1

Introduction

Adam Abukari, Athina Sachoulidou, Dimitrios Kafteranis, and Umut Turksen

1.1 KEY CONCEPTS AND DEFINITIONS

Europol has stated that 'to effectively disrupt and deter criminals involved in serious and organised crime, law enforcement authorities need to follow the money trail as a regular part of their criminal investigations with the objective of seizing criminal profits' (Europol, 2020a). Law enforcement agencies (LEAs) around the world continue to face old, new, and complex transnational security threats, inter alia, ransomware and cyberattacks on critical sectors and supply chain networks, white supremacist terrorists, social platform financial transactions, illicit use of crypto-currencies, and money laundering.

Countering organised financial crime and terrorist financing requires targeting financial flows related to these groups. Generally speaking, identification of suspicious financial flows is governed by anti-money laundering (AML) regimes of each country and the protocols under these regimes take a risk-based approach to single out individuals, companies, or transactions for closer scrutiny. Information from public and private sources is used on a case-by-case basis to establish sufficient evidence for further action. However, it is difficult to integrate these single cases into a larger strategic context for a variety of reasons such as national legal barriers, lack of inter-agency communication, technical capacities or human resources, insufficient cooperation between public and private sectors, and conflicts of interest. Furthermore, analysing hundreds of thousands of suspicious activity reports (White & Chase, 2025) and establishing risk profiles and intelligence based on real-time analysis of money flows between organised criminals (including terrorists of all stripes) are major challenges.

Indeed, according to a Europol 2016 report, 98.9 per cent of estimated criminal proceeds in the European Union (EU) are not confiscated and remain at the disposal of criminals and only 1 per cent of criminal assets are recovered. Given the estimation that criminal proceeds reach up to 3.6 per cent of global gross

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

domestic product (GDP) (Europol, 2016),[1] there is an urgent need to improve not only detection and tracking of money flows but also asset recovery methods.

This context has given the impetus for the book, which aims to critically analyse how emerging technologies such as artificial intelligence (AI) and machine learning can be leveraged to aid complex financial crime investigations in Europe. In doing so, our study has focused on the responsible and effective integration of AI into the detection, investigation, and governance of financial crime, with a particular emphasis on law enforcement, ethical considerations, and regulatory frameworks.

The book employs doctrinal, socio-legal, comparative, and empirical research methodologies. The book is an output of rigorous discourse on the beneficial interaction between law in books and law in action regarding the evidential basis and new methods for fighting financial crimes and illicit money flows (IMFs). It is based on the findings of three years of research conducted by the TRACE project (https://trace-illicit-money-flows.eu), which has been funded by the EU Horizon 2020 Research & Innovation Programme (Grant Agreement No. 101022004). The research for the TRACE project has been developed – in close cooperation with policymakers, law enforcement agencies, tax authorities, financial intelligence units (FIUs), ministries, prosecutors, judges, lawyers, and non-governmental organisations.

While there are many studies and reports on the use of AI for the purposes of public governance, including law enforcement, these studies remain generic, lack input from end-users (e.g., empirical evidence and user requirements from LEAs), and do not consider the use of AI in specific organised financial crime schemes. As a result, this book is likely to become a pivotal reference point for ethical and legal use of AI in law enforcement and obtaining court-proof evidence for successful prosecution.

The book is not only an outcome of interdisciplinary investigation but also a practical guide. It provides an interdisciplinary analysis of whether and to what extent technological AI tools for law enforcement in Europe are fit for purpose in countering some of the most pressing forms of financial crime in Europe and the recovery of proceeds from such crimes. It introduces novel frameworks for risk assessment, due diligence, and cross-border cooperation, enriched by stakeholder perspectives from law enforcement, banking, and policymaking communities.

By bridging theory and practice, and combining rigorous analysis with actionable insights, the book makes a vital contribution to the global discourse on AI and financial crime. It advocates for a harmonised approach that effectively integrates normative standards with innovative technical design to counter financing crime. Additionally, the book offers foresight into emerging technologies and virtual assets (e.g., non-fungible tokens – NFTs) that may be used for criminal purposes. The

[1] Global GDP is estimated to be USD 106.172 trillion thus making proceeds of crime to be around USD 3.8 trillion (World Bank, 2023).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

book also puts forward recommendations as to how technological advancements and legal gaps can be addressed to optimise efficacy and efficiency of law enforcement and exchange of information amongst LEAs and judicial authorities.

The book consists of ten chapters. Before we provide the summary of each chapter of this book, explanations of key terms that are utilised in our study may be useful for the readers.

1.1.1 *What Are Illicit Financial (or Money) Flows (IFFs)?*

When we refer to IFFs we have adopted the definition provided by the International Monetary Fund (IMF, 2020) that states 'the movement of money across borders that is illegal in its source, its transfer, or its use'. Having said that illicit financial transactions also encompass assets other than money such as real estate, crypto currencies, artwork, precious metals, and so on.

In tandem with IMF's definition of IFFs, there have been slightly different explanations of IFFs. According to the Organisation for Economic Co-operation and Development (OECD), IFFs include flows 'generated by methods, practices and crimes aiming to transfer financial capital out of a country in contravention of national or international laws' (OECD, 2014, p. 16).

High Level Panel on Illicit Financial Flows from Africa defines IFFs as 'Money that is illegally earned, transferred, or utilised. These funds typically originate from three sources: commercial tax evasion, trade mis-invoicing, and abusive transfer pricing; criminal activities, including the drug trade, human trafficking, illegal arms dealing, and smuggling of contraband; and bribery and theft by corrupt government officials' (African Union, 2015, p. 9). World Bank (2017) defines IFFs as 'Money illegally earned, transferred, or used that crosses borders'. Global Financial Integrity (GFI, 2025) defines IFFs as 'Illegal movements of money or capital from one country to another', or, in other words, funds crossing an international border that are illegally earned, transferred, and/or utilised (GFI, 2025).

1.1.2 *What Is AI?*

Since McCarthy coined the term in 1955, artificial intelligence (AI) has fascinated everyone's imaginations, though no single definition exists. AI is commonly described as machines mimicking human cognitive functions like learning and problem-solving (Norvig & Russell, 2015). Its future is often viewed as cognitive rather than purely 'artificial' (Kelly et al., 2023), aligning with human intelligence in processing information and solving problems (Gardner, 1999).

AI has been defined through four approaches: thinking humanly, acting humanly, thinking rationally, and acting rationally (Norvig & Russel, 2015). Thinking and acting humanly equate to machines performing tasks requiring human-like intelligence (Haugeland, 2000; Kurzweil, 1999). However, unlike human cognition, AI

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

depends on hardware, advanced algorithms, and reliable data – all provided by humans (Joseph and Turksen, 2022).

'Thinking rationally' frames AI as the study of computations enabling perception, reasoning, and action (Charniak & McDermott, 1985), while 'acting rationally' sees it as designing intelligent agents (Poole, Mackworth, & Goebel, 1998).

Although AI has existed for over 50 years, only recent advances in data, hardware, and algorithms have made widespread application viable. AI's development is also categorised by generation: First-generation or 'narrow AI' handles specific tasks (e.g., facial recognition, autonomous vehicles) and supports business functions such as process automation, cognitive insight, and engagement (Davenport & Ronanki, 2018). Process automation transitions tasks with minimal human input. Cognitive insight uses algorithms to analyse data patterns for decision-making (Van Camp et al., 2017; Labadze et al., 2023) and it is this type of AI that has been the focus of this book. These systems are probabilistic, producing not just outputs but hypotheses and recommendations which can be followed further by financial crime investigators. For AI to support investigation of financial crime and tracing IFFs effectively, access to reliable data is essential because fragmented, manipulated or proprietary datasets could undermine analyses and decisions provided by AI (UK Ministry of Defence, 2018).

The anticipated second-generation AI, or artificial general intelligence (AGI), will reason and solve unfamiliar problems autonomously. It will operate through non-deterministic systems that can explain their reasoning.

A future third-generation AI, or artificial superintelligence, would involve conscious, self-aware systems capable of surpassing human decision-making. This could pose significant ethical, legal, and societal challenges, demanding new governance models (UK Ministry of Defence, 2018).

AI's rapid evolution has prompted growing discussion around ethics and regulation, particularly in government use (Ranchordas, 2021), a topic that is discussed in detail in Chapter 5 of this book. Traditional regulatory frameworks struggle to keep pace with emerging technologies. AI's deployment in policing, in general, and in financial crime investigations, in particular, raises significant ethical and practical concerns, which are discussed in Chapter 6.

The EU AI Regulation defines AI systems as software using listed techniques to generate outputs – predictions, decisions, or recommendations – aligned with human-defined goals (EU AI Act 2024). It also categorises AI based on deployment risks and intended purposes.

1.1.3 *What Is Machine Learning?*

Machine learning refers to an area of computational algorithms that are designed to emulate human intelligence by learning from the surrounding environment and big datasets available (Mitchell, 1997; El Naqa and Murphy, 2015; Paria et al., 2023).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

Techniques based on machine learning have been applied successfully in diverse fields ranging from pattern recognition, computer vision, spacecraft engineering, finance, policing, entertainment, and medical applications (El Naqa and Murphy, 2015).

1.1.4 *What Is Decentralised Finance (DeFi)?*

DeFi is a growing area in the blockchain, cryptocurrency, and non-fungible tokens space. It refers to financial applications and services built on top of blockchain technology and operating in a decentralised and thrustless form (Sharma, 2021 and Adamyk et al., 2024). DeFi enables various financial transactions and activities without intermediaries such as banks or governments. DeFi can be exploited by criminals to move and launder their assets (Carpentier-Desjardins et al., 2025).

1.1.5 *What Are Automated Law Enforcement Systems (ALESs)?*

ALESs are AI-powered tools, which LEAs use to support investigative processes, surveillance, and decision-making. These include predictive policing algorithms, automated risk scoring systems, and facial recognition technologies. These systems can enhance efficiency and resource allocation in fighting financial crime, but they are also associated with concerns such as privacy, bias, and accountability (Bag, 2024). In Chapter 5 of this book, we critically examine the ethical and legal implications of automated law enforcement, proposing a 'matching exercise' that aligns normative standards with technical design. In Chapter 5, we also introduce frameworks for ensuring data integrity and de-biasing algorithms, which contribute to a more transparent and rights-respecting use of AI in policing.

1.2 BOOK OUTLINE

Summaries of the chapters of the book are as follows. Chapter 2 explores the landscape of global AI regulation, and how these emerging technologies are being defined and conceptualised. It offers a comparative analysis across four major legislative orders, namely the European Union, the UK, China, and the USA. Each of them is adopting distinct frameworks for regulating AI, shaped by diverse ideological and normative attitudes towards human rights, innovation, and the preservation of state power. The chapter explores the legal and socio-ethical implications of governing AI, especially how differing stances on transparency and risk are set to influence its international development. Building upon current governance approaches to AI, this chapter draws on insights from interviews and focus groups with LEA experts to address the use of AI-powered solutions in law enforcement and the operational and societal challenges that they present; focusing on the impact and use value of advanced data processing and data analysis technologies for daily

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

investigative work. Overall, the chapter contributes to a nuanced understanding of the multifaceted dimensions surrounding AI governance and its impact on law enforcement practices internationally.

In Chapter 3, we argue that obliged entities and LEAs face similar challenges in efficiently assessing and mitigating money laundering risks related to clients, transactions, and suspicious transaction reports (STRs). We present a novel geographic risk assessment framework designed for use in both administrative and commercial practice. The framework builds on the notion that financial secrecy creates a criminogenic environment, enabling IFFs to hide and move more easily. Since IFFs are sensitive to jurisdictional levels and types of financial secrecy, incorporating measures of secrecy is crucial for effective risk assessments in large-scale financial datasets. We combine Financial Secrecy Index scores as proxies for geographic markers of financial secrecy with transaction values to compute an IFF risk score for each transaction. The framework requires only minimal input data and produces a clear, dynamic risk score that avoids subjective, discriminatory, or politically biased judgements. We exemplify this approach by applying it to the FinCEN files – leaked STRs published by the International Consortium of Investigative Journalists (ICIJ). Ultimately, we demonstrate how even modest harmonisation of STR formats, when paired with robust risk assessment, can transform a largely under-utilised volume of reports into a structured and strategic repository of prioritised red flags, empowering more effective countermeasures against IFFs.

In Chapter 4, we provide an exploration of the intersection between artificial intelligence (AI) and the evolving landscape of law enforcement in the context of financial crimes. We also offer a detailed examination of the transformative impact of AI technologies on traditional investigation techniques. The chapter begins with an overview of the need to integrate AI tools, as emerging technologies expand, in law enforcement. Through a series of case studies inspired by the TRACE project, the authors illustrate how AI is reshaping law enforcement practices, from crime analytics to the use of knowledge graphs. Key themes include an analysis of the operational benefits derived from AI, such as enhanced investigative capabilities, resource optimisation, and improved decision-making processes. The ethical considerations inherent in the use of AI in law enforcement are carefully dissected, addressing issues of bias, privacy concerns, and the need for transparency and accountability. By delving into the challenges and opportunities presented by AI adoption, the chapter offers a nuanced understanding of the complex dynamics at play. Policymakers, law enforcement professionals, and academics will find this work to be a valuable resource, providing insights into the responsible integration of AI to augment public safety efforts.

In Chapter 5, we demonstrate that as cybercrime blends with traditional offences and criminal investigations become more complex, LEAs require innovative investigative tools, enhanced skills, organisational and regulatory adaptations. Enabling technologies, including but not limited to AI, may have the potential to

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

revolutionise how LEAs operate, but often this comes along with concerns for fundamental rights. The need for a careful balancing act has already been reflected in the contents of the EU AI Act – with the use of AI for law enforcement purposes becoming – not surprisingly – the 'apple of discord' during the trilogue negotiations. These debates made it prevalent that normative standards alone may be insufficient if not combined with creative technical design solutions that will be inspired by human rights considerations and translate abstract ethical values and normative standards into tangible results. Driven by this, this chapter first discusses the implications of automated law enforcement – with a focus on AI-enabled crime analytics – for fundamental procedural rights. Second, it scrutinises the EU approach to AI-enabled crime analytics as crystallised in the final text of the EU AI Act. Third, it argues in favour of integrating socio-ethical and normative standards with technical design solutions, elucidating this intricate process through a 'matching exercise'. Finally, it informs a socio-ethical approach to AI-enabled crime analytics on the basis of bias detection and mitigation to address the (organisational) realities of automated law enforcement. By addressing the interplay between socio-ethical, legal, and technological standards, this chapter contributes to a holistic understanding of the implications and governance of AI-powered crime analytics, fostering a multi-disciplinary discourse at the crossroads of automation and law enforcement.

Chapter 6 navigates the intricate landscape of financial wrongdoing, presenting a comprehensive examination of how cutting-edge AI technologies empower and transform cross-border investigations. The chapter begins by laying the groundwork for understanding the evolving nature of financial crime in a globalised world. It then delves into the pivotal role that AI plays in enhancing the efficiency and effectiveness of investigative processes. Through the lens of real-world cases and practical examples, the authors demonstrate how AI tools, ranging from machine learning algorithms to advanced data analytics, revolutionise the identification, tracking, and prosecution of financial criminals across borders. Key themes include the utilisation of AI to decipher complex financial transactions, predict illicit activities, and analyse vast datasets for patterns indicative of fraud or money laundering. As governments, law enforcement agencies, and financial institutions grapple with the increasing sophistication of financial crimes, this chapter emerges as an indispensable guide for professionals and researchers seeking a nuanced understanding of the synergy between AI and cross-border investigations.

In Chapter 7, we contend that financial systems are being reshaped by the convergence of emerging technologies such as AI, Internet of Things (IoTs), blockchain, and decentralised finance (DeFi). This nexus unlocks the potential for automated smart contracts and peer-to-peer transactions. It also enables secure, efficient, and transparent financial services that fundamentally alter traditional financial systems. For example, blockchain forms the basis of DeFi to facilitate the creation of tokenised assets and digital currencies, which empowers users to engage in financial transactions without relying on intermediaries of the traditional

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

financial system – thus, enhancing transparency and reducing transaction costs. Despite these benefits, there are significant challenges associated with the dual use of these technologies along with DeFi, including issues concerning scalability, security, regulatory compliance, and interoperability with traditional financial architecture. There are potential risks, such as facilitation of illicit activities such as fraud, money laundering, and cyber extortion through anonymous platforms provided by DeFi. Thus, the dual use of these technologies and DeFi assets presents a new dawn of financial innovation and empowerment, whilst there are evolving challenges to address. This chapter presents an overview of the dual use landscape of these technologies and explores measures that can effectively navigate dynamic complexities to best exploit transformative benefits of this emerging ecosystem.

In Chapter 8, we posit that Financial Crime Risk Management (FCRM) is one of the top priorities of senior managers in the banking industry. The use of AI tools, products, and services by banks is on the rise. Using AI in FCRM is a natural progression in combating financial crime such as fraud detection. It also enables financial institutions such as banks to reduce costs as well as to improve customer satisfaction and their performance ratings with regulators, including the Financial Conduct Authority (FCA) and Competitions Market Authority (CMA). Current approaches to managing financial crime risk (FCR) may become outdated if banks do not align themselves with the opportunities that can be derived from the use of AI. Artificial intelligence already in use to combat fraud and other financial crimes in banks includes AI tools and products that have successfully mitigated against money laundering, blocked suspicious transactions and phishing emails, and managed sanctions risks, while strengthening Know Your Customer (KYC) processes.

The use cases of AI within banks, such as pattern recognition and data analysis as well as machine learning for predictive analysis, are explored further in this chapter. Despite the risks and vulnerabilities associated with the use of AI to counter financial crime such as algorithmic bias and data privacy, financial institutions and their employees have increasingly continued to use it. The voices of bank employees on the use of AI in their banks to fostering its responsible use are, therefore, included in this study, using empirical data gathered from three UK high street banks. Harnessing AI's power and promise responsibly will help in managing FCRs. This chapter, as such, offers novel ways in which stakeholders of banks can use the transformative power of AI in FCRM sustainably and responsibly, while promoting the principles of Fairness, Education, Accountability, and Transparency (FEAT).

Chapter 9 examines the integration of AI into due diligence (DD) processes within the Investment Migration (IM) sector, focusing on Citizenship by Investment (CBI) programmes. CBI programmes grant citizenship to qualified individuals in return for investment in a country's economy and are increasingly recognised as a significant source of foreign direct investment (FDI). However, concerns around misuse – such as money laundering and tax evasion – highlight the urgent need for robust DD frameworks.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

The chapter introduces a framework that leverages established AI technologies, including machine learning (ML) and Distributed Ledger Technology (DLT), to standardise DD procedures across specific CBI programmes. This framework draws heavily on historical CBI data, which often involves personal information held in private databases. As such, legal safeguards and policies must ensure that access to and processing of this data remain lawful and ethical. These processes must also be cross verified with independent, external data sources to meet DD requirements effectively.

A critical component of this AI integration is the development of 'legally explainable' AI, enabling transparency for stakeholders regarding how automated decisions and risk profiles are generated. Furthermore, mechanisms for auditing AI decision-making must be established to uphold transparency, accountability, and trust in CBI administration. By embedding AI in DD procedures, CBI programmes can significantly enhance operational integrity, efficiency, and resistance to abuse, ultimately strengthening their global legitimacy and their role in combatting financial crime.

Chapter 10 concludes the book, highlighting key conclusions, recommendations and prospects for law and policies on AI and law enforcement in the EU. The chapters in this book seek to bring together interdisciplinary research and empirical insights to examine how AI is reshaping the detection, investigation, and governance of financial crime across borders. The book also aims at addressing one of the most pressing challenges of the digital era: how to harness the power of AI responsibly and effectively in the fight against IMFs.

As financial, technological, and law enforcement systems become more interconnected and criminal tactics more complex, the insights offered in this book should be indispensable for shaping the future of law enforcement and financial regulation in the digital era. We invite readers to use this book to consider how AI can be used to fight financial crime and how it should be used – legally, transparently, ethically, and collaboratively.

REFERENCES

Adamyk, B., Turksen, U. and Benson, V. (2024) Dark side of decentralized finance: A call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, 32(1), pp.80–97.

African Union (2015) *High Level Panel on Illicit Financial Flows from Africa*. (online) https://au.int/sites/default/files/documents/40545-doc-IFFs_REPORT.pdf (Accessed 9 June 2025).

Bag, S. (2024) *The Use of AI in Arresting Financial Crime*. ORF Issue Brief No. 726. (online) Observer Research Foundation. https://www.orfonline.org/research/the-use-of-ai-in-arresting-financial-crime (Accessed 26 May 2025).

Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S. and Haslhofer, B. (2025) Mapping the DeFi crime landscape: an evidence-based picture. *Journal of Cybersecurity*, 11(1), tyae029, pp.1–19.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

Charniak, E. and McDermott, D. (1985) *Introduction to Artificial Intelligence*. Reading, MA: Addison-Wesley Longman Publishing Co.

Davenport, T. H. and Ronanki, R. (2018) Artificial Intelligence for the Real World. *Harvard Business Review*. https://hbr.org/2018/01/artificial-intelligence-for-the-real-world (Accessed 9 June 2025).

El Naqa, I. and Murphy, M. J. (2015) What Is Machine Learning? In: El Naqa, I., Li, R. and Murphy, M., eds. *Machine Learning in Radiation Oncology*. Cham: Springer.

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 (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (Accessed 9 June 2025).

Europol (2020a) *Europol launches the European Financial and Economic Crime Centre*. (online) www.europol.europa.eu/media-press/newsroom/news/europol-launches-european-financial-and-economic-crime-centre (Accessed 9 June 2025).

Europol (2016) *Does crime still pay? Criminal Asset Recovery in the EU*. www.europol.europa.eu/cms/sites/default/files/documents/criminal_asset_recovery_in_the_eu_web_version.pdf (Accessed 9 June 2025).

Gardner, H. (1999) *Intelligence Reframed: Multiple Intelligences for the 21st Century*. New York: Basic Books.

Global Financial Integrity (2025) *Illicit Financial Flows*. https://gfintegrity.org/issue/illicit-financial-flows/#:~:text=Illicit%20financial%20flows%20(IFFs)%20are,utilized%20across%20an%20international%20border (Accessed 9 June 2025).

Haring, W. and Zapf, D. (2025) Unsubstantiated suspicious transaction reports. *White & Chase*. www.whitecase.com/insight-alert/unsubstantiated-suspicious-transaction-reports (Accessed 9 June 2025).

Haugeland, J. (2000) *Artificial Intelligence: The Very Idea*. Cambridge, MA: MIT Press.

International Monetary Fund (2020) *What are illicit financial flows?* www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-illicit-financial-flows (Accessed 9 June 2025).

Joseph, J. and Turksen, U. (2022) Harnessing AI for due diligence in CBI Programmes: Legal and ethical challenges. *Journal of Ethics and Legal Technologies*, 4(2), pp.3–25.

Kelly, S., Kaye, S. A. and Oviedo-Trespalacios, O. (2023) What factors contribute to the acceptance of artificial intelligence? A systematic review. *Telematics and Informatics*, 77, p.101925.

Kurzweil, R. (1999) *The Age of Intelligent Machines*. Cambridge, MA: MIT Press.

Labadze, L., Grigolia, M. and Machaidze, L. (2023) Role of AI chatbots in education: Systematic literature review. *International Journal of Educational Technology in Higher Education*, 20(56), pp.1–17.

Mitchell, T. M. (1997) *Machine Learning*. New York: McGraw-Hill.

Norvig, P. and Russell, S. J. (2015) *Artificial Intelligence: A Modern Approach*. 3rd ed. Harlow: Pearson.

OECD (2014) *Illicit Financial Flows from Developing Countries: Measuring OECD Responses*. www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf (Accessed 9 June 2025).

Poole, D. L., Mackworth, A. K. and Goebel, R. (1998) *Computational Intelligence: A Logical Approach*. Oxford: Oxford University Press.

Ranchordas, S. (2021). Experimental Regulations for AI: Sandboxes for Morals and Mores. *University of Groningen Faculty of Law Research Paper*, 7/2021. https://ssrn.com/abstract=3839744 (Accessed 9 June 2025).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002

Paria, S., Qusay, M., Akramul, A., Bauer, G. and Bowles, I. (2023) A systematic review of using machine learning and natural language processing in smart policing. *Computers*, 12(2), p.255.

Sharma, R. (2021) Decentralized finance (DeFi) definition and use cases. *Investopedia*. www.investopedia.com/decentralized-finance-defi-5113835 (Accessed 9 June 2025).

UK Ministry of Defence (2018) *Human-Machine Teaming, Joint Concept Note 1/18*. (online) Available at: www.gov.uk/government/publications/human-machine-teaming-jcn-118 (Accessed 9 June 2025).

Van Camp, L. S. C., Sabbe, B. G. C., and Oldenburg, J. F. E. (2017) Cognitive insight: A systematic review. *Clinical Psychology Review*, 55, pp.12–24.

World Bank (2023) *Global GDP*. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (Accessed 9 June 2025).

World Bank (2017) *Illicit Financial Flows*. www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs#:~:text=It%20now%20generally%20refers%20to,corruption%2 C%20tax%20evasion)%3B%20or (Accessed 9 June 2025).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 10 Nov 2026 at 03:50:27, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.002