council, of 14 December 2022 ("NIS 2")[1] and Decree-Law No 125/2025, of 4 December[2] ("Decree-Law No 125/2025") (together, the "instruments"), start from an apparently simple criteria: as a rule, provided that the territorial scope is met, medium-sized enterprises and enterprises exceeding the thresholds for medium-sized enterprises (or "large enterprises") that operate in the sectors identified by the instruments and provide their services or carry out their activities in the European Union are covered.[3]

The relevant quantitative criteria results from the express reference to the European definition of micro, small and medium-sized enterprises (SMEs) set out in Commission Recommendation 2003/361/EC, of 6 May 2003. Under Article 2(1), the category of SMEs is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million or an annual balance sheet not exceeding EUR 43 million.[4]

However, the provision on the subjective scope of application is extensive, and only a hasty reading could lead to the conclusion that micro and small enterprises would fall outside its reach. Thus, the instruments call for an in-depth analysis, incompatible with an uncritical application.[5]

The relevance of the quantitative criteria is mitigated by a set of exceptions enshrined in NIS 2 and implemented by Decree-Law No 125/2025, which provides that certain entities may be covered « [...] regardless of their nature and size and provided that the territorial scope criteria are met [...] ». Accordingly, the instruments allow certain entities to be classified as essential or important on the basis of their material relevance, even if they do not reach the typical thresholds for medium-sized or large enterprises.

In general terms, this prevalence of the material criteria occurs where an activity is intrinsically

1 Concerning measures designed to ensure a high common level of cybersecurity within the Union.

2 This Decree-Law incorporated NIS 2 into national law.

3 We refer exclusively to business entities. We will not address the application of Decree-Law No. 125/2025 to the Public Administration, to public entities integrated in the institutional structure of the State, or to higher education institutions, whose subjection to the regime is direct and independent of the size criterion (cf. Article 3, paragraphs 3, 4 and 6, of that statute).

4 Under Recommendation 2003/361/EC of 6 May, a micro-enterprise is defined as one which employs fewer than 10 people and whose annual turnover or annual balance sheet total does not exceed EUR 2 million; a small enterprise is one which employs fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million; a medium-sized enterprise is one which employs fewer than 250 persons and whose annual turnover does not exceed EUR 50 million or whose annual balance sheet total does not exceed EUR 43 million. Large enterprises are those that exceed the thresholds applicable to medium-sized enterprises.

5 With a formulation that is not entirely coincident (and, in certain segments, less straightforward in one statute or the other), the subjective scope of application is laid down, respectively, in Article 2 of NIS 2 and in Article 3 of Decree-Law No. 125/2025.

critical and structural to the functioning of the economy and society, at national or regional level. Consider, first and foremost, electronic communications operators, providers of digital **trust services or entities involved in Domain Name System** management (areas whose vulnerability entails an immediate and cross-cutting impact).

On the other hand, size also ceases to be relevant where the entity plays an irreplaceable or highly significant role in a given sector, whether because it is the sole provider of an essential service; because of the impact that disruption of the service may have on public safety, security or health: because of the possibility of generating considerable systemic risks; or because of its specific importance, at national or regional level, for the sector, type of service or to interdependent sectors. The law also covers situations in which the entity has already been previously identified as critical.[6]

The subjective delimitation of the instruments therefore requires not only the verification of quantitative thresholds, where the criteria of enterprise size constitutes the rule as a first approximation, but also a substantive assessment of the potential impact of the activity carried out, which entails a case-by-case evaluation that operates as a mechanism of exceptional inclusion, but no less significant for that.

Exclusion from the subjective scope does not, however, mean immunity from the framework. The instruments mandate covered entities with risk management duties in respect of their supply chain.[7] This means, for example, that a medium-sized or large enterprise subject to the regime will have to ensure that its providers and suppliers adopt adequate levels of security, and may, for that purpose, impose on them enhanced contractual requirements in matters of cybersecurity and cyber-resilience.

Accordingly, an entity (not covered) that provides services to an entity subject to the regime should adopt and be able to demonstrate the existence of adequate security policies, incident response plans, access control mechanisms, audit procedures, among others. Ignoring this reality may give rise to various types of risks, which are not limited to contributing to the propagation of incidents with an impact on third parties, but may also result in the non-award of contracts, on the grounds of non-compliance in this area.

Thus, even though micro and small enterprises are not, by virtue of their size, formally covered by cybersecurity obligations, it should be considered that, operating in critical ecosystems, the regulatory impact will reach them, at a minimum, through contractual means.

But there is yet an additional factor. An entity which, considered in isolation, meets the requirements to be classified as a micro or small enterprise, may lose that status, for the purposes of application of the regime, if it is part of a corporate group which, in aggregate terms, exceeds the aforementioned thresholds.[8] The assessment of size for the purposes of application of the regime will not, in principle, be exclusively individual, requiring a consolidated analysis of the corporate structure and existing control or participation relationships, regardless of the

6 In light of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

7 This is the case, namely, of the provision of Article 21(2)(d) of NIS 2, as well as Article 28 of Decree-Law No 125/2025. With regard to supply chain management, particular relevance is assumed, among others, by Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024, which lays down rules for the implementation of NIS 2 concerning the technical and methodological requirements of cybersecurity risk management measures, as well as the Technical Implementation Guidance, version 1.0, of June 2025, and the Good Practices for Supply Chain Cybersecurity, of June 2023, both prepared by the European Union Agency for Cybersecurity (ENISA).

8 The Legal Framework for Cyberspace Security still in force (Law No 46/2018, of 13 August, which transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016) makes its application dependent on qualifications based on essentially material criteria, neither providing for nor referring to any quantitative parameters. Nevertheless, in order to begin charting a path, alongside the Recitals of NIS 2, the guidelines adopted by national cybersecurity authorities of other Member States have proven particularly relevant, as is the case with the Centre for Cybersecurity Belgium, whose Frequently Asked Questions (FAQs) on NIS 2 and its transposition into the Belgian legal order are already in version 2.1.3 (03/2026). Although less detailed, the FAQ published by the Agenzia per la Cybersicurezza Nazionale in Italy, as well as the FAQ issued by the Instituto Nacional de Ciberseguridad (INCIBE-CERT) in Spain, are also relevant.

geographical origin of the different companies in the group.[9]

This element must, however, be read with caution. The consolidated analysis of the group's size should not be applied automatically, because that could lead to materially disproportionate results. This is precisely the concern reflected in Recital 16 of NIS 2, which acknowledges that Member States may take into account the degree of independence of the entity in relation to its partner or linked enterprises, particularly as regards the information networks and systems used and the services actually provided.

This means that an entity forming part of a group should not, in each and every case, be automatically equated with the aggregate size of that group. Consequently, where it demonstrates sufficiently relevant functional autonomy and, considered in isolation, does not exceed the applicable thresholds, it may be justified to depart from a merely flat application of the said criteria.

These elements – which, moreover, do not exhaust the possible scenarios – lead to the conclusion that the apparent exclusion of micro and small enterprises is, strictly speaking, merely a problem of perception that must be carefully studied, by anticipating situations of non-compliance, with the consequent risk of exposure and liability of the entities involved.

[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*"). The European Commission has also made available, for these purposes, an electronic tool designed to assist in determining the size of the enterprise, accessible here.

NEWS

Cybercrime and digital evidence

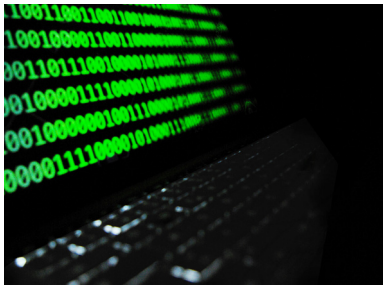
GLOBAL SCALE OF THE THREAT

The global cybercrime landscape in 2026 is marked by increasingly sophisticated threats and their unprecedented scale. **The IOCTA 2026** report (Internet Organised Crime Threat Assessment), published by Europol, documents the evolving threat landscape of organised online crime, identifying as structural trends the professionalisation of criminal organisations, the growing interdependence between cybercrime and other forms of organised crime, and the systematic exploitation of legitimate infrastructure for illicit purposes (Europol, IOCTA 2026). The FBI's figures confirm the severity of the phenomenon: according to the annual report of the Internet Crime Complaint Center (IC3), **financial losses from cybercrimes reached an all-time high of USD 20** billion, with phishing and spoofing dominating the complaints received, although actual figures are estimated to be significantly higher (FBI Internet Crime Report).

INTERNATIONAL LAW ENFORCEMENT OPERATIONS

In terms of law enforcement operations, recent months have been marked by large-scale initiatives across multiple jurisdictions. Interpol **identified and neutralised approximately 45,000 malicious IP** addresses associated with ransomware and phishing worldwide (Interpol). With a focus on the African continent, the same organisation arrested **651 individuals in 16** countries for cybercrime offences, illustrating the growing spread of organised cybercrime in regions historically underrepresented in these statistics (Interpol). Europol in turn reported an operation in which two seized mobile phones enabled, through forensic analysis, the uncovering of connections to a large-scale global criminal network – underscoring the central role of mobile device forensic extraction in combating organised crime (Europol). **Brazil led the largest international operation against online child sexual** abuse on record, involving **16** countries and resulting in numerous arrests and the identification of victims – a paradigmatic example of the importance of international police cooperation and digital investigation capabilities in this field (Observador). **Eurojust** also coordinated a successful operation against illegal streaming services, with an impact on millions of users worldwide (Eurojust).

ENCRYPTED NETWORKS: SKY ECC, ENCROCHAT AND ANOM



The debate on the admissibility of digital evidence obtained through encrypted communications networks remains in full swing in European courts, with divergent decisions across multiple jurisdictions. **With regard to the Sky ECC** network, the Antwerp Court will, in the near future, have to rule on the admissibility of evidence obtained from intercepts, having already been confronted with the testimony of a forensic expert who raised doubts as to the transparency and reliability of the interception mechanisms (Computer Weekly); in Switzerland, the Basel Court adopted a similar position, refusing to admit evidence whose collection did not comply with the procedural safeguards required by Swiss law; in Spain, a court acquitted

defendants who had been prevented from accessing the raw intercepts, placing the right to defence evidence at the centre of the discussion (Computer Weekly); and in Italy, challenges to Sky ECC and EncroChat evidence have likewise been filed, with the defence contesting the chain of custody and the authenticity of the intercepts.

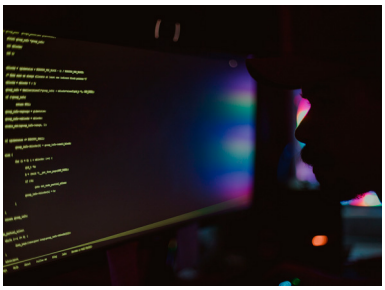
INTEGRITY OF CRIMINAL INVESTIGATION AND POLICE EVIDENCE

The period under review also brought disturbing developments regarding the reliability of police evidence. In Spain, **the former head of the UDEF** (Economic and Tax Crimes Unit of the National Police) **gave testimony before a judge describing what he classified as an institutionalised "system"** of falsifying the origin of major anti-drug operations, through the manipulation of detection circumstances and the attribution of investigative credit. The case raises fundamental questions about the integrity of the chain of custody of evidence and the veracity of police reports, with potential implications for several drug trafficking cases in which UDEF evidence plays a central role (El Diario). In a different vein, Wired **revealed that an FBI informant ran a dark web** site selling fentanyl-laced drugs for years, raising questions about the limits of undercover operations in the digital environment and the responsibility of authorities for offences committed in the course of managing infiltrated platforms (Wired). The same magazine detailed the escape of a collaborator who revealed the secrets of the scam compounds of Southeast Asia and was forced to leave the country to save his life, shedding light on the reality behind the cybercrime networks based on forced labour that fuel pig butchering scams (Wired).

ENCRYPTION, DEVICE ACCESS AND DIGITAL EVIDENCE

The issue of access to encrypted devices gave rise to two American cases that illustrate, in opposite directions, the structural tension between lawful access to data and robust encryption. Forbes **revealed that Microsoft provided the FBI** with BitLocker decryption keys to access data on a confiscated device, setting a relevant precedent on the cooperation of major technology companies with authorities in obtaining digital evidence (Forbes). Conversely, in another case, the FBI **admitted that it was unable to access the iPhone of a Washington Post** journalist because the device had Lockdown mode enabled – an enhanced Apple security feature that proved effective against the authorities' forensic tools (404 Media).

SECURITY INCIDENTS AND PERSISTENT THREATS



Researchers detected indications of the use by the Lazarus group (linked to North Korea) of the **Medusa** ransomware, namely in attacks on the healthcare sector in the United States of America (Security.com). In terms of the most impactful security incidents, **Coinbase** confirmed an internal breach linked to screenshots of support tools extracted by an employee (Bleeping Computer). The European Commission opened an investigation into a cyberattack targeting its internal systems (IT Security PT). The French government confirmed the exposure of data from **1.2** million bank accounts following a data breach (SecurityWeek).

COMMUNICATION PLATFORMS AND LIABILITY

With regard to major communication platforms, the founder of **Telegram**, Pavel Durov, was confronted with legal proceedings brought in Russia for alleged contribution to terrorism – a development that underscores the growing pressure from states on encrypted communication platforms and raises questions about platform liability for third-party content (NowCanal). At the European level, **WhatsApp** saw its transparency and accountability obligations strengthened by the European Commission under the Digital Services Act (Tek.pt).

ARTIFICIAL INTELLIGENCE IN THE JUDICIAL CONTEXT

Two significant developments mark the period with regard to the use of artificial intelligence in the judicial context. In Brazil, the Regional Labour Court of the 8th Region issued a pioneering decision on an attempt to manipulate the generative AI system used by the court through prompt injection – a technique consisting of the insertion of hidden instructions in a procedural document, in white text on a white background, intended to induce the system to produce a superficial defence to the detriment of the opposing party. The Court classified the conduct as an act against the dignity of Justice and imposed on the subscribing lawyers a joint and several fine of 10% of the amount in dispute (see case law section). In parallel, the Superior Court of Justice analysed for the first time (AgRg in HC No 1,059,475/SP) the validity of a police report prepared with the aid of generative AI, in contradiction with official expert reports, raising the question of whether AI can replace expert activity with direct implications for the rights of the defence (STJ Brasil).

PORTUGAL AND THE NATIONAL LANDSCAPE

In Portugal, **the National Security Office launched the myCiber.gov.pt** portal, which allows companies to simulate their potential inclusion within the scope of the NIS2 transposition law (myCiber.gov.pt). In terms of training, ECTEG **launched eFirst version 2.1**, with new serious games and a revamped module on lawful decryption for first responders (ECTEG). On a less positive note, illegal online gambling continues to generate more than two thousand complaints, evidencing the persistence of a robust illegal market (Jornal Económico).

Crypto-assets

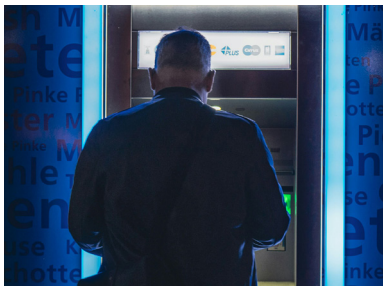
GENERAL OVERVIEW OF CRYPTO CRIME

The TRM Labs annual cryptocurrency crime report for 2026 paints a concerning picture of crypto crime trends, highlighting the growth of investment scams, attacks on DeFi protocols and the use of stablecoins in money laundering. The erosion of the boundary between the licit and illicit crypto ecosystem, as well as the ability of state actors to use cryptocurrencies to finance illicit activities, emerge as central concerns (TRM Labs).

BYBIT AND LAZARUS: THE LARGEST CRYPTO MONEY LAUNDERING IN HISTORY

The most high-profile case of the period is the Bybit hack, **attributed to the North Korean Lazarus** group, **valued at approximately USD 1.5** billion. Researchers at Arkham Intelligence confirmed that Lazarus completed the laundering of the entirety of the stolen funds, **converting approximately ETH 500,000** into BTC **through THORChain** as a chain hopping mechanism – a decentralised network that, since the attack of 21 February 2025, has processed more than USD 5.5 billion in volume. Once in Bitcoin, the funds were sold through opaque OTC desks, frequently located in China and Southeast Asia, at a discount of 15 to 20% below market value.

CRYPTO ATMS AND MARKET TURBULENCE



Bitcoin Depot, **the largest operator of cryptocurrency ATMs in the US, declared insolvency and proceeded to shut down more than 9,000** machines across the country. CEO Alex Holmes pointed to increasingly restrictive regulatory requirements and the fragmentation of the regulatory framework across different states as the main causes. The abrupt shutdown raises doubts as to the situation of users with pending transactions. The case is also

relevant from an AML perspective, insofar as cryptocurrency ATMs have been repeatedly identified as high-risk vectors in FATF assessments (Jornal de Negócios).

LAW ENFORCEMENT OPERATIONS AND SEIZURES

In terms of law enforcement operations, the FBI **developed an innovative operation by creating its own crypto service called NextFundAI,** which allowed agents to communicate with market-makers **and observe how they operate. This operation enabled the identification of participants in a market manipulation scheme and the seizure of USD 25 million (TRM Labs).** Additionally, **the US Attorney's Office for the Eastern District of North Carolina announced the seizure of USD 61 million in tether, related to scams and thefts through pig butchering schemes (DOJ EDNC). In Florida,** the State sought the forfeiture of real estate and vehicles acquired with the proceeds of fraud and money laundering crimes that led to the arrest of the CEO of Goliath Ventures (DOJ MDFL).

NOTABLE CONVICTIONS

A French national was sentenced to **eight** years in prison for laundering hundreds of millions of dollars in cryptocurrency (DOJ SDNY). In the United States, the owner of **Incognito Market** – one of the largest dark web drug markets globally – was sentenced to **30** years in prison, one of the most severe sentences ever imposed in organised crime cases in the digital environment (DOJ SDNY). A Chinese national was convicted for his role in a crypto scam scheme targeting American citizens (DOJ). Former Olympic snowboard **champion Ryan Wedding** was arrested in connection with a transnational case combining drug trafficking, violence and money laundering in cryptocurrency (TRM Labs). **In the case of United States v. Roman Sterlingov** (Bitcoin Fog), the defence challenges on appeal the blockchain analysis methodologies used to prove ownership of the service – making the case a benchmark on the evidentiary standards applicable to forensic crypto analysis in criminal proceedings (Court Listener).

COMPLIANCE, REGULATION AND MARKET DEVELOPMENTS

Fortune **revealed that Binance** dismissed investigators who had internally flagged potential sanctions violations relating to Iran, raising questions about the compliance mechanisms of the world's largest exchange (Fortune). In Brazil, a civil court ordered the freezing of USDC issued by Circle, raising questions about the enforceability of court orders over digital assets issued by foreign entities (LiveCoins). In Africa, Angolan authorities dismantled a cryptocurrency mining centre in Luanda (Jornal de Negócios) and ten citizens were arrested in Ramiros for unauthorised mining (PTI Angola). Finally, the New York Times **published an investigation identifying Adam Back** as the most credible candidate for the identity of Satoshi Nakamoto (New York Times).

LEGISLATION AND SOFT LAW

Portugal

LEGISLATION

LAW NO 12-A/2026, OF 15 APRIL (DSA Implementation)

Law No 12-A/2026 was published, implementing in Portugal **the Digital Services Act (DSA – Regulation (EU) 2022/2065)**, establishing the competent national authorities, supervisory mechanisms, applicable procedural channels and the national sanctions regime. The law designates the competent sectoral authorities for supervising compliance with the obligations arising from the DSA across the different types of platforms and intermediaries, within a supervisory framework coordinated with the European Commission. The adoption of this instrument concludes the national implementation process of one of the most important European regulatory instruments in the field of digital platform liability for third-party content (Diário da República).

LAW NO 73/2025, OF 23 DECEMBER (DORA Implementation)

Published on 23 December 2025, Law No 73/2025 implements the European legal acts on the digital operational resilience of the financial sector, transposing and giving effect to the DORA Regulation. **It confirms the sectoral competence of the Banco de Portugal**, the **ASF** and the **CMVM**, **in coordination with the National Cybersecurity Centre (CNCS)**. In terms of sanctions, **it provides for fines of up to EUR 5,000,000 or 10%** of turnover for non-compliance with governance duties, ICT risk management, incident response, third-party management and resilience testing. This instrument introduces comprehensive sectoral amendments to the General Regime of Credit Institutions and Financial Companies (*RGICSF*), Securities Code (*CVM*), to the insurance and reinsurance sector, payment services and electronic money, pension funds and investment firms (Diário da República).

DECREE-LAW NO 25/2026, OF 28 JANUARY (Terrorist Content Online)

Published on 28 January 2026, **Decree-Law no. 25/2026 transposes into domestic law** Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. It designates the Judiciary Police (UNCT-PJ) as the competent authority to issue removal or blocking orders, **subject to validation by the DCIAP/**Public Prosecutor's Office within 48 hours and judicial review by the Investigating Judge (Diário da República).

CSMP WORKING GROUP – PROPOSAL FOR THE REVISION OF THE CODE OF CRIMINAL PROCEDURE (DIGITAL EVIDENCE)

The Superior Council of the Public Prosecution Service established, in February 2025, a working group composed of seven magistrates – coordinated by retired Deputy Attorney General José Góis and with Rui Cardoso (Director of the DCIAP) as spokesperson –, with the mandate to analyse and propose amendments to criminal procedural legislation. The proposals were presented at the Attorney General's Office (*PGR*) on 28 April 2026 and encompass amendments to 130 articles of the Code of Criminal Procedure.

In the specific field of digital evidence (corresponding, in substance, to the proposals set out at pp. 63 *et seq*. of the document), the most relevant amendments are the following:

a) Competence for the selection of email – transfer from the Investigating Judge to the Public Prosecutor's Office: the proposal provides that the selection of relevant email content and communications records shall be carried out by the Public Prosecutor's Office, on terms analogous to those already in force for telephone intercepts under Articles 187 *et seq*. of the Code of Criminal Procedure – thereby removing from the Investigating Judge the competence currently attributed to him by Article 17 of the Cybercrime Law read in conjunction with Article 179(3) of the Code of Criminal Procedure. The group's spokesperson justified the proposal on the basis of the delays – sometimes of years – that the current regime has caused in obtaining digital evidence: «The procedure that must be followed today because of the interpretation given to the law has led to delays, sometimes of years, before we can obtain digital evidence.». The group stressed that the amendment does not

jeopardise the right of defence, as the accused will retain access to the seized data.

b) Express extension of the wiretapping regime to the use of GPS tracking devices: the proposal provides that the judicial authorisation regime applicable to telephone intercepts shall be expressly extended to the use of GPS tracking devices, clarifying the legal framework applicable to this means of obtaining evidence and standardising the requirements for prior authorisation.

c) Revision of the Cybercrime Law – search and seizure of computer data: the group proposes the revision of the Cybercrime Law with regard to the regime governing the search and seizure of computer data, in line with the proposals referred to above and with the aim of simplifying and streamlining access to digital evidence in criminal investigations. The group acknowledged, however, that the issue of metadata – which the Lisbon Court of Appeal judgment of 19 March 2026 brought back into the spotlight – was not the subject of a specific amendment proposal in this package.

Foreign and international

LEGISLATION AND BINDING INSTRUMENTS

BUDAPEST CONVENTION ON CYBERCRIME – PAPUA NEW GUINEA BECOMES THE 82ND PARTY.

Papua New Guinea ratified the Budapest Convention (ETS No 185), becoming the 82nd party to this instrument and extending its geographical reach to the Pacific. The Convention thus consolidates its position as the principal multilateral legal framework for combating cybercrime (Council of Europe | Text of the Convention).

MOZAMBIQUE – CYBERCRIME LAW.

The Assembly of the Republic of Mozambique adopted specific legislation on cybercrime, harmonising the national legal framework with the principles of the Budapest Convention and placing Mozambique among the growing number of African countries with dedicated legislation in this area (Parliament of Mozambique).

CHINA – STRENGTHENING OF CYBERCRIME PENALTIES.

China announced legislative amendments strengthening penalties for cybercrime, adding the possibility of imposing exit bans following the completion of prison sentences, with the stated aim of curbing recidivism and transnational organised crime (South China Morning Post).

UNITED KINGDOM – VPN BAN FOR MINORS.

The House of Lords approved a proposal to ban the use of VPNs by children, as part of a broader legislative initiative for the protection of minors in the digital environment (ISPreview).

SOFT LAW AND OTHER INSTRUMENTS

COE C-PROC – GLOBAL STATE OF CYBERCRIME LEGISLATION (2013–2025).

The Cybercrime Convention Committee published a comprehensive analysis of the evolution of national regulatory frameworks and persistent gaps at the global level – an essential reference for comparing systems and identifying jurisdictions in need of harmonisation (Council of Europe).

EUROPEAN UNION – STRENGTHENING CYBERSECURITY.

The European Commission adopted a package of measures to strengthen the EU's resilience and cybersecurity capabilities within the framework of the implementation of the Cybersecurity Strategy and NIS2, including information-sharing initiatives, technical capacity-building and coordination among Member States (European Commission).

ENISA – NIS360 2024.

The European Union Agency for Cybersecurity (ENISA) **published the NIS360 2024** report, which assesses the maturity and readiness of the sectors covered by the NIS2 Directive across the different Member States, identifying implementation gaps and best practices. The report constitutes a reference tool for competent authorities, essential service operators and digital service providers in calibrating their NIS2 compliance programmes (ENISA).

EUROPEAN UNION – TRANSPARENCY GUIDELINES UNDER THE AI ACT (ARTICLE 50).

The European Commission submitted for consultation a draft set of guidelines on the transparency obligations applicable to certain AI systems under Article 50 of the AI Act – namely chatbots, synthetic content generation systems and AI-generated content labelling. The guidelines are directly relevant to the use of AI in judicial and criminal investigation contexts (European Commission).

FATF – REPORT ON STABLECOINS AND UNHOSTED WALLETS.

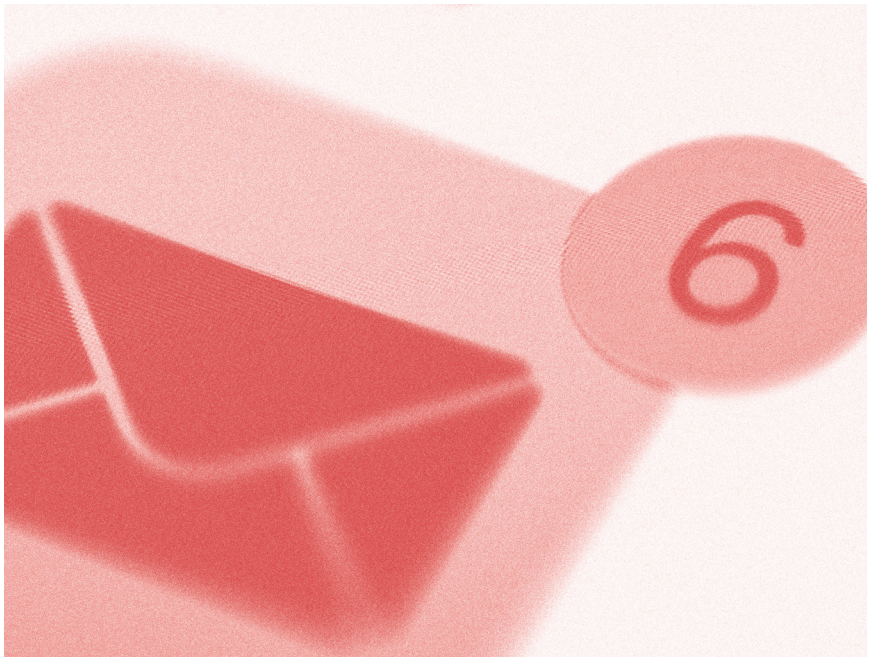
The FATF published a specific report on stablecoins and unhosted wallets, reinforcing AML/CFT compliance expectations for virtual asset service providers and addressing the specific risks of these categories for money laundering (FATF).

CASE LAW

Portuguese case law

LISBON COURT OF APPEAL, CASE NO 2221/19.3JFLSB-C.L1-5, JUDGMENT OF 23 JANUARY 2026.

Email – Competence for selection – Article 17 of the Cybercrime Law – Article 179(3) of the Code of Criminal Procedure.



The ruling held that it is the Investigating Judge who, in compliance with Article 179(3) of the Code of Criminal Procedure (applicable by virtue of Article 17 of Law 109/2009), is responsible for selecting and ordering the inclusion in the case file of the relevant email content and communications records. It further held that the accusatorial structure of the proceedings (Article 32(5) of the Constitution) is not violated by a decision refusing to hand over to the Public Prosecutor's Office, after the Investigating Judge has taken cognisance of the material and expunged prohibited content, the seized data for that office to conduct its own search and selection of relevant items. (DGSI)

LISBON COURT OF APPEAL, CASE NO 23/26.0GCALM-A.L1-9, JUDGMENT OF 19 MARCH 2026.

Traffic and location data – Metadata – Digital evidence collection regimes – Law No. 32/2008.

The ruling held that traffic and location data constitute metadata protected by telecommunications secrecy and the right to privacy, as they allow the inference of behaviour despite not relating to the content of communications.

Further clarified that the collection of digital evidence is organised into three distinct regimes: (*i*) real-time interception (Articles 187 to 190 of the Code of Criminal Procedure); (*ii*) search and seizure of computer data (Law No 109/2009); and (*iii*) access to stored traffic data (Law No 32/2008).

Clarified that, following Constitutional Court Judgments Nos. 268/2022 and 800/2023, **there is a requirement for a model of selective retention of traffic and location data for criminal investigation purposes, subject to prior judicial authorisation. Access to stored traffic data, even where retained by operators for other purposes** (*e.g.* commercial or billing), must comply with the specific regime laid down in Law No. 32/2008 and cannot be obtained on the basis of Articles 187 and 189 of the Code of Criminal Procedure, the Cybercrime Law or Law No. 41/2004.

Dismissed the appeal brought by the Public Prosecutor's Office, upholding the refusal of access to stored traffic data for lack of prior authorisation in the terms required by law. (DGSI)

Foreign case law

ISRAEL

SUPREME COURT, CASE ח"תע 65435-03-26, STATE OF ISRAEL V. ARTYOM NADORNENKO, JUSTICE ALEX STEIN, 19 MAY 2026.

Voluntary cooperation with stablecoin issuer – Freezing of crypto-assets – Extraterritoriality – Section 3 of the Police Ordinance.

The decision held that, by contacting Tether and obtaining the freezing of the wallet, the Israel Police did not exercise any legal power or perform any coercive act over the applicant or over Tether itself, but merely exercised its liberty of action (privilege), *i.e.* the faculty of seeking the cooperation of a private third party, without creating legal subjection or restricting the applicant's rights, who never had any right to prevent the police from taking such steps. It further held that Tether is a foreign company that does not operate in Israel, is not subject to Israeli law and is not subject to Israeli authority, and therefore the police had no means of regulatory pressure over the company; on the contrary, it was Tether itself that required an Israeli court order as a condition for proceeding with the freezing of the wallet, and the Israel Police merely satisfied that requirement. In these circumstances, the court concluded that there was no coercive state act requiring express statutory authorisation, the general authorisation conferred on the Police by Section 3 of the Police Ordinance being sufficient. The judgment further underscores that the detection and seizure of digital wallets faces considerable difficulties, given that crypto-assets such as Bitcoin are virtual assets without a defined geographical location, and states that, where wallets are associated with financial companies, voluntary cooperation with such companies, following the model adopted with Tether, can significantly assist the police, particularly since at least some of these companies have an interest in preserving their reputation and are therefore willing to cooperate.

BRAZIL

REGIONAL LABOUR COURT OF THE 8TH REGION, CASE ATORD 0001062-55.2025.5.08.0130, 3RD LABOUR COURT OF PARAUAPEBAS.

Prompt injection – Manipulation of judicial AI system – Act against the dignity of Justice – Articles 5 and 77, §2, of the Civil Procedure Code (CPC).

The Court held that the procedural party used a technique for manipulating artificial intelligence systems, known as prompt injection, by inserting in the petition text in white font on a white background – invisible to the human reader – containing a hidden command directed at the judicial AI, instructing it to contest the petition superficially and not to challenge the documents, regardless of any command given to it. The court classified this technique as the deliberate insertion of hidden instructions in documents for the purpose of manipulating AI systems that may process the text, inducing them to produce results favourable to the person who inserted the command. It further held that the attempt to manipulate the administration of justice is consummated at the moment the command is inserted into the document filed with the court, irrespective of whether it produces the intended result, since it constitutes a procedural offence of a formal nature, which is complete upon the conduct itself and does not require proof of concrete prejudice in order to justify the imposition of a sanction. On this basis, the Court found that an act against the dignity of Justice had been committed, in light of Articles 5 and 77, §2, of the Civil Procedure Code, and imposed a fine of 10% of the amount in dispute (BRL 842,500.87), jointly and severally, to be paid to the Federal Government, further ordering the communication of the facts to the Bar Association.

USA

FEDERAL COURT FOR THE DISTRICT OF COLUMBIA, CIVIL ACTION NO. 25-CV-1907.

***In rem* forfeiture complaint – 225 million USDT – Pig butchering – 18 U.S.C. §§ 981(a)(1)(A), 1956.**

The ruling describes that the cryptocurrency confidence scams known as "pig butchering" constitute a type of internet-based cryptocurrency investment fraud in which the victim is "fattened before the slaughter": first there is a cold contact by text, social media or another communication platform; then a relationship is built with the victim over days, weeks or months; the victim is then induced to send purported investments through fraudulent platforms; finally, the perpetrators cut all contact when the victim stops making payments. The Court noted that the analysis of the transactional activity associated with 144 accounts on the OKX platform revealed more than 263,000 deposit transactions, totalling approximately three billion dollars, with 98% of those transactions occurring between November 2022 and November 2023. In that one-year period, the 144 accounts carried out approximately 257,740 transactions involving virtual currency worth about 2.94 billion dollars, corresponding to an average of more than 700 transactions per day, moving over 8 million dollars per day. The Court further concluded that almost all of the 144 accounts were accessed from IP addresses in the Philippines, all associated with iCloud email addresses following a specific naming convention, and opened with Vietnamese identification documents and KYC photographs that appear to have been taken in the same location, which is a strong indicator that these accounts are controlled by individuals operating from a "scam compound". (Justice)

4TH CIRCUIT, UNITED STATES V. LOWERS, NO. 24-4546, 10 MARCH 2026

Google Drive – Reasonable expectation of privacy in cloud files – Hash-matching – Attenuation of unlawfully obtained evidence – 4th Amendment.

The ruling recognised that there is a reasonable expectation of privacy with regard to files stored in cloud accounts, namely on Google Drive, concluding that the police cannot open or view such files without a judicial warrant, unless a constitutional exception to the warrant requirement applies. Despite recognising that there was a violation of the 4th Amendment, as files were opened and viewed without a warrant, the Court upheld the refusal to suppress the evidence, finding that the evidence was sufficiently attenuated by virtue of the time intervals and voluntary acts that had occurred in the meantime – namely interviews and the defendant's consent –, which rendered the application of the exclusionary rule unjustified. (Justia)

5TH CIRCUIT, UNITED STATES V. BURGER, NO. 25-51021, 19 MARCH 2026.

Threats on online gaming platform (Roblox) – «true threats» – 1st Amendment – Factual question for the jury.

The Court reversed the decision that had dismissed the indictment at the pre-trial stage, holding that the classification of statements as "true threats" – and therefore outside the protection of the 1st Amendment – is typically a factual question to be submitted to the jury and not susceptible of early determination by the court. (Justia)

2ND CIRCUIT, UNITED STATES V. PENCE, NO. 24-1025, 10 APRIL 2026.

Dark web – Bitcoin payment – Pre-Miranda confession – Custody – 5th Amendment.

The defendant was investigated for allegedly having contracted, through the dark web, the murder of a couple, paying in Bitcoin. Following an FBI operation, he was questioned, without handcuffs, in a police vehicle and confessed before being informed of his rights as a suspect (Miranda Rights).

He subsequently sought to exclude that confession in Court, alleging that he was unlawfully detained at the time of the questioning.

The Court concluded that the defendant was not formally in custody, and therefore Miranda Rights did not yet apply. Thus, the conviction was upheld on appeal. (Justia)

7TH CIRCUIT, UNITED STATES V. BLOCKER, NO. 25-1536, 5 MAY 2026.

Dropbox – Terms of service as consent – Automated scanning – Report to NCMEC – 4th Amendment.

The case involved the detection of child pornography by Dropbox through monitoring permitted by the platform's terms of service, reporting to NCMEC and a subsequent FBI search warrant, with the discovery of further images. The Court upheld the validity of the interception: acceptance of the terms of service was considered effective consent for Dropbox to examine files and disclose them for purposes such as reporting to the authorities, and the motion to suppress was denied. (Justia)

INTERVIEW WITH NICK FURNEAUX: "CRYPTOCURRENCIES FUNDAMENTALLY ARE NOT THAT HARD"

Author of *Investigating Cryptocurrencies* and *There's no such thing as crypto crime*

By **David Silva Ramalho**

Nick Furneaux

Nick, once again, thank you for accepting to do this interview. Without further ado, I would go right into it: how did you get into crypto tracing?

By mistake. If I had known, I probably would never have done it – there's got to be an easier way of earning a living, you know. That's maybe a little glib, but I come from a background where we used to create a lot of covert data extraction tools, used by all of the types of agencies that would want to extract data from target computers quietly. And so we used to teach a lot of methodologies around that – memory analysis, for example, which could be done at high speed on the ground. Imaging the memory from a target machine is much quicker than imaging a hard drive, for example, in an internet cafe in some difficult country. And we were teaching a lot of these things. Then we started to bump into these long strings of letters and numbers on suspects' machines. They were early Bitcoin addresses. So I'd started reading around it, just trying to understand the technology and what it was all about, and I'll be completely honest: I just thought it was great for criminals.

And I could have bought Bitcoin when it was like a couple of hundred bucks, but I didn't, because I thought this

was definitely a criminal network and nothing good was ever going to come of it. So I think even now I own like six grand worth of Bitcoin. I mean, it's literally next to nothing in the great scheme of things.

I feel the same. I started researching this in 2012, 2013 and I should have bought it then.

Yeah, hindsight... but I don't take investment advice from an investigator; that's the lesson there. I was interested in it as a technology. I thought it was interesting and that it might be a good trigger: if we found this, we might be looking at a criminal. We're talking very early on here, not in the modern days where Wall Street is buying Bitcoin. It was a couple of years after that before we were first offered a Bitcoin investigation. There were no real tools around at the time – Chainalysis was just appearing – so we started doing a lot of these investigations manually, just using block explorers and things like that. There wasn't much in the way of attribution.

I guess the story circles around, and it's in my first book, actually, the story where a good friend of mine at a local police force called me about a hard drive that they had brought into the digital forensics lab. He asked: "how do I get the Bitcoin off this computer?"

And I said, "what do you mean?" He said: "well, how do I carve the Bitcoin off this computer? There's Bitcoin on it." I had a huge amount of respect for this guy – very intelligent and an excellent digital "forensicator", which is not a word, but you know – and I thought: "wow, that's the wrong question". And if he doesn't understand that's the wrong question, I'm guessing lots of people don't understand that that's the wrong question. So I just built a training course around investigating Bitcoin at the time, and it just went sort of law enforcement viral – we ended up teaching law enforcement in most primary countries around the world. And then, of course, we started doing lots and lots of investigations. A good friend of mine, myself and a guy called Luke, who's at TRM Labs, I think we did about 21 billion in value in Bitcoin investigations over the course of about four years. We then built advanced courses and so on and so forth, and then TRM Labs came along four years ago and bought CSI Tech, which was the company at the time. So there you go. There's the story.

«WE ENDED UP TEACHING LAW ENFORCEMENT IN MOST PRIMARY COUNTRIES AROUND THE WORLD. AND THEN, OF COURSE, WE STARTED DOING LOTS AND LOTS AND LOTS OF INVESTIGATIONS.»

And how would that course that went law enforcement viral hold up today??

Rock solid.

Really?

The only things that have changed are some of the block explorers. One or two no longer exist; some work in a slightly different way; some were generous in letting you download CSV files of accounts, and some no longer allow that. So some functionality has changed. But the book, *Investigating Cryptocurrencies* – which the course was based on, and which I was writing at the same time as the course – holds up. Bitcoin hasn't changed fundamentally. Addresses have changed over time and a few Bitcoin improvement protocols have gone through, but fundamentally nothing has really changed. It really is as it was.

But would you say crime through Bitcoin remains the same?

Well, that's interesting, because it segues into the second book, *There's No Such Thing as Crypto Crime*. The whole point of that clickbait title – if I can use that term – was that I was concerned we were seeing a great many very good police forces and investigation organisations building dedicated cryptocurrency investigation teams. Which is not, in itself, a bad thing.

It works.

But it is a bad thing if you see cryptocurrency crime as a new type of crime – which it isn't. I challenge anyone to come up with a brand new crime that doesn't have some background in the last 2,000 years of criminal history.

The Greeks were at it. Money laundering hasn't really changed; scams haven't really changed. We sometimes have a different mechanism, a different payment method, but fundamentally, somebody phoning you up and trying to socially engineer your seed words out of you is no different from somebody sending a text message asking for your password.

The techniques haven't changed at all. If you go back to people being told to go and buy a prepaid credit card, how different is that from being told to go to an ATM, buy some Bitcoin, and transfer it to the scammers? It's all the same. And it did worry me for quite some time that this wasn't being understood. I think it is now – that we can use the same fundamental investigative techniques we have always used and understood. Cryptocurrencies are just a plugin, and no more than that, really.

I'll quote you on that. But your course on investigating cryptocurrencies was built around the money laundering schemes that existed at the time. Now we're seeing funds moving through liquidity pools, bridges, and aggregators instead of centralised exchanges. And even with the increase in KYC requirements for centralised exchanges – doesn't this change the investigative methodology, or is the investigation fundamentally the same, just applied through different techniques?

Anyone that's been around policing, especially financial policing, so I would, you know, extend that out to all of those that are involved in financial crime, whether it be for legislature or whatever it might be, know that criminality is shifting very, very quickly and shifting those little methods and the way that they are achieving things and if there's a new service, can that service be exploited? And that's what changes. And if you read the money laundering chapter in the second book, it's good, but there are certainly a dozen more things that should be in there now.

That said, I've always believed that if you understand the fundamental way a cryptocurrency functions, you can get your head around new methodologies fairly quickly. You need something of a criminal mindset in that way. If you understand how Bitcoin works as a pseudo-currency – can we call it a currency? I don't think we can – if you understand how Ethereum works, how Tron works, if you understand their vagaries, then when new techniques emerge you can apply that knowledge to them. It's like a financial investigator who understands how a bank works: even if criminals use new techniques, the investigator understands the underlying system.

«IT IS A BAD THING IF YOU ARE SEEING CRYPTOCURRENCY CRIME AS A NEW TYPE OF CRIME, WHICH IT ISN'T.»

But do you think some techniques become genuinely independent new ways of committing crime? I'm thinking about privacy chains, Monero, layer 2 networks, are those game changers for fund tracing?

Yes, they are – they are technical methods for moving value. Are they truly new? In the way they function, yes, but we've had money mules walking across borders with fake passports. Is that not fundamentally the same as a non-traceable Monero address moving value from one place to another? I appreciate that sounds like a stretch, but there's often a historical parallel to what we're seeing now. I'm not underestimating the difficulty: some of these privacy coins do make things tricky. So we do have to keep up with technical innovation, but fundamentally, there are still very few crimes where the blockchain is the only evidence. There's almost always communication; there's almost always other evidence that helps you make those connections. If you're trying to dismantle an organised crime group using Monero tracing alone – enjoy, but you'll retire before you see success. In reality, tracing will form part of an investigation that, if successful, adds weight to a piece of the puzzle where you also have intelligence, surveillance, and other elements. And remembering that it's still very hard to buy anything with cryptocurrency: at some point, somewhere, it has to convert to fiat, and that's often the weak point. Good intelligence, good understanding of how these things work, that's what it comes down to. So again, it may sound like I'm downplaying it but I'm really not.

I understand. When you were talking about the mules, I was thinking it would be closer if they had those Stargate portals where they can just appear in different dimensions

Yeah, that's a very good point. And it feeds into something I've been saying for a long time: I've been a thorn in people's side about the language of sending and receiving cryptocurrency, because you don't send or receive anything. You simply unlock and lock on the blockchain. It never actually moves. And I've seen it written in court papers that "this Bitcoin was sent across borders into Russia".

It wasn't. It didn't move at all. Across the tens of thousands of blockchain ledgers for Bitcoin operating around the world at any given time, what may have happened is that someone else took control of it – someone who happened to be using a wallet and happened to be located in Russia, or wherever – but fundamentally, nothing moved.

I've seen a court decision where they said the suspect, who was my client, "had a blockchain", so, yes.

Nice. Maybe they did, and you gave it to them.

Well, it was the Bitcoin blockchain.

Well, there you go.

I see your point. The blockchain and tracing don't tell you a story, they give you breadcrumbs that you can build two different narratives around, either prosecution or defence. That's why you need corroborating evidence.

Yes, back when we were CSI Tech, prior to the sale to TRM Labs, we taught an open source intelligence gathering course alongside our cryptocurrency courses, because it was so important to be able to follow those breadcrumbs out into the broader digital world.

Understanding IP addresses, following the flow of network data, gathering information from social media – those things go hand in hand with blockchain tracing.

Slightly off topic, but you mentioned something about perhaps downplaying the relevance of cryptocurrency. We've seen people call it the internet of money – and yet you've rightly pointed out that you can't buy much with cryptocurrency, and that somewhere along the way anonymity tends to break down. Are you sceptical about the future of cryptocurrency as a legitimate medium of trade or investment?

I'm often asked this and I genuinely have no relevant opinion on it. What I will say is that I think blockchain technology is amazing. Satoshi Nakamoto – he, she, they, whoever it was – produced one of the most brilliant technical innovations of the last 100 years. The concept of cryptographically connected blocks and cryptographic transactions is just a beautiful thing, and it works. We do need to fix it for quantum computing in the next 15 years or so, perhaps sooner – Google seems to be making the fastest moves on that at the moment – but that's not an insurmountable undertaking. I think cryptocurrency has a future, because the technology is sound, even if it may look different from what we have today. And in many ways, because I never bought any, I'm not particularly invested in whether Tron succeeds or USDT gets adopted by the US government. As an investigator, I'm simply interested in how it can be used criminally and how investigators can best unravel the flow of funds.

«THERE'S STILL VERY, VERY, VERY FEW CRIMES WHERE THE BLOCKCHAIN IS THE ONLY EVIDENCE IN THE CRIME. THERE'S ALMOST ALWAYS COMMUNICATION. THERE'S ALMOST ALWAYS OTHER ELEMENTS OF EVIDENCE THAT COME TO BEAR THAT HELP YOU TO CREATE THOSE CONNECTIVES.»

That's interesting – you're personally not a big crypto investor, yet you say you need to think like a criminal to investigate. Does that mean you need to actually try how a mixer works, experiment with a liquidity pool, put it to improper use? Or is analy-

sing and studying how criminals use these tools sufficient?

People who specialise in identifying counterfeit banknotes spend most of their time studying what a genuine one looks like, not the fakes. Because when you truly know what a dollar or a five-pound note looks like, and all the security features built into it, identifying the counterfeit is straightforward. The same logic applies here: if you understand how a cryptocurrency or a mixer works, it's easier to recognise when it's being used badly. Do you need to actually use these things to understand them? Not really – the blockchain shows in public view what everyone else is doing with it. And many tools, like Tornado Cash, are open-source: it's a GitHub repo, you can download it and run your own instance in a lab if you want to. But it took Luke and me a single day, when Tornado Cash first appeared, to figure out how it worked and to find ways to trace through it – just by watching what everyone else was doing on-chain. We didn't need to feed funds through it ourselves.

As a tracer and investigator, what do you currently see as the biggest obstacle? The one you have a genuinely hard time getting past when tracing funds?

The problem isn't fundamentally the tracing. The problem is still the speed and capability of law enforcement's reaction – breadth of capability, the speed and willingness of exchanges to respond, and the weight of evidence required for a freezing order to get funds back to victims. Let me give you an example.

Or mutual legal assistance.

In the last two months, I had a call from a good friend of mine. His best friend's mother had just lost everything. Everything. GBP 1.2 million, everything she owned. She literally can't buy butter now. She had kept sending money to get her money back, the classic pattern: "we need another GBP 10,000 to release your funds", the whole thing. I heard about it, it had all been turned into crypto, I knew where it had gone. I'm not going to name the exchanges. I was able to call the heads of investigations at two exchanges and say: "it's Nick, this has happened, you've got the funds" – and they were on it immediately. They traced those funds.

I also called a very senior person in UK cryptocurrency policing, who said they were on it. I directed them to the exchanges. And we haven't recovered a penny. That pains me. These people had already reported the fraud to their local police, who said it was too big for them. It escalated to the team run out of City of London policing, who said they couldn't do anything. And then purely because I knew people, I was able to pick up the phone, and we still got nothing back. Nobody was at fault; it just all took too long.

And in that case, you knew the funds had reached a centralised exchange. But sometimes the problem is getting there. Before it reaches an exchange, it goes everywhere: mixers, money laundering schemes, chain hopping, bridges. Are those obstacles you find genuinely difficult to get through? Do you find them difficult to overcome, or is there always a lead, always a way?

No, they're not difficult to overcome.

The real question is: which case do you work on? People find me – my phone number, my email – and they reach out: "I've lost all this money, I don't know what to do". I get these constantly, and I try to help, usually for nothing.

Sometimes there are wonderful outcomes. I got EUR 15 million back for a woman a number of years ago, it's in the second book. Those results are wonderful, but it is always a question of which case you give your time to, and the police face exactly the same dilemma.

Everyone is in the same boat. The technology is not necessarily the hard part. Bridges are manageable, and I was tracing through mixers with pen and paper ten years ago. This stuff is doable. It just takes time. That's the issue.

You mentioned tracing with pen and paper, and now the tools are far more developed. But there comes a moment where all of this has to be written down in a report, put in front of a court, and used to make or break a case. What are the most common mistakes you see investigators making in those reports?

That's a difficult one to answer in 2026, because I work primarily with UK policing – very privileged to do so, some very good people – and an enormous amount has been invested in training crypto tracers and frontline officers: recognising when something is a crypto-related piece of evidence, understanding the pros and cons, knowing how to write it up. Within UK policing, I'm seeing really good reports, really good statements. So that's not where the biggest issue lies anymore. The next problem – and this is where I'd say the biggest challenge is in the UK – is the chain of understanding. The legal representative has to understand what's been written down, then the judge, and then twelve good men and women from the community who are not going to naturally understand how a blockchain works. One of the biggest vulnerabilities is this: cryptocurrency tracing is often inference. Very strong inference, but still inference. So, it's so easy for defence counsel to ask "is that 100%?". Because of the way a cluster is inferred, you have to say: "no, it's not 100%". And you can see where that goes. I've faced it in the witness box – much like DNA evidence, where someone can say "well, it's one in 17 million, but not 100%, is it?". You can never fully overcome that with inferred attribution, and that can be very damaging. Good charges are being laid in the UK, good statements are going in, but whether the Crown Prosecution Service, judges, and juries truly understand: that's the next major issue.

Do you ever provide assistance to defence counsel? That would require looking at the evidence collected and asking: "how do I break this? How do I show that this doesn't tell the story the prosecution says it does?".

I've done a great deal of defence work in the past, in digital crime more broadly. But about eight years ago, as we moved into crypto work, I made a decision to focus on supporting prosecution. I believe absolutely that everyone deserves a sound defence – in fact, a dear friend of mine was once sent by a judge on my course specifically to learn how to defend a client I was involved in prosecuting. He ended up being a very good friend, and he did a fantastic job for his client. But it was already a big enough undertaking to help get law enforcement trained to the right standard, without also working the other side. And very early on, as my name became known through the books, I was getting calls from both prosecution and defence simultaneously. Am I defence on this? Am I prosecution on this? It became unworkable. So with cryptocurrency, I placed myself in the prosecution camp, not because I think defendants don't deserve a good defence, but because hopping between the two was simply too difficult.

«THE PROBLEM IS STILL THE SPEED OF REACTION OF LAW ENFORCEMENT. I DON'T JUST MEAN SPEED, I MEAN CAPABILITY AS WELL, BREADTH OF CAPABILITY, THE SPEED AND DESIRE OF EXCHANGES TO RESPOND TO THOSE PROBLEMS, AND THE WEIGHT OF EVIDENCE NEEDED FOR FREEZING IN ORDER TO GET FUNDS BACK TO VICTIMS.»

Does your work involve exclusively the tracing, or do you also assist in building the narrative? Because the same tracing can support both a legal and an illegal explanation, especially with money laundering, where sometimes there's a predicate offence and sometimes there isn't...

That's absolutely true.

Sometimes you're using a mixer for privacy reasons rather than to launder money. And whether you're on the investigation side or the defence side, confirmation bias is human, it's inevitable. How do you try to guard against it?

It's a fascinating area. The OSINT course I mentioned actually spent the first half-day on bias, because it's so difficult to address. There are so many forms of bias in an investigation: some imposed by senior officers, some that arise simply from the feeling that someone looks guilty, or because other evidence is pointing in that direction. Very hard to manage.

My role has fundamentally been to teach and demonstrate: this is the evidence, these are the degrees of certainty that attach to it, this is what is definitive, this is

what is inferred, and then investigators have to write it up accordingly. It is very, very tricky.

But do you also teach how to interpret what the blockchain tells you and how do you find corroborating evidence of a specific narrative?

Always. One of the problems, David – and you touched on it earlier – is that there are simply so many techniques now. What do you even teach? I've always tried to build a tracing capability, with or without tools, and leave it to law enforcement and the appropriate legal representation to make of it what they will. But I've always felt it is critically important not to be definitive when something is not definitive. It's very easy to use the wrong language and find yourself in serious trouble once you're on the stand. "This equates to this" is a very different statement from "this almost certainly equates to this" – and the latter is usually the honest one.

«I HAVE PUT MYSELF SORT OF IN THE PROSECUTION CAMP, NOT BECAUSE I DON'T BELIEVE PEOPLE SHOULD HAVE A GOOD DEFENCE, BUT IT WAS TOO DIFFICULT HOPPING BETWEEN THE TWO.»

To conclude, you've been on both sides, prosecution and defence, but focusing now on the middle: what would you tell judges about what they should be alert to? What is the one thing you'd want them to pay attention to in order to assess whether the prosecution or the defence's narrative holds up?

Cryptocurrencies fundamentally are not that hard. Nobody tends to believe me when I say that, because the subject has become such a tangle of YouTube videos and noise that you have to set all of that aside and ask a simple question: how does a Bitcoin ledger work? Because fundamentally, it's very, very simple. How does an Ethereum ledger work? Slightly different, but equally simple. In my early courses, we used a spreadsheet to illustrate it and we even simulated mining with a couple of simple algorithms.

Very simple. We have built training programmes for the judiciary, and whether they engage with them, I don't know. But what we hope is that they understand the fundamentals, because from there, they can ask the right questions. Legal representatives are often very good at muddying the waters, at making something appear vastly complicated: "Don't worry about this, it's too hard to follow". I've seen that a great deal. Cryptocurrencies are not hard.

Thank you very much, Nick. We will use that as the opening line of the interview: "Cryptocurrencies fundamentally are not that hard".

Quote it freely – because they really aren't. At the start of *Investigating Cryptocurrencies*, I use the example of the stones on Yap – the great stone money – and how everyone in the village simply remembers who owns which stone. That is a distributed ledger in every sense. When you sold me some sheep and I gave you a stone, the stone never moved, because these things are the size of a person. We just told everyone in the village that I now own the stone that used to be yours. That is how Bitcoin works in its entirety: changing ownership on distributed ledgers. Very simple.

Although with crypto, new rocks appear every ten minutes, which is new.

Exactly, and that's the wonder of a distributed ledger. As I put it in the book: the moment you employ someone to sit in the middle of the village and write down who owns every stone, that's called a bank. You've taken it out of the distributed ledger in everyone's minds and put it onto a piece of paper. That's the fundamental difference.

Nick, thank you very much. This has been a true pleasure – we'll be in touch.

Fantastic – thank you for having me.

ARTIFICTIONAL INTELLIGENCE

In 2058, passwords had disappeared.

Authentication was done through memories: banks, courts and governments validated identities using personal recollections stored in neural vaults connected to the internet.

Until the “Gardener” appeared.

The victims began remembering crimes they had never committed. A judge confessed to a murder that never happened. A minister handed over military codes, convinced he had promised to do so years before.

Miguel Varela, a digital investigation specialist, discovered that all the victims had been through the same company: MnemoSyn, a memory optimisation clinic.

Upon infiltrating their servers, he found millions of human memories catalogued, editable and for sale.

Traumas could be erased. Alibis could be downloaded. Testimonies were fabricated like files.

But the worst came when Miguel found his own memories in the system – including the detailed recollection of a daughter who had never existed.

Days later, he actually began to remember her: the name, the voice, the laughter.

He then understood the true threat.

In a world where memory was the primary digital evidence, whoever controlled recollections controlled truth itself.

And justice had become nothing more than vulnerable software.

This image was generated using artificial intelligence.

DIGITAL DEFENSE

Digital Defence is a specialised service offered by Morais Leitão that addresses the legal, technical and evidential requirements arising from the intersection of cybercrime and law. ↗

Coordination

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

PORTUGAL
ANGOLA
MOZAMBIQUE
CAPE VERDE
SINGAPORE
TIMOR-LESTE
MACAU

LexMundi Member

mlgts.pt

3D: Digital Defense Dispatch
Coordination David Silva Ramalho
Volume 2
July 2026