LEVERAGING AI IN TRACKING ILLICIT FINANCIAL FLOWS

UMUT TURKSEN

LEVERAGING AI IN TRACKING ILLICIT FINANCIAL FLOWS

Umut TURKSEN
The University of Exeter

Abstract

This chapter delves into the intersection of artificial intelligence (AI) and the evolving role of law enforcement in addressing financial crimes, particularly those involving illicit financial flows. It offers an analysis of how AI technologies are transforming traditional investigative methods. The discussion begins by highlighting the growing necessity for integrating AI tools as emerging technologies become increasingly relevant in policing. Drawing on case studies inspired by the TRACE project, the chapter demonstrates how AI is reshaping law enforcement practices from advanced crime analytics to the application of knowledge graphs. Central themes include the operational advantages of AI, such as enhanced investigative efficiency, better resource allocation, and more informed decision-making. The chapter also critically examines the ethical dimensions of AI use in law enforcement, addressing concerns around bias, privacy, transparency, and accountability. By exploring both the challenges and opportunities of AI adoption, it provides a nuanced perspective on the complex dynamics shaping the future of law enforcement in the digital age.

Keywords

Illicit financial flows, policing, artificial intelligence, financial crime, money laundering

1. INTRODUCTION

Artificial Intelligence (AI) holds immense potential to revolutionise policing by executing certain tasks far more rapidly and efficiently than human officers. This capability offers Law Enforcement Agencies (LEAs) a strategic edge in combating crime, enabling more responsive, scalable, and effective operations. AI can streamline and enhance a wide range of investigative functions, including:

- Integration and analysis of complex datasets such as illicit financial flows, Suspicious Transaction Reports (STRs), electronic communications, images, and video footage (Sarzaeim et al., 2023; IBM, 2023).
- Prioritisation of threats and risks, allowing LEAs to focus resources on the most pressing dangers (Sarzaeim et al., 2023).
- Automated translation of large volumes of documents, facilitating cross-border investigations.
- Development of secure communication platforms to protect sensitive information.
- Creation of AI-powered training environments to enhance officer preparedness and decision-making.

However, the deployment of AI in law enforcement must be grounded in robust legal and ethical frameworks with specific requirements. Any AI tool used by LEAs must comply with legal standards related to data protection, fairness, bias mitigation, privacy, accountability, and the safeguarding of human rights. These considerations become even more critical when AI is used in contexts that may lead to criminal convictions and the deprivation of liberty. In such cases, the need for transparency, oversight, and due process is paramount.

While extensive research and publications have explored the intersections of predictive policing, AI, and fundamental rights (Sarzaeim et al., 2023; European Council, 2024; Council of Europe, n.d.), this chapter narrows its focus to the investigative phase of policing financial crime. Investigation phase often refers to the stage where a crime has moved beyond mere suspicion, and sufficient evidence exists to justify a formal investigation and initiate procedures for the seizure and confiscation of illicit assets.

Accordingly, the chapter identifies key areas where AI can be effectively deployed during investigations.

Before commenting on areas where law enforcement agencies need AI solutions, it is worth explaining key concepts and terms.

Illicit financial flows (IFFs):

In this study the definition of IFFs provided by the International Monetary Funds (IMF) is adopted.

IFFs refer to the illegal or illegitimate movement of money or capital across borders, typically in violation of national or international laws. These flows encompass funds that are illegally earned, transferred, or utilised, and they pose significant challenges to economic development, governance, and global financial stability. Although the specific language and emphasis vary among institutions, the core elements of IFFs are widely recognised.

Institutional definitions of IFFs include the following:

OECD (2014) defines IFFs as financial flows generated by methods, practices, and crimes that seek to transfer capital out of a country in contravention of national or international laws.

High Level Panel on Illicit Financial Flows from Africa (2015) describes IFFs as money illegally earned, transferred, or used, typically stemming from three main categories: commercial tax abuse, criminal activity, and corrupt practices by government officials. World Bank (2016) concisely defines IFFs as money illegally earned, transferred, or used that crosses borders. Global Financial Integrity (2017) emphasises IFFs as illegal movements of money or capital from one country to another i.e., funds that are illegally earned, transferred, and/or utilised across international boundaries. International Monetary Fund (2020) frames IFFs as the movement of money across borders that is illegal in its source, its transfer process, or its final use. All of these major definitions stress that IFFs involve illegality at one or more stages whether in how the funds are generated (e.g., through crime or corruption), how they are moved (e.g., through money laundering or falsified trade data), or how they are eventually used.

IFFs typically involve the international movement of funds, making them transnational in scope and difficult to trace and regulate, especially in the context of globalisation and digital finance.

Artificial Intelligence (AI): Definitions, Evolution, and Implications for Law Enforcement

There is currently no universally accepted definition of Artificial Intelligence (AI). However, the **EU AI Act** offers a broad and inclusive description, defining an AI system as software developed using one or more techniques listed in Annex I. These systems are capable of generating outputs such as content, predictions, recommendations, or decisions that influence the environments they interact with (European Council, 2024). The EU AI Act also categorises AI systems based on their intended purpose and the potential risks they pose.

Although this legal definition is relatively recent, the term "artificial intelligence" was first introduced by **John McCarthy in 1955** (Dick, 2019). Scholars such as **Russell and Norvig (2018)** describe AI as machines or computers that simulate cognitive functions typically associated with the human mind, such as learning and problem-solving. Some experts argue that the future of AI lies more in cognitive capabilities than in artificial mimicry (Joseph & Turksen, 2022).

AI is often classified into four conceptual categories:

1. **Thinking humanly;**
2. **Acting humanly;**
3. **Thinking rationally; and**
4. **Acting rationally** (Russell & Norvig, 2018).

However, equating AI with human thinking is misleading. Unlike human cognition, AI systems depend on three core components:

- **Computing power (hardware);**
- **Advanced algorithms (software); and**
- **Access to relevant and reliable data.**

All of these are designed, maintained, and provided by humans. Therefore, AI systems, especially in law enforcement, are inherently reliant on human input.

The "thinking rationally" approach defines AI as the study of computations that enable perception, reasoning, and action (Charniak & McDermott, 1991), while "acting rationally" focuses on designing intelligent agents (Poole, Mackworth & Goebel, 1998).

Although AI has existed as a concept for over half a century, its practical applications have surged only in the past decade due to the convergence of large datasets, powerful hardware, and sophisticated algorithms. This has led to the classification of AI into three generations:

- **First-generation AI** (Artificial Narrow Intelligence): These systems perform specific tasks and are embedded in everyday technologies like voice recognition, facial recognition, and autonomous vehicles (Poole, Mackworth & Goebel, 1998). Businesses also use them for process automation, cognitive insights, and engagement (Joseph & Turksen, 2022; Davenport & Ronanki, 2018).
- **Second-generation AI** (Artificial General Intelligence (AGI)): These AI agents can reason, plan, and solve problems beyond their original programming (Gutowska, 2024).

- **Third-generation AI** (Artificial Super Intelligence): Hypothetical future systems that could become self-aware and conscious, potentially surpassing human cognitive abilities. If realised, such systems would present profound technological, legal, ethical, and societal challenges, requiring new governance and law enforcement frameworks (UK Ministry of Defence, 2018).

For LEAs**,** this evolution means not only adopting AI to combat financial crime but also staying vigilant about new forms of AI-enabled criminal activity. Financial crimes often involve deception and the laundering of illicit proceeds. LEAs must sift through complex layers of legal and illegal activity as well as large volume of data to extract actionable intelligence. This includes identifying suspects, both individuals and entities, and tracing and recovering criminal assets.

The following sections explore user requirements, practical use cases and methods through which LEAs can leverage AI to enhance their investigative capabilities.

2. USER REQUIREMENTS

AI-supported forensic tools hold potential in financial crime investigations but remain underutilised due to training gaps, legal complexities, and limited resources. The TRACE project (2025) highlights key challenges such as legal fragmentation, cryptocurrency-related crimes, and digital communication tools used by criminals. TRACE project indicated that while digital forensic software is widely valued 64% of respondents rated it as important, AI tools are less frequently adopted, largely due to outdated infrastructure and a shortage of skilled personnel.

Law enforcement priorities include automatic data extraction, efficient sorting, and streamlined cross-border communication rather than adding more software (TRACE, 2025). Usability is key, with simple interfaces preferred over broad functionality. Additionally, encryption and decryption remain critical challenges as criminal groups advance faster than investigative technologies. Despite AI's promise, organisational deficits in infrastructure, expertise, and funding pose obstacles. LEAs stressed that balancing new technology with practical usability is essential for effective financial crime investigations (TRACE, 2025).

Furthermore, the lack of suspicious transaction reports (STRs) (also known as suspicious activity reports) that are submitted by designated non-financial businesses and professions (DNFBPs) has been given scant attention. Over recent years, the volume of Suspicious Transaction Reports (STRs) has increased markedly across multiple jurisdictions, reflecting enhanced regulatory vigilance, improved detection mechanisms, or a heightened awareness of financial crime risks. In Türkiye, STR submissions have surged from approximately 203,000 in 2019 to over 601,000 by 2023 (MASAK, 2024). This represents a nearly threefold increase and underscores significant progress in the country's anti-money laundering (AML) efforts, as well as a notable rise in the level of scrutiny applied by reporting institutions.

Further disaggregation of Türkiye's STR data reveals the growing relevance of DNFBPs. According to figures reported by MASAK, specific DNFBP segments contributed as follows in 2023:

- Courier services: 641 STRs
- Construction equipment suppliers: 42 STRs
- Lottery and gaming entities: 1,755 STRs
- Crypto asset service providers: 48,678 STRs
- Precious stones dealers and jewellers: 683 STRs

These figures demonstrate that while some DNFBP sectors remain relatively low in volume, others, particularly crypto asset providers, play an increasingly critical role in the country's STR ecosystem. The crypto sector alone accounted for over 8% of total STRs, reflecting its growing exposure to financial crime risks and the importance of regulatory engagement with digital finance.

In the United Kingdom, the landscape is similarly diverse. Between April 2020 and March 2022, the total number of STRs submitted rose from 742,317 to 901,255, representing an overall increase of 21.41%. Credit institutions, primarily banks, remained the leading source of reports, responsible for over 70% of total STRs across both periods. Banks submitted 637,776 reports in 2021–22, a 15.75% increase from the previous year.

Notably, building societies almost doubled their reporting activity (+90.8%), and other credit institutions also registered significant growth (+37.88%). Financial institutions such as money service businesses and non-bank entities posted moderate gains (13.28% and 13.01%, respectively).

In contrast, the engagement of non-financial professionals remains disproportionately limited. Despite a workforce comprising more than 357,000 accountants and 301,900 legal professionals, these sectors collectively contributed less than 1% of total STRs in both years. That said, their reporting volumes are trending upward, with accountants and tax advisers increasing submissions by 25.47%, and independent legal professionals by 29.07%.

Other sectors such as estate agents and high-value dealers reported minimal contributions and even registered slight year-on-year declines. Conversely, entities not regulated under Money Laundering Regulations (MLRs) saw a substantial increase in activity, with a 179.24% rise in STRs submitted during the period. This suggests either an expansion in voluntary compliance practices or a growing recognition of suspicious activity in areas previously considered peripheral to formal oversight.[1]

---

[1] For a detailed and comparative analysis of anti-money laundering regimes in the United Kingdom and Türkiye, see Turksen and Erken (2024).

In Germany a similar tend can be observed. In its fight against financial crime, the German banking sector stands at the forefront with 1,403 banks shouldering the overwhelming majority of STRs (Germany - FIU, 2020). Yet, a quieter puzzle lingers in the shadows of the 2020 FIU report whereby a vast network of professionals (particularly DNFBPs) legally obligated to report suspicious activity remains largely silent.

With over 61,000 accounting, bookkeeping, and auditing firms, and an estimated 165,000 lawyers, one might expect a robust stream of insights into possible money laundering or various predicate offences from these sectors. But their contribution to the national STR tally is surprisingly sparse. For example, accountants and auditors - despite being directly exposed to client finances - submitted only a trickle of reports. For example, according to figures from 2020, out of the 144,005 STRs, 23 came from lawyers, 7 from Auditors and chartered accountants and 15 came from tax advisors.

The narrative here is not one of blame but is one of opportunity. By enhancing outreach, clarifying expectations, and reinforcing the value of vigilance, all countries can better harness the untapped potential of information from its legal, accounting, and commercial sectors. After all, effective financial intelligence requires more than just watchful banks; it needs a whole-of-economy approach, with every obligated party playing its part. LEAs need to capture STRs from all sectors in its economy and draw up a holistic picture of financial crime, money laundering and IFF risks.

3. AI APPLICATIONS AND TOOLS IN POLICING

3.1. Examples of use cases

Various criminal activities involve IFFs ranging from:

- Financing of terrorism;
- Web forensics for tackling terrorism investigations;
- Property market transactions using cryptocurrency;
- Cyber extortion or ransomware;
- Deepfake payment scams;
- Money laundering with stolen art and antiquities; and to
- Online gambling for money laundering.

This non-exhaustive list of cases present scenarios that mirror the types of complex and organised crime operations often encountered by the police. These schemes frequently involve intricate money laundering tactics, the use of front companies, cross-border transactions, and digital methods of concealing funds, all of which tend to leave behind a trail of electronic evidence, such as emails, transaction records, or metadata. Given the scale, sophistication, and

digital nature of such crimes, it was determined that artificial intelligence–driven tools such as data mining, pattern recognition, and natural language processing could play a pivotal role in uncovering hidden connections, identifying anomalies, and supporting investigators in efficiently navigating large volumes of information to build strong cases.

Below are examples of how AI can feature in tackling some of these complex crimes and IFFs.

3.1.1. Digital and Web Forensics: A Critical Tool in Modern Investigations

Digital forensics, often referred to as web forensics when focused on internet-based evidence, is a specialised investigative process employed by cybersecurity professionals and law enforcement agencies. This discipline involves the systematic identification, extraction, analysis, and documentation of digital evidence, which can be pivotal in both criminal investigations and legal proceedings (Cobwebs, 2020).

The scope of web forensics encompasses a wide array of sophisticated and often creative methodologies. These are designed to uncover, compile, and present crucial information from digital environments, including computers, mobile devices, servers, and network infrastructures. The data retrieved from these sources is meticulously analysed to support investigative workflows and can serve as substantive evidence in the prosecution of crimes.

This technology has become an indispensable asset for LEAs, enabling them to unravel complex cases and trace digital footprints with greater precision (CEPOL, 2019). The integration of AI into forensic tools has further enhanced capabilities in Web Intelligence (WEBINT) and Open-Source Intelligence (OSINT). AI-powered solutions can automate data collection through Application Programming Interfaces (APIs) and web scraping, offering investigators advanced visual and analytical tools to interpret vast datasets.

The digital domain has also become a critical battleground in the fight against terrorism. Many activities associated with terrorist organisations such as financing, recruitment, and operational planning now occur in cyberspace. These activities often span global networks, utilising platforms ranging from mainstream social media to encrypted dark web forums. Terrorist groups can also receive direct financial support through online donations and transactions.

Given these evolving threats, there is a pressing need for innovative investigative techniques capable of capturing and analysing digital evidence related to terrorism (Joseph & Turksen, 2022). Past investigations have shown that relevant digital artifacts may include, but are not limited to:

- Passwords and encryption keys (e.g., BitLocker recovery keys found on separate devices)

- Communication records, analysed through keyword searches and manual review
- Content promoting anti-democratic ideologies or violent extremism
- Media files (texts, images, videos) linked to organised crime, such as arms or drug trafficking
- Evidence of blackmail, extortion, or money laundering
- References to events, gatherings, or affiliations (e.g., “Thor’s Thunder,” “Germanica”)
- Records of membership fees, donations, and financial transactions
- Real estate or goods-related transactions (rentals, leases, trades)
- Identifiable individuals and organisations, including aliases, hosted content, and blogs
- Financial documents, including unofficial agreements, bank details, and cryptocurrency transactions

The sheer volume and diversity of this data necessitate the use of AI-driven tools that can consolidate disparate sources, identify patterns, and generate visual representations of relationships and activities. These capabilities significantly enhance the efficiency and effectiveness of digital investigations, making them a cornerstone of modern law enforcement and counterterrorism efforts.

3.1.2. Property Market Transactions and Money Laundering: A Growing Concern

The real estate sector has long been a favoured avenue for criminals seeking to launder illicit funds. As noted by Forbes (2018), property transactions offer a seemingly legitimate front for integrating "dirty money" into the legal economy. Criminals often exploit the complexity and high value of real estate deals to obscure the origins of their funds.

According to a 2020 EUROPOL report, the economic downturn triggered by the COVID-19 pandemic has further exacerbated this issue. The recession has led to declining property prices in certain regions, making real estate even more attractive to criminal investors. These lower prices create opportunities for the acquisition of high-value assets using illicit profits, particularly in markets where oversight is weak or enforcement is inconsistent.

The property and construction industries are especially vulnerable to money laundering due to their dual utility: they serve both as investment vehicles and as plausible justifications for large financial transactions. Funds can be moved under the guise of construction costs, property development, or real estate purchases, making it difficult to distinguish legitimate activity from criminal enterprise.

In recent years, the integration of cryptocurrencies into property transactions has introduced new challenges for regulators and law enforcement agencies. As highlighted by PwC (2022), digital currencies such as Bitcoin, Dash, and Monero are increasingly being used to facilitate real estate deals. These privacy-focused coins offer a high degree of anonymity, making it difficult to trace the origin of funds or identify the individuals involved.

Unlike traditional financial systems, cryptocurrency transactions often bypass formal institutions like banks. This lack of institutional oversight complicates the process of conducting due diligence and verifying the legitimacy of funds. Moreover, blockchain, the underlying technology behind cryptocurrencies while transparent in structure, can still obscure the identities of transacting parties, especially when privacy-enhancing tools are used.

Without advanced analytical tools, LEAs face significant hurdles in mapping the flow of funds, identifying key actors, and establishing connections between transactions. The absence of such tools can severely limit the effectiveness of investigations into property-related money laundering schemes.

Several red flags can indicate potential money laundering through property transactions. These include:

- **Disproportionate Wealth:** Ownership of high-value properties by individuals whose declared income or assets do not justify such purchases.
- **Anonymity of Ownership:** Use of shell companies, trusts, or third parties to obscure the true owner of a property.
- **Price Manipulation:** Properties bought or sold at prices significantly above or below market value, potentially to disguise the movement of illicit funds.
- **Cross-Border Risk Indicators:** Countries identifying their citizens as posing a money laundering risk in foreign property markets.

Each of these typologies requires LEAs to analyse diverse datasets and uncover hidden relationships between entities, transactions, and assets. This necessitates the use of sophisticated digital tools capable of aggregating, visualising, and interpreting complex financial and ownership data.

3.1.3. Cyber Extortion & Ransomware

The **WannaCry ransomware outbreak** remains one of the most devastating cyberattacks in recent history, with global economic losses estimated at **£6.5 billion** (Acronis, 2025). While the ransom payments, typically demanded in cryptocurrencies like Bitcoin, garnered significant attention, the broader financial impact extended far beyond the immediate extortion. Ransomware attacks inflict **multifaceted damage** on affected organisations. These include:

- **Lost productivity** due to system downtime (Fouche & Solsvik, 2019);
- **Business continuity costs,** including emergency response and crisis management;
- **Service restoration expenses,** often extending beyond the targeted entity to its supply chain;
- **Reputational damage** and erosion of public trust; and
- **Long-term operational disruption,** affecting the normal course of business.

To effectively investigate ransomware incidents and uncover the infrastructure behind **Ransomware-as-a-Service (RaaS)** operations, cybersecurity professionals and law enforcement agencies rely on a diverse array of data sources. These include:

- Ransomware knowledge bases and removal guides;
- Reports from **Counter Threat Units (CTUs), Incident Response (IR)** teams, and **Security Operations Centers (SOCs);**
- Online forums where victims and researchers share Bitcoin wallet addresses linked to ransomware; and
- Secondary research databases and threat intelligence platforms.

The **fragmentation and heterogeneity** of these data sources present a major challenge. To address this, there is a growing need for **platform-agnostic AI tools** capable of automating complex analytical tasks and synthesising insights from different systems. One such solution is the **knowledge graph tool** developed by the TRACE project, which enables investigators to visualise relationships between entities, transactions, and digital artifacts, helping to bridge the gap in cyber extortion prosecution capabilities.

Based on well-documented cases of cyber extortion (FBI, 2025), several investigative techniques have proven effective in tracing ransomware actors:

- **Internal cybersecurity logs:** Analysing records maintained by the victim organisation's IT and security teams;
- **Criminal profiling:** Identifying patterns in the attacker's *modus operandi*;
- **Forensic linguistic analysis:** Examining phishing emails, ransom notes, and communications for linguistic fingerprints;
- **Malware attribution:** Identifying and linking malware code and exploitation techniques to known threat actors;

- **Data exfiltration tracing:** Locating repositories (e.g., Google Drive, Mega) where stolen data may have been uploaded; and
- **Open-Source Intelligence (OSINT):**
  - Scanning the **dark web** for chatter, leaked data, or illicit marketplaces
  - **Cross-referencing** information to build comprehensive threat profiles
  - **On-chain analysis** of cryptocurrency transactions to trace the flow of ransom payments.

While these investigative tasks are typically carried out by law enforcement and cybersecurity professionals, the **volume and complexity of data** involved can quickly become overwhelming. This is where **AI-powered tools** become indispensable. By connecting disparate data points such as IP addresses, wallet IDs, malware signatures, and communication patterns, AI can construct a **cohesive investigative framework** that highlights key actors, relationships, and potential leads.

Such tools not only **accelerate investigations** but also enhance the **accuracy and depth of analysis**, ultimately improving the chances of identifying and prosecuting cybercriminals involved in ransomware operations.

3.1.4. Online Gambling as a Channel for Money Laundering

Online gambling has emerged as a significant vector for **money laundering**, offering criminals a relatively low-risk and efficient method to disguise the origins of illicit funds (Fiedler, 2014). The laundering process often mirrors legitimate gambling activity, making it particularly difficult to detect (De Sanctis, 2019). By placing a series of bets often small and strategically designed to appear legitimate criminals can effectively "clean" large sums of money. Even with minor losses incurred during betting, the cost is often far lower than traditional laundering methods, which typically involve higher fees or riskier intermediaries.

The Online Gambling Market was valued at USD 78.66 Billion in 2024 and is projected to reach USD 153.57 Billion by 2030 (Yahoo Finance, 2025). This expansion, combined with the sector's inherent characteristics, makes it increasingly vulnerable to financial crimes such as fraud and money laundering. Several factors contribute to this vulnerability:

- **Virtual nature of products** – No physical goods are exchanged, making transactions harder to trace.
- **Virtual cash flows** – Digital transactions can be anonymised or routed through multiple platforms (EUROPOL, 2023).

- **Cross-border financial flows** – Funds often move across jurisdictions, complicating oversight.
- **Complex payment systems** – Use of e-wallets, cryptocurrencies, and layered payment processors obscures transaction trails.
- **Legal fragmentation** – Inconsistent or unclear regulatory frameworks across countries hinder enforcement.
- **High payout ratios** – These can be exploited to legitimise large sums of money quickly.
- **Tax-free winnings** – In jurisdictions like Germany, gambling winnings are not taxed, reducing scrutiny (European Council, 2022).

Moreover, many online gambling platforms are headquartered in **tax-friendly jurisdictions** such as Malta (Marx, n.d.), where regulatory oversight may be less stringent. These companies are often managed by a small number of specialised operators, further concentrating control and reducing transparency.

For LEAs, investigating money laundering through online gambling presents a formidable challenge. Tracing the flow of gambling proceeds, identifying associated individuals, and mapping their financial and asset networks requires the analysis of vast and complex datasets. Without advanced analytical tools, this process is time-consuming and resource intensive.

AI-driven data analytics and knowledge graph technologies offer a powerful solution. These tools can:

- **Aggregate and analyse data** from multiple sources, including gambling platforms, financial institutions, and blockchain ledgers.
- **Visualise cross-border transactions** and relationships between individuals, accounts, and assets.
- **Identify suspicious patterns** and anomalies in betting behaviour or fund movements.
- **Support real-time monitoring** and flagging of high-risk activities.

By enabling a holistic view of financial flows and connections, AI tools can significantly enhance the capacity of LEAs to detect, investigate, and prosecute money laundering activities in the online gambling sector.

The use of AI in combating money laundering through online gambling is just one example of its broader applicability in financial crime investigations. From asset tracking and fraud detection to counter-terrorism financing and tax evasion, AI technologies are increasingly essential in navigating the complexity and scale of modern financial ecosystems.

3.2. The application of OSINT and AI in criminal intelligence and counterterrorism

Open-Source Intelligence (OSINT) offers investigators a rich trove of publicly accessible data for various financial crime investigations. This includes financial documentation such as annual financial reports (e.g., accounting and audits), social media data revealing personal and professional networks, behavioural patterns, and digital footprints; public registries containing business ownership information, property records, and tax filings; and web-based materials such as online forums, blogs, and news articles pertaining to suspected criminal activity. The aggregation and analysis of these diverse data sources enable investigators to identify anomalies and previously unseen connections indicative of fraudulent activities or misconduct, providing crucial actionable intelligence to support effective investigations.

The capacity to leverage OSINT significantly enhances investigative capabilities, contributing to more efficient and comprehensive investigations of complex financial crime schemes. The incorporation of AI into OSINT workflows significantly improves the efficacy of financial crime investigations. Key AI technologies facilitating this enhancement include:

- Natural Language Processing (NLP), enabling the extraction of meaningful insights from unstructured text data within OSINT sources, identifying key phrases indicative of fraudulent activity, and analysing sentiment to gauge intent and deception;
- Machine Learning (ML), facilitating the detection of outliers and anomalies within vast datasets of financial transactions, and employing clustering algorithms to identify potentially collusive relationships between entities (e.g., manipulation of public procurement);
- Network Analysis, visualising and analysing complex relationships between individuals and organisations to uncover hidden connections and trace illicit financial flows;
- Computer Vision, including Optical Character Recognition (OCR), enabling the analysis of visual data such as scanned documents and images to extract textual information, identify forgeries, inconsistencies, or other anomalies indicative of fraudulent behaviour; and
- Image analysis techniques that can glean meaningful data from picture formats, identifying logos, individuals, locations, or objects relevant to the investigation.

The synergistic application of these AI techniques to OSINT data allows for the rapid identification of patterns and correlations that would be impossible to detect through manual analysis alone, substantially accelerating investigations and improving the probability of successful prosecution.

Furthermore, OSINT can facilitate a number of other tasks:

- Suspect and Associate Identification: The analysis of social media, public records (e.g., property and business registrations), and online forums reveals connections between individuals and organisations, enabling the mapping of potentially criminal networks.
- Financial Transaction and Asset Discovery: Examination of publicly available financial disclosures (e.g., annual reports, filings to competent authorities) facilitates the identification of suspicious transactions, hidden assets, and offshore accounts, enabling the tracing of illicit funds and supporting asset forfeiture proceedings.
- Timeline Reconstruction and Behavioural Pattern Analysis: OSINT data (e.g., social media posts, news articles) allows for the reconstruction of event timelines, revealing patterns of suspicious activity that may elude traditional investigative methods.
- Alibi and Statement Verification: OSINT data can corroborate or refute witness and suspect statements; for example, geolocation data from social media can be used to verify alibis.
- Investigative Lead Generation: OSINT frequently yields unforeseen insights that significantly advance investigations. This may include the discovery of undisclosed business relationships, conflicts of interest, or previously unknown evidence sources.

In addition to OSINT, data analytics can encompass Natural Language Processing (NLP) (Sarzaeim et al., 2023) and Large Language Models (LLMs) (IBM, 2023). NLP can be deployed in order enable AI to interpret and generate human language in a meaningful and useful way in various contexts such administrative tasks, record keeping, converting speech to written text, etc. Europol opines that large volume of text-based data such as interview transcripts, witness statements, online communications and social media posts, etc can be analysed swiftly and efficiently using NLP. As asserted earlier, a quick analysis of such information is particularly useful in crime-in-progress scenarios and during or in the aftermath of terrorist attacks (Europol, 2024). In particular, NLP can empower the investigators to classify, cluster, summarise, translate text (Dixon and Birks, 2021). In the TRACE project, NLP was utilised for entity recognition whereby legal and natural persons and their assets can be identified analysed in complex financial crime cases.

4. CYBER AND DIGITAL FORENSICS IN THE AGE OF AI

Cyber and digital forensics have long been foundational components of modern investigative practices, predating the widespread availability of artificial intelligence (AI). Traditionally, these disciplines have focused on the identification, preservation, extraction, and analysis of digital evidence from devices such as computers, mobile phones, servers, and networks.

However, the integration of AI has significantly transformed the landscape whereby we have seen **accelerating the speed, accuracy, and scope** of forensic investigations.

AI technologies now play a pivotal role in enhancing forensic capabilities across a wide range of applications. These include:

- **Video surveillance analysis** – Automating the detection of suspicious behaviour or anomalies in real-time footage.
- **Image and facial recognition** – Identifying individuals from photos or video frames with high precision.
- **Voice and speech recognition** – Matching audio samples to known voices or detecting synthetic speech.
- **Biometric analysis** – Including iris scans, gait recognition, and fingerprint matching.
- **Pattern recognition** – Detecting behavioural or transactional patterns that may indicate criminal activity.

For instance, what might take a human investigator for hours or even days - such as searching for a specific artifact in a massive dataset of stolen or missing items - can now be accomplished by AI in seconds. This efficiency not only saves time but also increases the likelihood of uncovering critical evidence that might otherwise be overlooked.

The rise of **deepfake technology** powered by AI-generated synthetic media that mimics real individuals' voices, faces, or behaviours has introduced new challenges in digital forensics. Criminals can now impersonate others to phish for sensitive information, commit fraud, or disseminate disinformation. AI tools are also being developed to **detect and verify the authenticity** of such content, helping to preserve the integrity of digital evidence and protect against deception (Press, 2024).

Moreover, AI's **predictive and analytical capabilities** are proving invaluable in tackling encrypted communications and concealed digital credentials. Advanced algorithms can assist in identifying patterns, decrypting data, and linking digital footprints to specific individuals or networks (Vurubindi & Narahari, 2024; Hayadi & Haryanto, 2022; Tan et al., 2022).

As AI continues to evolve and expand its role in cyber forensics, two critical considerations must be addressed. The first is **data quality and relevance**: AI systems are only as effective as the data they are trained on. For forensic applications, this means ensuring access to accurate, comprehensive, and contextually relevant datasets. Poor-quality or biased data can lead to false positives, missed connections, or flawed conclusions. The second is **legal and ethical Oversight**: The deployment of AI in policing and forensic investigations must adhere to **fundamental legal principles and ethical standards.** This includes respecting privacy

rights, ensuring transparency in decision-making, and maintaining accountability for how AI-generated insights are used. Without these safeguards, the credibility of both AI tools and the broader justice system can be undermined.

5. SAFEGUARDS IN POLICING WITH AI

As AI becomes increasingly integrated into law enforcement operations, it brings both transformative potential and significant ethical, legal, and operational challenges. To ensure that AI enhances public safety without compromising fundamental rights, a robust framework of safeguards is essential. These safeguards must address key areas of concern, including data privacy, algorithmic fairness, transparency, and accountability.

5.1. Data Privacy and Civil Liberties

One of the foremost concerns in deploying AI in policing is the potential infringement on **individual privacy and civil liberties**. AI systems often rely on vast amounts of personal data collected from surveillance cameras, social media, biometric databases, and other digital sources. Without stringent controls, this data can be misused or over-collected, leading to **unwarranted surveillance, profiling, or intrusion into private life.**

To mitigate these risks, law enforcement agencies must implement:

- **Clear data governance policies** outlining what data is collected, how it is stored, and who has access.
- **Strict access controls and audit trails** to prevent misuse.
- **Transparency with the public** about data usage and retention policies.

5.2. Algorithmic Bias and Fairness

AI systems are only as objective as the data they are trained on. If historical datasets reflect societal biases such as racial, gender, or socioeconomic disparities, AI can **replicate and even amplify these biases** in its outputs. This can result in **disproportionate targeting** of marginalised communities, eroding public trust and potentially violating anti-discrimination laws.

To promote fairness in the use of AI technologies, LEAs should adopt proactive strategies that address bias and accountability. This begins with conducting rigorous bias audits both before and throughout the deployment of AI systems, ensuring any potential discriminatory patterns are identified and mitigated. Equally vital is the use of training datasets that are diverse and reflective of the communities these agencies serve, to avoid reinforcing systemic inequalities. Additionally, involving independent oversight bodies to review algorithmic decisions enhances transparency and builds public trust, ensuring that the application of AI aligns with principles of justice and equity.

5.3. Complexity and Lack of Transparency

Many AI systems function as "black boxes", meaning their internal decision-making logic is opaque and not readily understandable, even to their own developers. This lack of transparency becomes especially problematic when such systems are employed in high-stakes environments, such as law enforcement, where they may influence decisions about arrests, surveillance priorities, sentencing, or the allocation of critical public resources. If these systems produce outcomes that cannot be clearly explained, it undermines accountability and public trust, especially in instances where decisions significantly impact individuals' lives. To mitigate these risks, it is essential that law enforcement agencies prioritise the adoption of explainable AI systems designed to make their reasoning and outputs understandable to human users. This goes beyond simply producing a result; explainable AI provides clear, interpretable justifications for each decision, allowing officers, supervisors, and even external auditors to evaluate whether the technology is operating fairly and within ethical bounds.

Moreover, training and education for law enforcement personnel are crucial. Officers and decision-makers must understand the capabilities, limitations, and potential biases of AI tools. Without this foundational knowledge, there is a real risk of over-reliance on automated systems or misinterpretation of their outputs, which can lead to unjust outcomes.

Most importantly, human oversight must remain central to all AI-assisted decision-making processes. AI should serve as a tool to support, not replace, human judgment. LEAs must retain ultimate responsibility for final decisions, ensuring that ethical reasoning, contextual awareness, and societal values are never sidelined in favour of algorithmic efficiency.

5.4. Over-Reliance on Technology

While AI can significantly enhance investigative efficiency, there is a risk that officers may become **over-reliant on automated systems**, potentially diminishing their own critical thinking and investigative skills. AI should be viewed as a **supportive tool**, not a replacement for human judgment.

To maintain balance, it is essential that regular **training** for officers on how to use AI responsibly is offered. It is also important that **collaborative decision-making** between human experts and AI systems are monitored as their accuracy. It goes without saying that **protocols for challenging or overriding AI recommendations** when necessary is absolutely necessary particularly in criminal investigations.

5.5. Cybersecurity Threats

AI systems themselves are vulnerable to **cyberattacks,** including data breaches, algorithm manipulation, and system sabotage. If compromised, these systems could be used to mislead investigations, leak sensitive information, or disrupt public safety operations. Accordingly, to safeguard AI infrastructure LEAs shall implement **robust cybersecurity protocols** and regular vulnerability assessments; use **encryption and secure authentication** for all AI-related systems; and develop **incident response plans** for AI-specific threats.

5.6. Legal and Ethical Uncertainty

The rapid pace of AI development often outstrips the evolution of legal and ethical frameworks. This creates a **regulatory grey area**, where law enforcement agencies must navigate complex questions about consent, accountability, and proportionality.

To ensure lawful and ethical use LEAs must:

- Align AI deployments with **international human rights standards**.
- Engage in **public consultations and stakeholder dialogues**.
- Advocate for **clear legislative guidance** on AI use in policing.

These safeguards and standards can strike the balance between responsible innovation, integrity and societal trust. The responsible use of AI in policing requires a **multi-stakeholder approach** involving technologists, legal experts, civil society, and law enforcement professionals. Continuous evaluation, ethical foresight, and transparent governance are essential to ensure that AI becomes a **trusted ally in the pursuit of justice**, rather than a source of harm or division.

6. RECOMMENDATIONS AND CONCLUSIONS

The following recommendations presented can be organised into distinct yet interrelated thematic policy areas. This structured approach facilitates a more cohesive and integrated development of legal and regulatory frameworks. By categorising the recommendations into themes such as regulatory reform, ethical governance, technological innovation, international cooperation, and capacity building, policymakers and stakeholders can better coordinate their efforts, avoid duplication, and ensure that reforms in one area reinforce and complement progress in others leading to a cohesive policy making. This interconnected strategy not only enhances policy coherence but also supports the creation of a resilient and adaptive ecosystem capable of responding to the evolving challenges posed by financial crime and emerging AI technologies.

6.1. Harnessing AI to Combat Financial Crime: Strategic Recommendations for the Future

The convergence of rapidly advancing artificial AI technologies and an increasingly complex geopolitical environment presents both transformative opportunities and significant challenges. As we approach breakthroughs in areas such as quantum computing and artificial general intelligence (AGI), the urgency for a proactive, adaptive, and forward-looking strategy to combat financial crime and money laundering becomes ever more critical.

This chapter builds on an analysis of current and emerging AI applications in financial crime investigations, offering a set of strategic recommendations aimed at equipping Law Enforcement Agencies (LEAs) with the foresight and agility needed to leverage AI effectively while mitigating its associated risks.

6.2. The Need for a Holistic and Coordinated Approach

TRACE project's scanning exercise revealed that the effective use of AI in anti-money laundering (AML) efforts depends on the intricate interplay between technological innovation, regulatory evolution, and international collaboration. While AI offers powerful tools to enhance AML capabilities, it also introduces new vulnerabilities such as the potential misuse of AI by criminal actors. Therefore, any national or international strategy must be comprehensive, addressing not only the technical deployment of AI but also its ethical, legal, and societal implications.

To build a resilient and future-ready AML ecosystem, the following actions are proposed:

6.3. Strategic Recommendations

As artificial intelligence (AI) becomes increasingly embedded in law enforcement and anti-money laundering (AML) efforts, it is essential to adopt a forward-looking strategy that balances innovation with responsibility. This requires a multi-dimensional approach that addresses legal, ethical, operational, and technological challenges.

To begin with, strengthening regulatory frameworks is paramount. Law enforcement agencies (LEAs) must ensure that legal and regulatory structures evolve in tandem with AI advancements. This includes enacting robust data protection and privacy laws, addressing ethical concerns around sensitive applications such as emotional recognition and automated financial surveillance, and clearly defining the legal boundaries for AI use in criminal investigations.

Equally important is the promotion of ethical AI development and deployment. AI systems must be designed and used in ways that respect fundamental rights. This involves ensuring transparency and explainability in AI decision-making, establishing mechanisms for informed consent and accountability, and actively mitigating bias particularly in high-stakes areas like predictive policing and AML analytics.

To uphold these standards, the establishment of independent AI ethics and oversight bodies is essential. These entities should be tasked with setting ethical guidelines, conducting regular audits and impact assessments, and ensuring compliance with human rights and anti-discrimination laws.

Given the transnational nature of financial crime, international cooperation is another critical pillar. Countries must work together to harmonise AML regulations, share intelligence and best practices, and participate in multilateral initiatives to prevent regulatory fragmentation and jurisdictional loopholes.

As AI and quantum computing evolve, so too do the threats they face. Therefore, enhancing cybersecurity infrastructure is vital. This includes investing in quantum-resistant encryption, developing AI-driven threat detection systems, and securing financial data and communication channels from malicious interference.

To support these efforts, there must be a concerted push to build expertise in AI and AML. This can be achieved through targeted education and training programs that bridge the disciplines of law enforcement, data science, cybersecurity, and ethics. Cross-disciplinary collaboration will be key to developing a workforce capable of navigating the complexities of AI-driven investigations.

At the same time, it is crucial to encourage responsible innovation. New AML technologies should undergo ethical impact assessments and be designed with privacy, fairness, and transparency in mind. Innovation must not come at the expense of public trust.

As financial ecosystems continue to evolve, particularly with the rise of blockchain, cryptocurrencies, NFTs, and decentralised finance (DeFi), AML strategies must adapt accordingly. This includes regulating smart contracts, monitoring emerging financial instruments, and addressing the unique risks posed by digital assets.

In an increasingly volatile world, LEAs must also prepare for geopolitical disruptions. This involves developing contingency plans, forming strategic alliances, and anticipating the impact of cyber warfare on financial systems and AML operations.

To stay ahead of sophisticated criminal tactics, investment in research and development is essential. Funding should support cutting-edge AI innovations, including artificial general intelligence (AGI) and multimodal systems, and foster public-private partnerships to drive progress in proactive threat detection and forensic analysis.

Finally, improving cross-border data sharing is critical to the global fight against financial crime. Establishing interoperable data-sharing protocols and fostering collaboration between financial institutions, regulators, and international partners will enable more effective detection and disruption of illicit financial networks.

Together, these strategic actions form a feasible roadmap for integrating AI into law enforcement and AML in a way that is effective, ethical, and future-ready. By embracing innovation while safeguarding fundamental rights, LEAs can not only keep pace with evolving threats but also lead the way in building a secure and just financial system for the future.

REFERENCES

Acronis. (2025). *Understanding the true, hidden costs of ransomware attacks on the business*. https://www.acronis.com/en-gb/blog/posts/costs-of-ransomware-attacks/

Apple. (2025). *Apple's first spatial computer*. https://www.apple.com/uk/newsroom/2023/06/introducing-apple-vision-pro/

Banks, J. (2014). *Online gambling and crime: Causes, controls and controversies*. Ashgate.

Bitcoin.org. . (n.d.). *Bitcoin – Open source P2P money*. https://bitcoin.org/en/

Bravyi, S., Gambetta, J. M., Klimov, P. V., & Martinis, J. M. (2022). The future of quantum computing with superconducting qubits. *Journal of Applied Physics, 132*(6). https://doi.org/10.xxxxx (add DOI if known)

BRICS. (2025). *BRICS is an intergovernmental organization consisting of ten countries - Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Indonesia, Iran, and the United Arab Emirates*. https://infobrics.org

Cellebrite. (n.d.). *Cellebrite – Digital intelligence for a safer world*. https://www.cellebrite.com/

Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution - Exploring technologies, applications, and emerging challenges. *Sensors, 24*, Article 1888. https://doi.org/10.3390/s24061888

Charniak, E., & McDermott, D. (1991). *Introduction to artificial intelligence*. Addison-Wesley.

Roodt, C., & Benson, B. (2015). Databases for stolen art. *SA Crime Quarterly, 52*, June.

CSIS. (2024). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cobwebs. (2020). *Web forensics for tackling terrorism investigation*. https://www.cobwebs.com/wp-content/uploads/2020/01/Web-Forensics-for-Tackling-Terrorism-Investigation-White-Paper.pdf

Council of Europe. (n.d.). *Financing of terrorism*. https://www.coe.int/en/web/moneyval/implementation/financing-terrorism

Cyber Management Alliance. (2025, January 20). *Top 10 biggest cyber-attacks of 2024 & 25*. https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about

Davenport, T., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, January–February. https://hbr.org/2018/01/artificial-intelligence-for-the-real-world

Dash.org. . (n.d.). *Dash – Digital Cash*. https://www.dash.org/

De Sanctis, F. M. (2019). *Technology-enhanced methods of money laundering: Internet as criminal means*. Springer.

Dewald, S. (2022). Detectives and technological frames: Integrating technology and social media into everyday work. *Policing and Society, 33*, 111.

Dick, S. (2019). Artificial intelligence. *Harvard Data Science Review, 1*(1). https://doi.org/10.1162/99608f92.92fe150c

Dixon, A., & Birks, D. (2021). Improving policing with natural language processing. In *Proceedings of the 1st Workshop on NLP for Positive Impact* (pp. 115–124). https://aclanthology.org/2021.nlp4posimpact-1.13.pdf

European Commission. (2012). *Online gambling in the Internal Market* (SWD(2012) 345 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0345&from=EN

European Commission. (2017). *Commission staff working document: Risks of money laundering and terrorist financing*(SWD(2017) 241 Final, pp. 124–128).

European Council. (2022). *Taxes in Europe Database v2*. European Commission. https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax

European Council. (2023). *Council adopts EU laws on better access to electronic evidence* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/

European Council. (2024, January 11). *Better access to e-evidence to fight crime*. https://www.consilium.europa.eu/en/policies/e-evidence/

European Council. (n.d.). *Taxes in Europe Database v2*. https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax

European Parliamentary Research Service. (2017). *Die Kapazität der Mitgliedstaaten zur Bekämpfung von Steuerstraftaten: Ex post Folgenabschätzung*. https://data.europa.eu/doi/10.2861/9432

European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence…*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

EUROPOL. (2020). *Beyond the pandemic: How COVID-19 will shape the serious and organised crime landscape in the EU*. https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know

EUROPOL. (2021). *Serious and Organised Crime Threat Assessment (SOCTA)*. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

EUROPOL. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment

EUROPOL. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement* (ISBN 978-92-95220-92-8).

Federal Bureau of Investigation. (2025). Major cases of cybercrime. https://www.fbi.gov/investigate/cyber/major-cases

Fiedler, I. (2014). Online gambling as a game changer to money laundering? In W. O. Ötsch et al. (Eds.), *The political economy of offshore jurisdictions* (pp. 79–98). Marburg.

Fiedler, I., Körner, M., & Najman, N. (2017). *Das Geldwäscherisiko verschiedener Glücksspielarten*. Wiesbaden. http://link.springer.com/10.1007/978-3-658-16625-0

Fiedler, I., et al. (2020). *Regulierung von Onlineglücksspielen*. https://doi.org/10.1007/978-3-658-29846-3

Financial Times. (2019, May 29). London properties worth £80m targeted in 'dirty money' probe. *Financial Times*. https://www.ft.com/content/9b1a3e7a-814d-11e9-b592-5fe435b57a3b

Forbes. (2018, November 21). Criminals are using your dream home to clean dirty money. *Forbes*. https://www.forbes.com/sites/vishalmarria/2018/11/21/criminals-are-filling-your-dream-home-with-dirty-money

Forbes. (2024, August 6). Detecting deepfakes: Fighting AI with AI. *Forbes*. https://www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/

Fouché, G., & Solsvik, T. (2019, March 19). Aluminium maker Hydro battles to contain ransomware attack. *Reuters*. https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUSKCN1R00NJ

Germany Financial Intelligence Unit. (2020). Annual report 2020. https://www.zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2020_en.pdf?__blob=publicationFile&v=2

Freeman, M., & Ruehsen, M. (2013). Terrorism financing methods: An overview. *Perspectives on Terrorism, 7*(4), 112–130.

GetMonero.org. . (n.d.). *Monero – Private digital currency*. https://www.getmonero.org/

Gottschalk, P. (2010). Knowledge management technology for organized crime risk assessment. *Information Systems Frontiers, 12*, 267–281.

Gottschalk, P., & Solli-Sæther, H. (2010). Computer information systems in financial crime investigations. *The Journal of Computer Information Systems, 50*, 41–47.

Grand View Research. (2019). *Online gambling market size, share & trends analysis report*. https://www.grandviewresearch.com/industry-analysis/online-gambling-market

Gutowska, A. (2024, July 3). What are AI agents. *IBM*. https://www.ibm.com/think/topics/ai-agents

Hodgson, G. S., & Jiang, S. (2021). *Online money laundering: Methods and countermeasures*. Edward Elgar Publishing.

Home Office. (2018). *UK anti-corruption strategy: 2017 to 2022*. https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

i2 Analyst's Notebook. (n.d.). *IBM i2 Analyst's Notebook*. https://www.ibm.com/products/i2-analysts-notebook

IBM. (2023, November 2). What are large language models (LLMs)? https://www.ibm.com/think/topics/large-language-models#:~:text=LLMs%20consist%20of%20multiple%20layers...

IMF. (2022). *Global financial stability report: Navigating the high-inflation environment*. International Monetary Fund. https://www.imf.org/en/Publications/GFSR

Knapp, E. D., & Langill, J. T. (2015). *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems* (2nd ed., Ch. 7). Elsevier.

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of cryptocurrency in money laundering: Examining bitcoin transactions. *International Criminal Justice Review, 27*(4), 355 372. https://doi.org/10.1177/1057567717738263

KPMG. (2023). *2023 fraud outlook report*. https://home.kpmg/xx/en/home/insights/2023/01/kpmg-2023-fraud-outlook.html

Khullar, K. (2025, March 6). World's first 'body in a box' biological computer uses human brain cells with silicon-based computing. *Tom's Hardware*. https://www.tomshardware.com/tech-industry/worlds-first-body-in-a-box-biological-computer-uses-human-brain-cells-with-silicon-based-computing

Levi, M., & Soudijn, M. (2020). Understanding the laundering of criminal proceeds via online gambling. *European Journal on Criminal Policy and Research, 26*(1), 85–103.

Littler, A. (2020). How the EU's regulatory approach to gambling is failing. *Maastricht Journal of European and Comparative Law, 27*(1), 56–72. https://doi.org/10.1177/1023263X19888997

Lugo, G., & Faiella, G. (2020). *Cryptocurrencies and money laundering: An overview*. Bank of Italy Occasional Paper No. 559. https://www.bancaditalia.it/pubblicazioni/qef/2020-0559/QEF_559_20.pdf

MASAK. (2024). Annual report 2024. https://ms.hmb.gov.tr/uploads/sites/12/2025/05/Annual-Report-2024-f38e7dcb6b09ee98.pdf

MI5. (2023). *Threats to the UK: Espionage, cyber-attacks and terrorism*. https://www.mi5.gov.uk/threats-to-the-uk

Mutalib, N. H. A., Sabri, A. Q. M., Wahab, A. W. A., et al. (2024). Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: A review. *Artificial Intelligence Review, 57*, 297.

National Crime Agency (NCA). (2021). *National strategic assessment of serious and organised crime 2021*. https://nationalcrimeagency.gov.uk/who-we-are/publications/539-national-strategic-assessment-of-serious-and-organised-crime-2021/file

OECD. (2022). *Tax crime investigation maturity model*. https://www.oecd.org/tax/crime/tax-crime-investigation-maturity-model.htm

Palmer, C. (2021). *Digital forensics: The fascinating world of forensic science*. Rosen Publishing.

Poole, D. L., Mackworth, A. K., & Goebel, R. (1998). *Computational intelligence: A logical approach* (pp. 1–2). Oxford University Press.

Press, G. (2024, August 6). Detecting deepfakes: Fighting AI with AI. *Forbes*. https://www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/

PwC. (2022). *Bitcoin, cryptocurrency, blockchain... So what does it all mean?* https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html#:~:text=Blockchain%20is%20the%20technology...

PwC. (2023). *Global economic crime and fraud survey 2023*. https://www.pwc.com/gx/ en/services/ forensics/economic-crime-survey.html

Reuters. (2024, January 30). Elon Musk's Neuralink implants brain chip in first human. *Reuters*. https://www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/

Roodt, C., & Benson, B. (2015). Databases for stolen art. *SA Crime Quarterly, 52*.

RsCase. (n.d.). *rsCase – Investigation case management software*. https://www.rstech.de/en/products/rscase/

Russell, S., & Norvig, P. (2018). *Artificial intelligence: A modern approach*. Prentice Hall.

Sandotra, N., & Arora, B. (2024). A comprehensive evaluation of feature-based AI techniques for deepfake detection. *Neural Computing & Applications, 36*, 3859–3887. https://doi.org/10.1007/s00542-024-06491-x

Sarzaeim, P., Ahmadi, H., Alipour, M., & Borumand, M. (2023). A systematic review of using machine learning and natural language processing in smart policing. *Computers, 12*(12), 255.

Shami, S., & Rohatgi, S. (2024). Understanding and mitigating advanced persistent threats in a dynamic cyber landscape. In G. Shrivastava et al. (Eds.), *Emerging threats and countermeasures in cybersecurity*. Scrivener Publishing LLC.

Tan, Y. J., Ramachandran, S., Jabar, M. A., et al. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

Tombul, F., & Cakar, B. (2015). Police use of technology to fight against crime. *European Scientific Journal, 11*, 286.

TRACE Project. (2025). *Developing AI solutions to disrupt illicit money flows*. https://trace-illicit-money-flows.eu

Turksen, U., & Erken, E. (2024). Anti-money laundering and the law: Comparative approaches to countering predicate crimes. Routledge.

UK Ministry of Defence. (2018). *Joint concept note 1/18* (p. 11).

UK National Cyber Security Centre. (2024, January 1). Heightened threat of state-aligned groups against western critical national infrastructure. https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

UNODC. (2021). *Money laundering through the gambling sector*. https://www.unodc.org/unodc/en/money-laundering/gambling-sector.html

Uyar, T. (2024, March 23). ASI as the new god: Technocratic theocracy. *Computers and Society*. https://arxiv.org/abs/2406.08492

Van Duyne, P. C. (2016). Money laundering: Estimates in fog. *Trends in Organized Crime, 19*, 199–213. https://doi.org/10.1007/s12117-016-9282-3

Vurubindi, P., & Narahari, S. C. (2024). Encryption and decryption algorithms in private AI. In U. V. Maheswari & R. Aluvalu (Eds.), *Sustainable development using private AI*. CRC Press.

Werner, J. (2024, June 19). God-like AI and the decentralized internet. *Forbes*. https://www.forbes.com/sites/johnwerner/2024/06/19/god-like-ai-and-the-decentralized-internet/

World Bank. (2016). *Do digital technologies facilitate illicit financial flows?* http://hdl.handle.net/10986/23803

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023

Yahoo Finance. (2025, May 16). Online gambling industry report, Research & Market. https://uk.finance.yahoo.com/news/online-gambling-industry-report-2025-115100418.html

Yates, D. (2016, April 21). Soft control and the illicit trade in antiquities. *Trafficking Culture*. http://traffickingculture.org/

ABOUT AUTHOR

Prof. Dr. Umut TURKSEN | The University of Exeter |
U.Turksen[at]exeter.ac.uk | ORCID: 0000-0002-3143-6072

Dr. Umut Turksen is a Professor in Law at the University of Exeter. Umut is a business-facing legal scholar, and he is interested in the practical application of the law in risk, compliance and development for businesses. He has provided consultancy and training to prestigious international businesses and government projects on societal security, countering financial crime and terrorist financing and AI governance. He led the EU funded project "PROTAX," which focused on countering tax crimes and corruption in Europe and he has recently coordinated the EU funded project, TRACE, which has created technology based solutions (including AI) for investigation of illicit money flows. Umut is an advisor for legal, social and ethics impact assessment of the EU funded project, KEYSTONE, which focuses on standardisation of data management and data exchange and compliance across transport sectors and state authorities. In addition to his expertise in comparative risk and compliance across civil and common law jurisdictions, Umut is an expert in international law and EU law and has published extensively on energy law and security, international trade law and development, and arbitration.