AI, Law and Ethics in Countering Financial Crime

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



CAMBRIDGE

https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 06 Nov 2026 at 07:25:07, subject to the Cambridge Core terms
https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4880003C39BD245

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

AI, LAW AND ETHICS IN COUNTERING FINANCIAL CRIME

Artificial intelligence (AI) is transforming the fight against financial crime, but how can it be deployed responsibly? In answer to that question, this book provides a comprehensive roadmap that integrates legal clarity, ethical guidance, and operational strategies on AI governance. Leveraging the EU's AI Act, national legal instruments and comparative insights, the book examines the challenges of AI governance and offers practical tools for bias mitigation, explainability, accountability, and risk management. The book's use of real-world case studies and contributions from academics and practitioners – including experts with law enforcement experience – enables scholars, students, and professionals in disciplines such as law, criminology, finance, and policing to bridge theory and practice. This makes it an indispensable resource for research, teaching, and professional training. Whether you are shaping policy, implementing compliance frameworks, or exploring AI's role in fighting financial crime, this book provides the roadmap you need to balance innovation and responsibility. This title is also available as open access on Cambridge Core.

Adam Abukari is an assistant professor in law at Coventry University.

Athina Sachoulidou is an assistant professor of criminal law at the Aristotle University of Thessaloniki (AUTH).

Dimitrios Kafteranis is an associate professor of law at the Centre for Resilient Business and Society, Coventry University.

Umut Turksen is Professor of Law at the University of Exeter.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

AI, Law and Ethics in Countering Financial Crime

Edited by

ADAM ABUKARI

Coventry University

ATHINA SACHOULIDOU

Aristotle University of Thessaloniki

DIMITRIOS KAFTERANIS

Coventry University

UMUT TURKSEN

University of Exeter

CAMBRIDGE UNIVERSITY PRESS

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781009623636

DOI: 10.1017/9781009623605

© Cambridge University Press & Assessment 2026

This publication is in copyright. Subject to statutory exception and to the provisions
of relevant collective licensing agreements, with the exception of the Creative Commons
version the link for which is provided below, no reproduction of any part may take
place without the written permission of Cambridge University Press & Assessment.

An online version of this work is published at doi.org/10.1017/9781009623605 under a Creative
Commons Open Access license CC-BY-NC 4.0 which permits re-use, distribution and reproduction
in any medium for non-commercial purposes providing appropriate credit to the original work is
given and any changes made are indicated. To view a copy of this license visit
https://creativecommons.org/licenses/by-nc/4.0

When citing this work, please include a reference to the DOI 10.1017/9781009623605

First published 2026

Cover image: Eye of an Eagle Owl, close up © Jonathan Knowles / Collection: Stone / Getty Images

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication Data
NAMES: Abukari, Adam editor | Sachoulidou, Athina, editor | Kafteranis, Dimitrios editor | Turksen, Umut editor
TITLE: AI, law and ethics in countering financial crime / edited by Adam Abukari, Coventry University; Athina Sachoulidou, Aristotle University, Thessaloniki; Dimitrios Kafteranis, Coventry University; Umut Turksen, University of Exeter.
OTHER TITLES: Artificial intelligence, law, and ethics in countering financial crime
DESCRIPTION: Cambridge, United Kingdom ; New York, NY : Cambridge University Press, 2026. | Includes bibliographical references and index.
IDENTIFIERS: LCCN 2026022179 | ISBN 9781009623636 hardback | ISBN 9781009623643 paperback | ISBN 9781009623605 ebook
SUBJECTS: LCSH: Artificial intelligence – Law and legislation – European Union countries | Artificial intelligence – Moral and ethical aspects – European Union countries | Commercial crimes – Law and legislation – European Union countries | Commercial crimes – Technological innovations – Law and legislation – European Union countries
Classification: LCC KJE959.5.C65 A45 2026
LC record available at https://lccn.loc.gov/2026022179

ISBN 978-1-009-62363-6 Hardback
ISBN 978-1-009-62364-3 Paperback

Cambridge University Press & Assessment has no responsibility for the persistence
or accuracy of URLs for external or third-party internet websites referred to in this
publication and does not guarantee that any content on such websites is, or will remain,
accurate or appropriate.

For EU product safety concerns, contact us at Calle de José Abascal, 56, 1°, 28003 Madrid, Spain, or email
eugpsr@cambridge.org

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Contents

List of Figures *page* viii
List of Tables ix
List of Contributors x
Preface xi
Acknowledgements xii

1 Introduction 1

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

1.1 Key Concepts and Definitions 1
1.2 Book Outline 5

2 Governing AI Internationally and Its Socio-legal Implications for Law Enforcement Processes 12

Alexander Murphy, Joshua Hughes, Anastasia Kordoni, and Reinhard Kreissl

2.1 Introduction 12
2.2 AI Regulation and Law Enforcement in the EU, the UK, China, and the USA 13
2.3 Comparative Overview of AI in Law Enforcement 21
2.4 Challenges and Concerns for Law Enforcement 26
2.5 Conclusion 27

3 Know Your Red Flags: Detecting Trends and Patterns in Financial Crime 33

Moran Harari, Dimitrios Kafteranis, Markus Meinzer, Lucas Millan-Narotzky, and Alison Schultz

3.1 Introduction 33
3.2 Literature Review and Contribution 34
3.3 Modelling Geographic Risk in Financial Transactions 40

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

3.4 Results 49
3.5 Conclusion and Policy Recommendations 49

4 **Use of AI in Law Enforcement: The Present and Future Prospects** 59
Joachim Klerx, Lukas Vilim, Stefan Hopf, Thea Sogenbits and Umut Turksen
4.1 Introduction 59
4.2 User Requirements 60
4.3 AI Applications and Tools in Policing 67
4.4 Safeguards in Policing with AI 78
4.5 Future Prospects and Emerging Trends 79
4.6 Recommendations and Conclusion 91

5 **The Interplay between Socio-Ethical, Legal and Technological Standards in Developing Automated Law Enforcement Systems: The Case of AI-Enabled Crime Analytics** 100
Anastasia Kordoni, Athina Sachoulidou and Cristina Rego de Oliveira
5.1 Introduction 100
5.2 The Impact of AI-Driven Crime Analytics Tools on Defence Rights 101
5.3 AI-Powered Crime Analytics Tools: The Normative Context 104
5.4 How to Merge Socio-ethical, Legal and Technical Standards: The Matching Exercise 106
5.5 Ethics and Fundamental Rights-by-Design: Identifying Bias Detection and Mitigation Measures for Fairer Outcomes 110
5.6 Conclusions and Recommendations 115

6 **Cross-Border Investigation of Financial Crime Empowered by AI** 121
Adam Abukari, Dimitrios Kafteranis, Stefan Hopf, and Thea Sogenbits
6.1 Introduction 121
6.2 Evolving Nature of Cross-Border Financial Crime and AI 122
6.3 Cross-Border Cooperation between LEAs in the EU 124
6.4 Technology as a Facilitator and Barrier to Cross-Border Cooperation 132
6.5 Conclusion 134

7 **Dual Use of Emerging Technologies and Decentralised Financial Assets** 139
Bogdan Adamyk and Vladlena Benson
7.1 Introduction 139
7.2 Conceptual Framework for Dual-Use Technologies in Finance 140

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

7.3 Technological Underpinnings: Blockchain, DeFi, AI, and IoT 142
7.4 Benefits of Integrating Emerging Technologies in DeFi 145
7.5 Dual-Use Risks: Illicit Exploitation of DeFi and Emerging Tech 148
7.6 Ethical and Regulatory Considerations 151
7.7 State-of-the-Art Developments and Current Initiatives 155
7.8 Future Outlook and Conclusion 158

8 **The Use of AI by Banks in Financial Crime Risk Management** 166
Adam Abukari, Julia Werberich, and Ololade Durodola
8.1 Introduction 166
8.2 Applications of AI in Financial Crime 169
8.3 Voices of Bank Employees on the Use of AI 173
8.4 Challenges and Opportunities of AI in FCRM 175
8.5 AI and FEAT in FCRM 179
8.6 Conclusion 181

9 **Leveraging Artificial Intelligence in Citizenship by Investment Programmes: A Framework for Minimum Due Diligence Standards to Counter Financial Crime** 189
Jeiel Joseph, Lucas Millan-Narotzky, and Umut Turksen
9.1 Introduction 189
9.2 Regulation of CBI 190
9.3 DD in CBI 192
9.4 Legality and Ethical Issues in the Use of AI 202
9.5 Operationalising AI in CBI DD 204
9.6 AI Facilitating Minimum DD Standards 208
9.7 Conclusion 208

10 **Conclusion** 214
Adam Abukari, Athina Sachoulidou, Dimitris Kafteranis, and Umut Turksen

Bibliography 217

Index 255

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Figures

3.1 Distribution of transaction volumes in the FinCEN leaks dataset. *page* 46
3.2 Risk contribution of different countries in the FinCEN files. 50
4.1 Work tasks requiring improved software solution. 65
4.2 User needs of 'non-users'. 66
4.3 User needs of 'frequent users'. 66
4.4 Example knowledge graph of Financing of Terrorism use case. 70
4.5 Ways of movements of illegal proceeds/fund. 74
4.6 Roadmap of future AI developments to counter financial crime. 80
6.1 Perceived barriers for information exchange and cooperation. 129

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Tables

2.1 Comparison of law enforcement AI regulations in the EU, UK, China, and USA as of April 2025 *page* 23
3.1 The twenty financial secrecy indicators underpinning the secrecy score 43
3.2 Priority ranking of STRs in the FinCEN files 51
4.1 Overview of quantitative sample 60
4.2 Overview of qualitative sample 62
4.3 Types of crime and IMFs 63
4.4 Frequency of digital or AI-based/supported investigation software usage 64
5.1 AIA compliance test (example) 109
6.1 Improvement of cooperation and information exchange 132
9.1 CBI DD process 195

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Contributors

Adam Abukari, Coventry University

Bogdan Adamyk, Aston University

Vladlena Benson, Aston University

Ololade Durodola, Coventry University

Moran Harari, Tax Justice Network

Stefan Hopf, VICESSE

Joshua Hughes, Trilateral Research

Jeiel Joseph, Coventry University

Dimitrios Kafteranis, Coventry University

Joachim Klerx, AIT

Anastasia Kordoni, Trilateral Research

Reinhard Kreissl, VICESSE

Markus Meinzer, TJN

Lucas Millan-Narotzky, TJN

Alexander Murphy, Trilateral Research

Cristina Rego de Oliveira, Mackenzie Presbyterian University

Athina Sachoulidou, Aristotle University of Thessaloniki

Alison Schultz, Tax Justice Network

Thea Sogenbits, ETCB

Umut Turksen, University of Exeter

Lukas Vilim, CNCA

Julia Werberich, PLMJ

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Preface

This edited volume is the result of years of collaborative research and innovation involving a broad network of experts across Europe. Scholars, practitioners and end-user stakeholders from diverse backgrounds have come together to address a critical challenge of our time: the role of artificial intelligence (AI) in combating financial crime and money laundering.

Grounded in real-world engagement, the book explores how AI tools, particularly within decentralised finance (DeFi), blockchain and law enforcement can both facilitate criminal activity and strengthen regulatory oversight. It examines the ethical, legal and institutional implications of AI, especially its impact on fundamental rights such as privacy and due process.

Advocating for context-aware regulation, transparency and international cooperation, the volume proposes innovative, proactive frameworks for anti-money laundering (AML). More than a collection of analyses, it offers a roadmap for responsible innovation and collaborative governance, urging stakeholders to actively shape AI's role in financial integrity and democratic resilience.

We hope it will inspire continued dialogue, critical engagement and meaningful action in the pursuit of ethical and effective AI-driven financial governance and countering financial crime.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Acknowledgements

This book would not have been possible without the generous financial support of the European Union and the steadfast guidance of Dr Elina Manova, our project officer at the EU Research Executive Agency. Her support was instrumental throughout the duration of the TRACE Project.

The substantive research, along with its findings, insights and proposed solutions, is the result of the dedicated efforts of the TRACE Project Consortium. Their commitment and collaboration were vital to the success of this work.

We are deeply grateful to our Advisory Board, whose invaluable experience and expertise in Horizon 2020 projects, artificial intelligence, ethics and law enforcement provided essential direction and insight at every stage.

The face-to-face events, workshops, seminars, webinars and conferences that informed our findings were made possible thanks to the generosity of hundreds of law enforcement and judicial officers from over twenty-five countries across Europe and beyond. We also extend our sincere thanks to policymakers, academics and professionals from the legal and financial sectors worldwide, whose contributions enriched our research.

We would like to express our appreciation to Europol's Innovation Centre and the European Commission DG Home, who – despite their many pressing priorities – provided us with opportunities to present and test our solutions.

Our thanks also go to the following organisations for their collaboration and support: Inland Revenue Service (CI), USA; University of Luxembourg; National Organised Crime Agency – Czech Republic; Hellenic Police – Greece; Research Institute for Transparency, Corruption and Financial Crime – Aristotle University of Thessaloniki – Greece; and Polícia Judiciária (PJ) – Portugal.

We gratefully acknowledge the following individuals for offering a wide spectrum of views on the issues explored in this book: Dr Daniel Frendo, Financial Intelligence Analysis Unit, Malta; Jan Ellerman, Europol; and Madison Leeson, RITHM Project.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

We also extend our sincere thanks to our visiting fellow, Dr Huseyin Unozkan (Mudanya University) and Lt. Col. Dr. Engin Erken (Gendarmerie General Command, Türkiye) for their valuable input.

Finally, a heartfelt thanks goes to our colleagues at the Centre for Resilient Business and Society (CRBS) and the Research Support Team at Coventry University. Their collaboration and encouragement have been a cornerstone of this work.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

2

Governing AI Internationally and Its Socio-legal Implications for Law Enforcement Processes

Alexander Murphy, Joshua Hughes, Anastasia Kordoni, and Reinhard Kreissl

2.1 INTRODUCTION

As artificial intelligence (AI) evolves at an unprecedented pace, the need for effective governance has emerged as a global imperative. This has become particularly pertinent in four legislative orders, the European Union (EU), the United Kingdom (UK), China, and the United States of America (USA); each embodying distinct regulatory philosophies rooted in divergent socio-political values and priorities. These territories are key loci for AI development and leadership, as legal orders across the entire world begin to grapple with the challenges of AI. The regulation of AI is especially critical in the domain of law enforcement, where a complex institutional landscape is increasingly interwoven with data-driven processes (Kreissl and von Laufenberg, 2022). Across jurisdictions, law enforcement practices typically centre on suspect identification, future threat assessment, resource allocation, and crime prevention. These aims interconnect a wide range of actors, from forensic specialists and street officers to financial crime investigators and community-based responders, whose work increasingly relies on AI-enabled tools and digital data processing. These practices and actor collaborations reflect a sociotechnical policing system, wherein global AI regulations intersect with organisational routines and structures.

Understanding these developments necessitates an interdisciplinary lens on how regulatory approaches not only reflect geopolitical priorities but also shape justice in digitalised societies. This chapter introduces initial relevant AI regulatory frameworks in the EU, UK, China, and the USA as of April 2025, and their implications for AI-enabled law enforcement tools (Section 2.2). It provides a comparative analysis of nascent regulatory approaches towards the controversial law enforcement solutions of predictive policing, generative AI, facial recognition, and biometrics with a focus on risk and transparency (Section 2.3) and explores the operational challenges to investigative work that impact on law enforcement practices internationally (Section 2.4).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

2.2 AI REGULATION AND LAW ENFORCEMENT IN THE EU, THE UK, CHINA, AND THE USA

2.2.1 *The EU and UK*

The EU is engaged in a comprehensive effort to regulate impactful technologies, covering personal data, AI, digital services, and digital markets. Its approach takes into account both a commitment to safeguarding fundamental rights as well as the promotion of its internal market. Its efforts have global influence, with data protection regulation as far away as Brazil and California taking inspiration from EU legislation. This demonstrates the EU's capacity to shape international regulatory norms through the extraterritorial impact of its legal standards, the so-called Brussels effect. In contrast, the UK, whilst broadly retaining EU law in relation to data protection following its departure from the EU, has pursued a more flexible, innovation-oriented regulatory model that delegates rule-making authority to sector-specific regulators in relation to AI. Whilst the EU emphasises legal certainty and uniformity across the Union, the UK is taking a different path creating different impacts, including for law enforcement.

Regulation of AI systems for law enforcement use in the EU is primarily shaped by Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, or, as it is more commonly known, the EU AI Act (AIA), which is designed to regulate technological issues, especially those presented by AI and complement the existing data protection legislation (Nash *et al.*, 2024); in the case of processing by police, the Law Enforcement Directive (LED) where processing of personal data is for the 'prevention, investigation, detection or prosecution of criminal offences' (Article 1(1), LED). Both pieces of legislation take a risk-based approach. As with the General Data Protection Regulation (GDPR), the LED requires a higher standard of compliance for those processing special category personal data or engaging in high-risk processing (Article 9, GDPR; Article 10, LED). The AIA prohibits systems deemed to present unacceptable risk (Article 5, AIA) and requires conformity assessments of systems presenting high risks (Chapter III, Section 2, AIA).

For law enforcement-related activities, the following are prohibited: the use of AI to predict the risk of criminal offences based solely on personality traits/characteristics without human intervention; untargeted scraping of facial images for facial recognition databases; and real-time biometric identification in public spaces (unless for searching for victims of specified crimes or missing persons, preventing an imminent threat to life or terrorist attack, or localising a suspect for law enforcement purposes) (Article 5, AIA). Under national laws implementing the LED, EU Member States are required to prohibit automated decision-making creating adverse legal effects (unless there are appropriate safeguards provided (Article 11, LED)).

High-risk AI systems in the law enforcement area are specified as: AI systems for assessing the risk of someone becoming a victim of crime; polygraphs or similar

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

tools; AI systems for evaluating the reliability of evidence; AI systems for assessing the risk of (re-)offending not solely on the basis of profiling, or to assess personality traits and characteristics or past criminal behaviour; AI systems for profiling in the course of detecting, investigating, or prosecuting crimes (Annex III (6), AIA). Under the LED, high-risk data processing would require a data protection impact assessment to be conducted (Article 27, LED).

The preambles of both pieces of legislation indicate that they are fundamentally intended to protect people, and their data, from harm whilst enabling commercial gains from AI to be seized. Almeda *et al.* (2021) note that citizens expect the use of policing technologies to be different according to what is acceptable in different situations. An example of this is seen in the AI Act where real-time remote biometric identification systems are prohibited except in certain circumstances (Article 5, AIA). Yet, as Lynskey (2019) notes in relation to data protection legislation, some of the protections can be more illusory than real. As law enforcement interacts with the public in ways that interact with their rights regularly, particular attention should be paid to law enforcement use of AI. This is especially the case where innocent people suspected of a crime could be subject to serious and significant impacts whilst having done nothing wrong.

It is worth noting that the AIA will have effects beyond the EU, including in the UK, for several reasons. First, the AIA has extraterritorial effect (Article 2, AIA) and where, for example, UK police use an AI system in a cross-border investigation and outputs are used within the EU, or there are persons affected by that use of an AI system within the EU, then that use of AI would come under the AIA. Further, the European Committees for Standardisation (CEN) and for Electrotechnical Standardisation (CENELEC) have accepted a request from the European Commission to develop standards supporting the implementation of the AIA. The British Standards Institution remains a member of CEN-CENELEC, and so compliance with the AIA will be integrated into British standards for AI systems (CEN-CENELEC, 2025). Finally, because of Brexit, Northern Ireland is subject to some EU rules under the Windsor Framework. The EU could propose the AIA applies in Northern Ireland (Article 13(4), European Union and United Kingdom, 2019). If the UK government agreed to this, then the Police Service of Northern Ireland would be subject to the AIA in its operations.

In contrast to the EU, the UK is prioritising innovation in its approach to AI regulation. Rather than risk-based legislation with specific requirements for different sectors, the UK has developed a principles-based framework that will inform legal compliance across sectors (Department for Science, Innovation and Technology, 2024, para.10). Instead of developing UK AI legislation, the UK's ninety regulators such as the Information Commissioner's Office, Ofcom, and the Financial Conduct Authority will be able to provide guidance on AI use within their areas of oversight, with central functions for risk monitoring, coordination, and multi-agency advisory services (Department for Science, Innovation and Technology, 2024, paras.16, 19).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

As Finocchario (2024) notes, a sectoral approach has advantages in being able to respond to sector-specific issues and avoid unnecessarily onerous bureaucracy in lower-risk contexts. However, the UK government has been clear that, in relation to general purpose AI models, where compliance with voluntary measures is ineffective or existing legal powers are unsuccessful in dealing with risks and opportunities, targeted legislation could be introduced. For highly capable narrow AI and Agentic AI, the UK government will continue to monitor developments (Department for Science, Innovation and Technology, 2024, paras. 65–67).

With respect to law enforcement, the UK government has praised the Chief Scientific Advisor for Policing's Covenant for Using AI in Policing. This provides principles for AI users in law enforcement that operationalise them to the UK policing context; for example, the transparency principles show that manufacturers might be required to provide expert evidence in open court (National Police Chiefs' Council, 2023). However, as the GDPR and LED were brought into UK law prior to Brexit, policing in the UK is subject to substantially the same rules under Part 3 of the Data Protection Act 2018 as EU Member States are in their implementations of the LED. As such, whilst there is no substantive AI legislation covering law enforcement, or any sector, there are relevant data protection provisions that still apply.

2.2.2 *China*

China has implemented a range of regulations and policies to govern the use of AI, particularly in sensitive domains such as national security and public safety (Roberts *et al*., 2021). These regulatory frameworks serve China's endeavours both domestically and internationally. Domestically, these regulations address ethical and security concerns, through mechanisms such as algorithm audits and content moderation (Lucero, 2019). Internationally, these regulations aim to position China as a global leader in AI technology, not only in its development and deployment but also in AI governance, establishing regulatory precedents for other nations (Dorwart *et al*., 2025).

China's AI regulatory framework is structured on three key pillars. First, existing regulations target specific applications or manifestations of AI technology, such as recommendation algorithms, deep synthesis, and generative AI. The Regulations on the Management of Algorithm Recommendations for Internet Information Services, enacted in March 2022, govern platforms that use recommendation algorithms, such as the social media whose data is often used for investigative purposes. They require algorithm providers to ensure that content aligns with 'mainstream value orientations' while preventing the dissemination of politically undesirable content (Sheehan, 2023). The Administrative Provisions on Deep Synthesis, effective January 2023, target AI-generated synthetic content, including deepfakes, and voice cloning. They mandate that AI-generated content be clearly labelled to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

distinguish it from non-AI content, that providers take steps to mitigate misuse, and enforce measures to ensure AI-generated material adheres to government policies.

In response to the rise of generative AI technologies, China further introduced the Interim Measures for the Management of Generative AI in August 2023 (China Law Translate, 2023). These regulations aim to provide a balance between innovation and security (Article 3) and mandate that generative AI services undergo ex ante security assessments, making China the first country to impose a licensing requirement for such technologies (Zhang, 2024). Concurrently, the regulations impose data privacy protections to regulate the collection and use of training data in AI systems, prevent the creation of discrimination (Article 4, paragraph 2), and safeguard physical and psychological well-being (Article 4, paragraph 4).

Although China has yet to implement AI-specific administrative regulations, two major laws – the Network Data Security Regulation (effective from 1 January 2025) and the Online Protection of Minors Regulation (effective since 1 January 2024) – address key AI-related issues such as data privacy, algorithmic discrimination, cybersecurity, and content moderation. To supplement these overarching frameworks, China adopts a technology-contextual regulatory approach through laws that target specific sectors including finance, biometrics, and autonomous driving to facilitate more adaptive oversight of AI applications (Wang *et al.*, 2025).

In its second pillar, the government has established specialised regulatory tools, such as algorithm filing requirements and security self-assessments, to monitor AI systems (Dorwart *et al.*, 2025). Similar to the algorithm recommendation regulation, deep synthesis and generative AI providers are required to register their products by filing the algorithm with the Cyberspace Administration of China (CAC). The algorithm filing requires a wide range of documents and other information, including basic information for the filing entity, security self-assessments, algorithm mechanism review, technology ethics review, information release review, data security, personal information protection, and emergency response (Dorwart *et al.*, 2025). The CAC periodically publishes a list of filed algorithms, but the announcement includes only limited details, such as the name of the algorithm, its intended area of use and primary function, the filing number, and the filing entity. China's AI filing process appears to address not only the technical and operational dimensions of AI, but also its broader societal implications (Mao and Shi-Kupfer, 2021).

Third, China employs an iterative legislative approach, allowing regulators to refine existing policies in response to emerging AI-related challenges (Zhang, 2024). For example, the Model AI Law (MAIL) proposed by the Chinese Academy of Social Sciences presents an adaptable governance framework for AI in China. It emphasises core values, such as safety, transparency, fairness, and human oversight, and adopts a risk-based 'negative list' approach, which imposes strict controls on high-risk AI activities while enabling low-risk innovations to proceed with minimal regulatory interference, aiming to strike a balance between effective oversight and technological development.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

In preparing to introduce its Artificial Intelligence Law (Scholarly Draft Proposal), China is expected to unify AI governance under a single regulatory framework. While the details are still under discussion at the time of writing, the draft law proposes a broader definition of AI as 'technology that utilises computers to simulate human intelligent behaviour for use in prediction, recommendation, decision-making, or content generation, among other specialised or general purposes' (Article 97). By embracing a more open definition and promoting international cooperation, while ensuring foreign AI services comply with domestic rules (Lucero, 2019), the law seeks to regulate key elements of AI development (e.g. transparency, explainability, intellectual property), safeguard user rights (e.g. fairness), and define developer obligations (e.g. liability, security). It also supports digital literacy, green development, and includes exemptions for scientific research and open-source AI. The draft replaces the negative list with a notification-based system, allowing AI development without pre-approval. Compliance is required only once AI is classified as 'critical', promoting early innovation while maintaining safety and accountability through targeted oversight at later stages.

This multi-tiered regulatory structure has significant implications for law enforcement and public security. Prior to the draft AI law, China developed targeted measures for the use of AI in law enforcement, such as the Measures for the Administration of Public Security Organs' Use of Facial Recognition Technology, which set rules for the collection, storage, and use of facial recognition data, directly impacting the use of AI in policing (Roberts *et al.*, 2021). The 2025 National Security Law further extends provisions affecting the use of AI technologies for national security and public safety. Sector-specific regulations, such as those governing autonomous driving, facial recognition, and genomic research may also influence the use of AI by law enforcement agencies. The draft AI law complements these existing regulations in two ways. First, the definition of AI in the law suggests that crime analytics and relevant AI-enabled law enforcement tools may be included. Second, Article 81 of the draft law explicitly refers to combating crime, emphasising international cooperation in law enforcement and justice, and preventing the misuse of AI technology by terrorist, extremist, and transnational organised crime groups.

This evidence indicates convergence between the AIA and China's proposed AI regulations in terms of ethical principles and human-centric governance. While interpretations of these principles may differ in each jurisdiction, they both emphasise fairness, transparency, and the protection of individual rights, integrating data protection frameworks into AI oversight. Each regime also mandates security measures, such as audits, vulnerability assessments, and human oversight, adopts a joint AI standards model (Wang *et al.*, 2025), and addresses cross-border cooperation for combating AI-related crimes and AI-enabled law enforcement. Although the EU adopts a horizontal, risk-based legal framework, China employs a risk-informed

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

approach grounded in administrative guidance. Chinese classifications include prohibited practices and assessments of public opinion impact and social mobilisation capacity. Unlike the EU's legally binding structure, China's legal framework consists of non-binding best practices and strategic documents, such as the Ministry of Science and Technology's code of practice for AI ethics.

2.2.3 *The USA*

The USA is a global centre of technological innovation, but its moves towards AI regulation have been inconsistent and the prospect of comprehensive national legislation is remote. Consequently, substantial AI policy efforts in the USA have chiefly taken place at the executive and state level. Within Congress, debates on development rules, institutional roles, the funding of research, and the enticement of expertise have accompanied the rising public profile of AI in recent years, with patches of bipartisan agreement on issues such as precluding AI from nuclear warfare decisions (Matthews, 2023). A lack of consensus has nonetheless stymied broader efforts, with pitches such as the Algorithmic Accountability Act (Gongress.Gov, 2023) languishing at committee stage prior to the disruption of administrative turnover. White & Case (2024) stated in December 2024 that 120 bills focused on AI, machine learning, or related issues were under congressional consideration as of the close of that session, when their prospects of passing will have diminished.

A handful of American federal legislation has passed. The most significant is the 2020 National Artificial Intelligence Initiative Act, which coordinated and assigned AI oversight and development throughout federal agencies. This involved the commission of studies, programmes, and committees through bodies like the National Science and Technology Council and Department of Energy, as well as the establishment of a National AI Initiative Office. A similar emphasis is evident in the 2020 AI in Government Act, which mandated the creation of an AI Center of Excellence within the General Services Administration to drive adoption across government. Acknowledgements of the potential of AI for defence and aviation applications were entrenched in the National Defense Authorization Act for Fiscal Year 2019 and the 2024 Federal Aviation Administration Reauthorization Act, respectively, both of which called for reviews of prospective AI opportunities. Also of note is the 2022 CHIPS and Science Act, which aimed to bolster US semiconductor production, science investment, data centre technologies, and AI expertise with around 280 billion USD in new funding (Taylor, 2023), championing American global AI competitiveness (Stanford University Human-Centred Artificial Intelligence, 2022). A final congressional signal came in the closing days of the Biden Administration, when the bipartisan House Task Force on Artificial Intelligence (2024) issued a report on the principles that should underpin further national legislation. Its sixty-six key findings and eighty-five recommendations include seven foundational principles: identify AI issue novelty; promote AI

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

innovation; protect against AI risks and harms; empower government with AI; affirm the use of a sectoral regulatory structure; take an incremental approach; keep humans at the centre of AI policy. These principles tend to prioritise the empowerment of innovation and industry, in a way that is consistent across a piecemeal American regulatory landscape.

Executive Orders (EOs) permit US presidents to redirect the executive branch by fiat, circumventing congressional gridlock to enact change at the price of a volatile federal picture. Donald Trump's 2019 EO on 'Maintaining American Leadership in Artificial Intelligence' proposed five principles, centred around American leadership on technology development, technical standards, workforce training, public trust, and the international promotion of American AI (Executive Office of the President, 2019). Following this, Joe Biden signed an EO on the 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' in 2023, which constitutes the most comprehensive AI regulations advanced in the USA and outlined the administration's stance (Executive Office of the President, 2023). The Order codified earlier guidelines, demanding transparency from AI companies and a raft of standards and measures such as the need to watermark AI-generated content (Ryan-Mosley and Heikkilä, 2023). The Order tasked the National Institute of Standards and Technology to set standards for the testing of accuracy and bias in AI systems but opted for voluntary compliance rather than mandatory adherence. Federal agencies were again directed to develop structures to harness AI, and to safeguard workers' rights, civil rights, and consumer privacy, while the Trump Order's calls for global leadership and skills development are reinforced. A returning President Trump revoked the Biden Order, although he spared another relevant Biden EO on AI data centres and energy infrastructure (Shepardson, 2025) and one driving the use of AI for the purposes of 'Strengthening and Promoting Innovation in the Nation's Cybersecurity' (Executive Office of the President, 2025).

Trump's replacement EO ('Removing Barriers to American Leadership in Artificial Intelligence') comprehensively undoes its predecessor, tasking federal bodies to review any actions taken downstream of Biden's EO, but is sparse in its own right. It advocates leadership, security, and innovation in general terms, and decries 'ideological bias or engineered social agendas'. A pair of Office of Management and Budget memoranda in April 2025 set guidelines for the implementation of the Trump EO throughout executive agencies, making it somewhat more concrete (Nandivada and Haan, 2025). This effective abolition of federal guidance has created concerns about data harvesting, surveillance, cybersecurity, and bias; ethical and regulatory considerations on which the US has effectively ceded influence to its global competitors (Kimery, 2025). The AI Risk Management Framework issued by the National Institute of Standards and Technology (2023) may be of use to wary developers, with an overview of risks and principles (such as transparency and explainability) that would be recognisable to EU regulators.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Space does not permit a full overview of regulation at the US state level, with more than forty states having introduced AI bills since 2023 (White & Case, 2024); indicating the fractured regulatory landscape that characterises the US model. The first expansive AI legislation (SB24-205 Consumer Protections for Artificial Intelligence) came from Colorado in May 2024, with an emphasis on consumer protections and algorithmic discrimination from the date of its enactment in February 2026 (Colorado General Assembly, 2024). The bill requires impact assessment and risk management from developers, incentivising adherence as a presumptive rebuttal to future legal challenges, and mandates transparency and human appeal processes ('if technically feasible') to protect consumer rights (Colorado General Assembly, 2024). The bill is the first US measure to directly target high-risk AIs and, with a start date ahead of the AIA's full implementation, it is arguably the first comprehensive AI regulation in the world (Rice, Lamont, and Francis, 2024). The California model has been more sectoral but is of particular interest given California's dominance of tech industries. Assembly bills have targeted deepfake generation, the mimicking of deceased figures' voices or appearances without the permission of their estates, the need to label AI content in healthcare settings or on large online platforms, and the need for 'high-level' transparency over training data sets (White & Case, 2024). A wider bill, the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (California Legislative Information, 2024), was passed by the state legislature in late 2024 but subsequently vetoed by Governor Gavin Newsom, sparing leading tech companies from an array of requirements focused on the most dangerous AI prognostications (Loring and Lee, 2024). Elsewhere, the consumer protections and disclosure model of Utah's S.B. 149 Artificial Intelligence Amendments (Utah State Legislature, 2024), the rigid risk restrictions proposed in the Texas Responsible AI Governance Act (TRAIGA), and New York's early efforts to prevent discriminatory AI hiring processes (Ryan-Mosley, 2023) typify the plurality of American AI regulation at the state level.

This diversity is replicated across the law enforcement landscape, where the capacity of AI to assist and expand (or replace) human processes has been embraced by American policing (Ezeh, Widgery, and Canada, 2025). AI use cases have involved the automation of investigative processes, such as speech or facial recognition, anonymisation and redaction, as well as predictive policing and real-time biometrics (of the types expressly proscribed by the EU) (Congressional Research Service, 2023). Concerns over the ethics, privacy, and reliability of these tools, in applications from report writing (Ferguson, 2024; Lewis, 2024; Almeida, Shmarko, and Lomas, 2022) to gunshot detection (Joh, 2024), are prevalent but the direction of travel is clear. The US Department of Justice (2024) outlines AI innovations across surveillance and identification, forensics, predictive policing and risk assessment, and recommends cautious, targeted use, while the US Department of Homeland Security (2024) AI Roadmap lauds technical advances to flag suspicious vehicles at borders, identify the victims of sexual exploitation, or streamline emergency

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

response and airline security processes. The DHS (2024) AI Use Case Inventory lists 199 tools as of its July 2025 update. Across the US law enforcement spectrum, investigators are routinely assisted via generative text efficiencies, virtual assistants to streamline analysis, virtual reality training techniques, case prioritisation and management tools, and rapid data analysis (US Treasury Department, 2024). In the American regulatory landscape, AI-enabled law enforcement tools do not require additional or mandatory oversight. This absence of explicit scrutiny distinguishes the USA from the EU, UK, and China, where regulatory frameworks are evolving to address the specific risks posed by such technologies.

2.3 COMPARATIVE OVERVIEW OF AI IN LAW ENFORCEMENT

This section provides a comparative overview of the regulatory frameworks and practical approaches to AI deployment in law enforcement across the EU, UK, China, and the USA, using three contentious applications – generative AI, predictive policing, and facial recognition with real-time biometrics – as illustrative case studies.

Generative AI refers to systems capable of autonomously producing new content, such as text, images, music, code, and video, by analysing large datasets and identifying underlying patterns (Farber and Vyas, 2025; Madiega, 2023). Generative AI is increasingly applied in law enforcement, supporting digital forensics by reconstructing crime scenes, generating chronological incident reports and providing insights into communication patterns in criminal investigations, for example (Nikolakopoulos *et al.*, 2024; Sakshi and Wadhwa, 2023). It can reconstruct missing or altered evidence (Zhao *et al.*, 2021), and improve digital evidence evaluation, language interpretation, and forensic linguistics, which, in turn, facilitates conceptual comprehension and criminal network analysis (Emehin *et al.*, 2024). In financial fraud investigations, it enables near-instantaneous anomaly detection and flagging, predictive modelling, and fraud prevention through advanced data analytics (Emehin *et al.*, 2024). Generative AI can assist in drafting primary documents for international police cooperation, translating reports, prioritising cases (Meijer and Wessels, 2019), and developing public communication tools (Dubravova *et al.*, 2024). It can create realistic simulations for training purposes, including cyberattack scenarios (Emehin *et al.*, 2024), but also present security challenges. It can be exploited for evidence fabrication, deepfake creation, cyberattacks, and data forgery, which led to the emergence of 'Generative AI-led Crime as a Service' (CaaS) (Matejic and Wilson, 2024). This involves deceptive and coercive tactics, introducing new criminal threats to policing.

Predictive policing is the term for using statistical patterns and software to anticipate offending, and thus guide police decision-making and resource allocation (Meijer and Wessels, 2019). This is based on the assumption that crime events can be predicted from the analysis of historical data about crime, augmented with information from other sources. Recognition of temporal and spatial pattern of

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

crime, based on algorithms, trained with large data sets, including police documents, is the underlying technology here. These technologies have been treated with scepticism, with recent scholarship suggesting that much more evidence is needed of the efficacy of big data analytical algorithms; despite their administrative allure for governments and LEAs (Almasoud and Idowu, 2024; Lee, Bradford, and Posch, 2024). Even where predictive policing models are effective, concerns around the replication of biased policing patterns, their misleading aura of objectivity, and legitimacy considerations endure (Pearsall, 2010). The campaign group Liberty (2019) differentiates predictive policing into mapping programmes, where areas are monitored based on historic crime, and individual risk assessments, where the prospect of offending or victimisation at the personal level is assessed. They express ethical concerns about the data quality, human error, discrimination, and obscurantism of these systems for the public and LEAs employing them.

Facial recognition technology (FRT) and real-time biometrics present a novel change for police and their ability to evaluate those they encounter. Previously, an individual officer needed to recognise and remember information about a person of interest, probably because they had interacted with them as part of their specialist investigatory area (e.g. an officer investigating drug crime may know local dealers). Now, however, such information could be available to all police officers in a jurisdiction for a variety of different reasons, presenting a change in how police interact with the public.

There are obvious utilities for such systems in locating wanted criminals, but also clear privacy and ethical concerns. As people are unable to easily opt out of their data being captured, control of personal data falls to the data controllers, most likely the police. Where such tools are used legitimately and lawfully, this still allows for police to know much more about individuals than they would otherwise do. This could not only feel invasive but can also lead to self-censorship where people feel they are being watched (Penney, 2022). Where safeguards are missing or inadequate, there is a plain risk of mass surveillance. Additionally, facial recognition and biometric analysis tools have been demonstrated to be less accurate when recognising people from ethnic minority backgrounds (Leslie, 2020). As such, whilst these tools can be presented as functioning in a particular way, the actual results are often very different (Raji *et al.*, 2022). Table 2.1 presents the applicable regulations for each case study per country, with key context on their stances towards AI in policing.

The analysis suggests that AI governance is deeply contextual, shaped by the distinct epistemic, political, and cultural infrastructures of each jurisdiction. That is, differences in political and power dynamics, socio-cultural environments and organisational structures dynamically determine how ethical principles are interpreted and embedded within AI regulatory frameworks for law enforcement, and more broadly. The EU's emphasis on human rights and risk mitigation is evident in its AIA, underpinning a precautionary regulatory approach through its tiered, risk-based AI deployment for critical domains such as policing. The US approach is

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 2.1 *Comparison of law enforcement AI regulations in the EU, UK, China, and USA as of April 2025*

AI use case	EU	UK	China	USA
Generative AI	Generative AI could be considered as 'general purpose AI model' under Article 51 of the AIA and could potentially pose 'systemic risk' under Article 52. Potentially high-risk under Annex III (6) where used in certain risk assessments, lie detection, evidence evaluation, profiling.	No specific legislation. Generative AI could be a target for future legislation where it meets the standard of 'General Purpose AI'.	Key regulations include the Interim Measures for the Management of Generative Artificial Intelligence Services (with exemptions for scientific research and industrial applications), Cybersecurity Law, Data Security Law, Personal Information Protection Law, Regulations on the Management of Deep Synthesis of Internet Information Services, and the Draft AI Law. Generative AI is used by LEAs processing big data and conducting semantic analysis to collect case elements for online fraud (e.g. financial and telecommunication).	No federal regulation. In widespread and growing use across American LEAs, e.g. for writing reports or analysing unstructured data.

TABLE 2.1 *(continued)*

AI use case	EU	UK	China	USA
Predictive policing	Potentially prohibited under Article 5(1)(c) where evaluation of social behaviour leads to detrimental or unfavourable treatment for a group of persons. Potentially prohibited under Article 5(1)(d) where fully automated risk assessments only use profiles, personality traits, or characteristics.	No specific regulation. Predictive policing tools are stated by Amnesty (2025) to have been deployed by 33 UK police forces, or almost three quarters, raising concerns around bias and due process.	No specific regulation, only related projects (e.g. drug-related crimes, telecommunication fraud, terrorism).	No federal regulation. Police in Los Angeles and Chicago were among early adopters of tools to identify high-risk offenders, with Operation LASER and the Strategic Subjects List respectively (Thomas, 2024). Both programmes have since been discontinued, and debates around bias and effectiveness led Santa Cruz in California to be the first city to ban predictive policing tools in 2020. Police in several states continue to use predictive policing tools to identify offences, perpetrators and victims – with varying degrees of success (Thomas, 2024).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Facial recognition and real-time biometrics	Potentially prohibited under Article 5(1)(e) where untargeted scraping of facial images is used to expand databases. Potentially prohibited under Article 5(1)(g) where systems categorise people based on biometric data and then infer further sensitive data about them. Potentially prohibited under Article 5(1)(h) where real-time biometric identification systems are used in public spaces without an exemption (other specific requirements are present in Article 5(2)–(7)). Otherwise considered high-risk under Annex III (1).	No specific regulation. However, following *R (Bridges) v Chief Constable of South Wales*, a new Surveillance Camera Code of Practice came into force in 2022.	Security Management Measures for the Application of Facial Recognition Technology (with exemptions for research or algorithm training purposes). Potential processing of facial information/biometric data to identify offenders, known criminals and detect disturbances.	No federal regulation. Adoption has been uneven, with cities such as San Franciso and Boston banning facial recognition while Florida, for example, routinely uses its Facial Recognition Network to identify detainees based off its database of millions of citizens culled from driver records. There is little algorithmic training transparency on FRT used at scale by US LEAs (in some cases leading to large fines and restrictions). At the end of 2025, 15 US states had limitations on police use of facial recognition technology (Laperruque, 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C04884E80003C398D145

more fragmented, favouring innovation and private sector leadership in the absence of centralised oversight of the deployment of AI-enabled law enforcement solutions – with the UK erring towards this model. By contrast, China's governance model is positioned to develop regulatory approaches that are anticipatory and centralised, aligning AI regulation with state-led objectives that prioritise technological advancement for social governance and economic competitiveness. These variations are reflected in the ethical discourse and, therefore, decision-making in relation to the use of AI-enabled law enforcement tools. While the EU conceptualises ethics as a legally binding moral imperative, China integrates ethical considerations within a broader state governance narrative, and the US approaches ethics as a decentralised and often negotiable set of values mediated by industry and civil society. Addressing the challenges of AI law enforcement tools should be sensitive to these contextual factors, which determine the interpretative repertoire of international regulatory frameworks.

2.4 CHALLENGES AND CONCERNS FOR LAW ENFORCEMENT

The governance approaches in the EU, US, UK, and China establish distinct normative baselines that frame the permissible scope of AI use in policing, the thresholds for accountability, and the weight given to civil liberties versus public order. These contextualised ethical-legal ecosystems form the backdrop against which specific operational concerns emerge. For example, there is a considerable body of research on the detrimental effects and threats related to datafied, algorithmic models of social analysis and their implementation by state and private (corporate) actors (see, for instance, Crawford, 2021; Eubanks, 2018; O'Neil, 2017; Wiggins and Jones, 2023). Some of these criticisms, when seen through the lens of law enforcement, take on very specific shape and are intertwined with regulatory and ethical complexities that comprise law enforcement-specific variations of these more general themes.

The first challenge that is well-established across different contexts refers to the quality of data used by AI-empowered law enforcement tools. Each activity of an LEA staff member creates a documentary trail, and these documents connect along a kind of value chain; starting from the police collecting data to produce information that is summarised in a report. This feeds into further investigation by the public prosecutor, to finally end up before a court where the indicted person stands trial. Transforming these trails from traditional paper files into an electronic format produces a wide variety of more or less easily accessible databases that can be used to train AI-empowered analysis tools to identify suspicious patterns. The quality of the results depends on the quality of the data used to train the tools. Any bias or blank spot in the original data will be present (if not reinforced) in the tool's performance. The need for bias detection and mitigation can be universally identified, but specific

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

regulatory processes that address its sociotechnical dimensions within law enforcement remain overlooked (see Chapter 5 for a discussion in the context of the AIA).

Second, AI-empowered tools can add to the cognitive overload of LEA staff by producing a redundant amount of information that can be hard to effectively handle. For example, in prominent cases of terrorist attacks in recent years (from the Boston bombers to terrorist attacks in Brussels, Berlin, and Paris), offenders had been on the radar of LEAs but, due to a lack of human resource coordination, the initial investigative leads were not followed up comprehensively. This is a fundamental problem that all forms of large-scale dragnet operations need to address (Kreissl, 2017). A general regulatory shift towards safeguarding human oversight over AI-enabled law enforcement tools and context-specific human resources may need to account for AI literacy and mitigation measures towards these emerging outcomes, especially in critical security domains.

Third, the underlying assumptions of algorithmic reasoning that uses statistically construed risk categories while ignoring the idiosyncratic features of the individual case have become an international debate, as demonstrated in sentencing guidelines. There are rarely any independent evaluation studies, based on rigid standards of scientific research, to assess the underlying risk perceptions and impact of these models. To determine whether a decline in the registered crime rate in an urban environment can be causally attributed to the implementation of predictive crime management tools is almost impossible, as long as not all relevant data (and the algorithms for their analysis) are made available for independent academic research (Meijer and Wessels 2019; Strikwerda, 2021). Commercial providers of such tools tend to showcase success stories from the police departments that have introduced their solutions, but whether these marketing narratives would stand a closer critical look is hard to determine as long as the key information is publicly inaccessible. This challenge points to algorithmic and procurement transparency and a need for independent evaluation before AI deployment as a normative practice.

2.5 CONCLUSION

The global divergences in regulatory approaches to AI shown in this chapter and the inherently complex nature of AI-empowered policing challenge regulatory frameworks for AI-enabled law enforcement tools. Our analysis suggests that this requires a dynamic approach to risk management that accounts for the socio-cultural and legal specificities of the respective jurisdictions. While transparency remains a foundational principle, particularly in exposing the decision-making processes of AI systems in policing (Pasquale, 2015), it should be combined with a nuanced understanding of local norms, expectations, civil liberties, and organisational structures that may also facilitate international regulatory and operational collaborations. Given the high-stakes implications of AI use in law enforcement, including potential infringements on privacy and disproportionate impacts on marginalised

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

communities, the deployment of AI in policing merits context-aware AI governance models that are likely to secure the legitimacy of AI interventions and the protection of fundamental rights in each societal setting.

REFERENCES

Almasoud, A. S. and Idowu, J. A. (2024) 'Algorithmic fairness in predictive policing'. AI and Ethics, 2025(5), pp.2323–2337.

Almeda, M., Garrett, P. and Zuboff, S. (2021) *Public expectations and the deployment of AI in law enforcement*. Cambridge: Centre for AI and Society.

Almeida, D., Shmarko, K. and Lomas, E. (2022) The ethics of facial recognition technologies, surveillance, and accountability in an age of AI: a comparative analysis of US, EU, and UK frameworks. AI and Ethics, 2(3), pp.377–387.

Amnesty (2025) Automated racism: How police data and algorithms code discrimination into policing. www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf (Accessed 25 August 2025).

California Legislative Information (2024) SB-1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (2023–2024). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1047 (Accessed 8 July 2025).

CEN-CENELEC (2025) Artificial Intelligence. CEN-CENELEC. www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/ (Accessed 25 August 2025).

China Law Translate (2023) Interim measures for the management of generative artificial intelligence services. https://www.chinalawtranslate.com/en/generative-ai-interim/ (Accessed 25 August 2025).

Colorado General Assembly (2024) *SB24-205 Consumer Protections for Artificial Intelligence: Concerning consumer protections in interactions with artificial intelligence systems*. 17 May. https://leg.colorado.gov/bills/sb24-205 (Accessed 8 July 2025).

Congress.Gov (2023) S.2892 – Algorithmic Accountability Act of 2023. 118th Congress (2023–2024). www.congress.gov/bill/118th-congress/senate-bill/2892/text (Accessed 8 July 2025).

Congressional Research Service (2023) *Law Enforcement Use of Artificial Intelligence and Directives in the 2023 Executive Order*. https://crsreports.congress.gov/product/pdf/IN/IN12289 (Accessed 8 July 2025).

Crawford, K. (2021) *The atlas of AI: power, politics, and the planetary costs of artificial intelligence*. London: Yale University Press.

Department for Science, Innovation and Technology (2024) *A pro-innovation approach to AI regulation: government response*. www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response (Accessed 8 July 2025).

Dorwart, H., Qu, H., Brautigam, T. and Gong, J. (2025) *Preparing for compliance: Key differences between EU, Chinese AI regulations*. https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations (Accessed 8 July 2025).

Dubravova, H., Cap, J., Holubova, K. and Hribnak, L. (2024) Artificial intelligence as an innovative element of support in policing. *Procedia Computer Science*, 237(2024), pp.237–244.

Emehin, O., Emeteveke, I., Adeyeye, O. J. and Akanbi, I. (2024) Generative AI in forensic data analysis: opportunities and ethical implications for cloud-based investigations. *International Journal of Research Publication and Reviews*, 5(10), pp.2941–2957.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Eubanks, V. (2018) Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press.
European Parliament (2024) *United States approach to artificial intelligence*. www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf (Accessed 8 July 2026).
European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, (59), 4 May 2016 (General Data Protection Regulation).
European Parliament and Council, Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119/89, (59), 4 May 2016 (Law Enforcement Directive).
European Parliament and Council, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, OJ L 2024/1689, 12 July 2024 (Artificial Intelligence Act).
European Union and United Kingdom (2019) Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community; Protocol on Ireland/Northern Ireland OJ C 384 I/01.
Executive Office of the President (2019) Maintaining American Leadership in Artificial Intelligence. *Federal Register*, 11 February. www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence (Accessed 8 July 2025).
Executive Office of the President (2023) Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. *Federal Register*, 30 October. www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (Accessed 25 August 2025).
Executive Office of the President (2025) Strengthening and Promoting Innovation in the Nation's Cybersecurity. *Federal Register*, 16 January. www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity (Accessed 25 August 2025).
Ezeh, N., Widgery, A. and Canada, C. (2025) Artificial Intelligence and Law Enforcement: The Federal and State Landscape. *NCSL*. www.ncsl.org/civil-and-criminal-justice/artificial-intelligence-and-law-enforcement-the-federal-and-state-landscape (Accessed 8 July 2025).
Farber, H. B. and Vyas, A. (2025) Truth and technology: deepfakes in law enforcement interrogations. *University of Pennsylvania Journal of Constitutional Law*, 27(5), pp.977–1034. https://repository.law.upenn.edu/Documents/Detail/truth-and-technology-deepfakes-in-law-enforcement-interrogations/529663 (Accessed 8 July 2026).
Ferguson, A. G. (2024) Generative suspicion and the risks of AI-assisted police reports. *Northwestern University Law Review*, 120(2), pp.299–363.
Finocchiaro, G. (2024) The regulation of artificial intelligence. *AI & Society*, 39(n.i.), pp.1961–1968.
H.R.2575 – AI in Government Act of 2020.
H.R.3935 – FAA Reauthorization Act of 2024.H.R.4346 – CHIPS and Science Act.
H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019.
H.R.6216 – National Artificial Intelligence Initiative Act of 2020.
Jarovsky, L. (2025) DeepSeek's Legal Pitfalls: Emerging AI Governance Challenges. Edition167. *Luiza's Newsletter*, 2 February. www.luizasnewsletter.com/p/deepseeks-legal-pitfalls?utm_

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

source=post-email-title&publication_id=808767&post_id=156291145&utm_campaign=email-post-title&isFreemail=true&r=54z7ep&triedRedirect=true&utm_medium=email (Accessed 23 April 2026).

Joh, E. E. (2024) Police technology experiments. *Columbia Law Review Forum*, 125(1), pp.1–28.

Kimery, A. (2025) Trump's new executive order on AI underemphasizes privacy, security issues. *Biometric Update*. www.biometricupdate.com/202501/trumps-new-executive-order-on-ai-underemphasizes-privacy-security-issues (Accessed 23 April 2026).

Kreissl, R. (2017) Will more data bring more security? Remarks on the European Security Union's approach to interoperability. In CEPS (ed.), *Constitutionalising the Security Union*, Brussels, pp.93–99. www.cepol.europa.eu/sites/default/files/26-reinhard-kreissl.pdf (Accessed 8 July 2025).

Kreissl, R. & von Laufenberg, R. (2022) Das Verbrechen lesen – Fakt, Fiktion und Phantasma kriminalistischer Spurensuche im digitalen Zeitalter. *Neue Kriminalpolitik*, 34(2), pp.175–189.

Laperuque, J. (2025) Status of state laws on facial recognition surveillance: continued progress and smart innovations. *Tech Policy Press*. www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ (Accessed 23 April 2025).

Lee, Y., Bradford, B. and Posch, K. (2024) The effectiveness of Big Data-driven predictive policing: Systematic review. *Justice Evaluation Journal*, 7(2), pp. 127–160.

Leslie, D. (2020) Understanding Bias in Facial Recognition Technology. *The Alan Turing Institute*. www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf (Accessed 23 April 2026).

Lewis, S. (2024) How artificial intelligence is changing the reports US police write. *The Guardian*, 3 October. www.theguardian.com/technology/2024/oct/03/artificial-intelligence-police-reports (Accessed 8 July 2025).

Liberty (2019). Report: Policing by Machine. *Liberty*. www.libertyhumanrights.org.uk/issue/policing-by-machine/ (Accessed 23 April 2026).

Loring, J. M. and Lee, A. R. (2024) California Poised to Further Regulate Artificial Intelligence by Focusing on Safety. *The National Law Review*, 17 September. https://natlawreview.com/article/california-poised-further-regulate-artificial-intelligence-focusing-safety (Accessed 3 February 2025).

Lucero, K. (2019) Artificial intelligence regulation and China's future. *Columbia Journal of Asian Law*, 33(1), pp.94–171.

Lynskey O. (2019) Criminal justice profiling and EU data protection law: precarious protection from predictive policing. *International Journal of Law in Context*, 15(2), pp.162–176.

Madiega, T. (2023) Generative AI and watermarking. *EPRS | European Parliamentary Research Service Briefing*. www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf (Accessed 3 February 2025).

Mao, Y. and Shi-Kupfer, K. (2021) Online public discourse on artificial intelligence and ethics in China: context, content, and implications. *AI & Society*, 38(1), pp.373–389.

Matejic, N. and Wilson, C. (2024) Crimes of influence: generative artificial intelligence-led crime as a service. *The Commonwealth Cyber Journal*, n.v.(n.i.), pp.75–95.

Matthews, D. (2023) The AI rules that US policymakers are considering, explained. *Vox*, 1 August. www.vox.com/future-perfect/23775650/ai-regulation-openai-gpt-anthropic-midjourney-stable (Accessed 23 April 2026).

Meijer, A. and Wessels, M. (2019) Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), pp.1031–1039.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Nandivada, S. N. and Haan, J. H. (2025) Kickstarting AI in the Federal Government: OMB's Policy to Implement Executive Order 14179. *Morrison Foerster*, 15 April. https://govcon.mofo.com/topics/kickstarting-ai-in-the-federal-government-omb-s-policy-to-implement-executive-order-14179 (Accessed 23 April 2026).

Nash, I., Kennedy-Mayo, D., Swire, P. and Antón, A. (2024) Legal issues in reconciling data protection, AI, and cybersecurity under EU law. *Missouri Law Review*, 89(3), pp.871–939.

National Institute of Standards and Technology (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0). *NIST*, January. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (Accessed 23 April 2026).

National Police Chiefs' Council (2023) Covenant for Using Artificial Intelligence (AI) in Policing, Version 1.1. *Office of the Police Chief Scientific Adviser*.

Nikolakopoulos, A., Evangelatos, S., Veroni, E., Chasapas, K., Gousetis, N., Apostolaras, A., Nikolopoulos, C. D. and Korakis, T. (2024) Large language models in modern forensic investigations: Harnessing the power of generative artificial intelligence in crime resolution and suspect identification. In *2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE)*, pp.1–5.

O'Neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pearsall, B. (2010) Predictive policing: The future of law enforcement. *National Institute of Justice Journal*, n.v.(266), pp.16–19.

Penney, J. W. (2022) Understanding chilling effects. *106 Minnesota Law Review*, 1451(2022), pp.1451–1530.

Raji, I. D., Kumar, I. E., Horowitz, A. and Selbst, A. (2022) The Fallacy of AI Functionality. Proceedings of the *2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)*, Seoul, Republic of Korea, ACM, New York, NY, USA.

Rice, T., Lamont, K. and Francis, J. (2024) The Colorado Artificial Intelligence Act: FPF US Legislation Policy Brief. *Future of Privacy Forum*, July. https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf (Accessed 23 April 2026).

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V. and Floridi, L. (2021) The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation, *AI & Society*, 36(n.i.), 59–77.

Ryan-Mosley, T. (2023) Why everyone is mad about New York's AI hiring law. *MIT Technology Review*, 10 July. www.technologyreview.com/2023/07/10/1076013/new-york-ai-hiring-law/ (Accessed 23 April 2026).

Ryan-Mosley, T. and Heikkilä, M. (2023) Three things to know about the White House's executive order on AI. *MIT Technology Review*, 30 October. www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/ (Accessed 8 July 2025).

Sakshi, S. and Wadhwa, M. (2023) Enhancing Digital Investigation: Leveraging ChatGPT for Evidence Identification and Analysis in Digital Forensics. In *2023 IEEE International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India.

Sheehan, M. (2023) China's AI regulations and how they get made. *Horizons: Journal of International Relations and Sustainable Development*, 24(2023), pp.108–125.

Shepardson, D. (2025) Trump revokes Biden executive order on addressing AI risks. *Reuters*, 21 January. www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/ (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Stanford University Human-Centred Artificial Intelligence (2022) What the CHIPS and Science Act means for Artificial Intelligence. *Explainer*, August. https://hai.stanford.edu/sites/default/files/2022-08/HAI%20Explainer%20-%20What%20The%20CHIPS%20and%20Science%20Act%20Means%20for%20AI.pdf (Accessed 8 July 2025).

Strikwerda, L. (2021) Predictive policing: The risks associated with risk assessment. *The Police Journal*, 94(3), pp.422–436.

Taylor, M. (2023) The US CHIPS and Science Act of 2022. *MRS Bulletin*, 48.

Texas Responsible AI Governance Act (TRAIGA).

Thomas, G. (2024) Politicians Move to Limit Predictive Policing After Years of Controversial Failures. *Tech Policy Press*, 15 October. www.techpolicy.press/politicians-move-to-limit-predictive-policing-after-years-of-controversial-failures/ (Accessed 23 April 2026).

US Department of Homeland Security (2024) *Department of Homeland Security Artificial Intelligence Roadmap 2024*. www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf (Accessed 23 April 2026).

US Department of Homeland Security (2025) Artificial Intelligence Use Case Inventory Library. *US Department of Homeland Security*, 1 July. www.dhs.gov/publication/ai-use-case-inventory-library (Accessed 23 April 2026).

US Department of Justice (2024) Artificial Intelligence and Criminal Justice: Final Report. *US Department of Justice*, 3 December. www.justice.gov/olp/media/1381796/dl (Accessed 23 April 2026).

US House of Representatives (2024) Bipartisan House Task Force on Artificial Intelligence. *US House of Representatives*, December. https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/E4AF21104CB138F3127D8FF7EA71A393.ai-task-force-report-final.pdf (Accessed 23 April 2026).

US Department of the Treasury (2024) *2024 National Strategy for Combatting Terrorist and Other Illicit Financing*. *Department of the Treasury*, May. https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf (Accessed 23 April 2026).

Utah State Legislature (2024) S.B. 149 Artificial Intelligence Amendments. https://le.utah.gov/~2024/bills/static/SB0149.html (Accessed 8 July 2025).

Wang, W. W., Zhu, L., Wang, X., Di, X. and Zhu, Y. (2025) Artificial intelligence 'law(s)' in China: Retrospect and prospect. *Journal of AI Law and Regulation*, 2(1), pp.29–36.

White & Case (2024) AI Watch: Global regulatory tracker – United States. *White & Case*. www.jdsupra.com/legalnews/ai-watch-global-regulatory-tracker-2931403/ (Accessed 23 April 2026).

Wiggins, C. and Jones, M. L. (2023) *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. New York: W. W. Norton & Company.

Zhang, H. A. (2024) The promise and perils of China's regulation of artificial intelligence. *Columbia Journal of Transnational Law*, 63(1), pp.102–157.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

3

Know Your Red Flags: Detecting Trends and Patterns in Financial Crime

Moran Harari, Dimitrios Kafteranis, Markus Meinzer, Lucas Millan-Narotzky, and Alison Schultz

3.1 INTRODUCTION

In response to high-profile money laundering scandals, global and EU anti-money laundering (AML) frameworks have been significantly strengthened (Ates et al. 2025a; Jackson et al. 2023). Obliged entities (OEs) such as banks, real estate agents, and lawyers are now required to file suspicious transaction reports (STRs) under broadened criteria, and growing awareness – especially after record fines imposed on major financial institutions – has led to a sharp increase in filings (Cusack 2022). As a result, Financial Intelligence Units (FIUs) and law enforcement agencies (LEAs) face a mounting volume of STRs, often with limited resources to process them (FATF-GAFI 2022 p. 37; Lando & Landry 2023 p. 3). Given the high proportion of false positives, effective systems for red flagging by OEs and for STR analysis and prioritisation by authorities are now essential.

We propose a novel geographic risk assessment methodology to improve both red-flagging practices in transaction monitoring by OEs and the prioritisation of growing numbers of STRs for more effective identification, investigation, and prosecution of financial criminal conduct. Designed on the basis of the Financial Action Task Force (FATF)'s conceptualisation of risk, our approach integrates geographic risk considerations derived from objective and verifiable data, mirroring a macro approach discussed recently in the context of National Risk Assessments (Grondona et al. 2025). It builds on the notion that financial secrecy creates a criminogenic environment which enables illicit financial flows (IFFs) and transactions. Not least in the EU's AML regulation 2024/1624 (European Parliament and Council 2024b), secrecy is explicitly recognised as a key enabling factor in illicit finance (Annex III(3)(f)). Everything else equal, the more secretive a transaction (involving sender, recipient, and means of transfer), the higher the risks of illicit activity. The higher the value of the transaction, the bigger its potential harm.

Our methodology for improved geographic risk assessment combines data on the likelihood of an illicit activity to occur with a measure of the scale of harm or damage that would result if it was to occur. To this end, our model focuses on two types of

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

variables that are difficult to manipulate and mostly available in financial transactions as well as STRs: transaction amount and jurisdiction of the sender and the receiver of the money flow. To operationalise the geographic component of this simplified framework, we use the Secrecy Scores (SS) of the Financial Secrecy Index (FSI) (Tax Justice Network 2025) for the approximation of the diverse opportunities for IFFs in a given jurisdiction.

In order to showcase the methodology, we apply it to the FinCEN leaks dataset made available by the International Consortium of Investigative Journalists (ICIJ), including over 18,000 transactions stemming from 534 Suspicious Activity Reports (SARs) (Shiel & Starkman 2020).[1] As the quantitative and qualitative analysis of these results indicate, our proposed risk model adds substantial value to national and regional LEAs. Previous research has shown the same approach can be applied to monitor financial transactions in the context of SWIFT and ISO 20022 wire transfers (Meinzer et al. 2023).

This chapter is organised as follows. Section 3.2 includes a literature review and positions our contribution in the literature. In Section 3.3, we discuss the methodology, data, the model and limitations. Section 3.4 presents the results of applying the model to the empirical dataset of available STRs. Section 3.5 concludes.

3.2 LITERATURE REVIEW AND CONTRIBUTION

Supported by a global system of norms, policy recommendations and standards as well as mutual evaluations of their implementation via peer reviews, a transnational legal order (Halliday & Shaffer 2015) for the prevention of money laundering has been established since the creation of the FATF in 1989. While some elements of this order remain contested and are still in the process of normative settlement (such as beneficial ownership transparency (Ates et al. 2025b)), other elements are firmly established. This chapter contributes to and connects two of those established elements, namely the system of mandatory filing of STRs by OEs from the private sector, and the risk-based approach (RBA) for countering money laundering. We proceed by revisiting relevant debates across criminology, law, economics, and computer science.

3.2.1 *Suspicious Transaction Reports (STR)*

STRs are central to AML and counter-terrorist financing efforts, enabling LEAs to identify potentially illicit activity. Since the FATF's first recommendations in 1990, which required countries to enact suspicious transaction reporting (FATF 1990), STRs have become standard practice. In 2025, FATF Recommendation 20

[1] For our purposes, we consider there is no significant difference between SARs and STRs. Henceforth, we will collectively refer to them as STRs.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

mandates that financial institutions report suspected criminal or terrorist-related funds to FIUs (FATF 2012–2025). However, beyond general requirements like identifying transaction originators and beneficiaries (Rec. 16), global STR formats and content are not harmonised.

Legal scholars have examined the broadening scope of reporting duties (Borlini & Montanaro 2017; Ping 2005) and the lack of comparative research on FIUs and STR practices in Europe (Panevski et al. 2021). Compliance among Designated Non-Financial Businesses and Professions (DNFBPs), such as lawyers and real estate agents, is often weak (Nduka & Sechap 2021; Omar & Johari 2015). While, in some jurisdictions, disclosures may be legally constrained by professional secrecy, low STR submissions from these sectors can mislead authorities about the level of risk. Recent work highlights how data-driven systems influence AML professionals' behaviour in monitoring and red-flagging transactions (Ogbeide et al. 2024).

STR submission processes vary widely, even within the EU. Despite broad use of the goAML software (United Nations n.d.), differences persist in technology, red flags, legal frameworks, and automation. The fourth AML Directive (Directive (EU) 2015/849 or '4AMLD') does not standardise format or content, while other countries across the globe allow STRs to be submitted in paper format (European Parliament and Council 2024a; FATF 2019). Although the latest EU AML package aims to harmonise these elements (European Council 2024), earlier explicit ambitions have been scaled back (European Commission 2021 Article 50).

A key concern in the literature is the exponential growth of STRs, often generating an 'overflow of useless AML information' (Dalla Pellegrina & Masciandaro 2009 p. 932). Defensive over-reporting by OEs, driven by fear of penalties and lack of reward for precision, reduces the effectiveness of STRs (Ross & Hannan 2007 p. 107; Takáts 2007). Though RBA were introduced to curb this trend, STR volumes often keep growing and false positive rates remain high – ranging from 30 per cent to over 95 per cent (Chen et al. 2018 p. 276; Jensen & Iosifidis 2023 p. 8889; Riccardi & Reuter 2024; Richardson et al. 2019).

Scholars emphasise the need for a feedback loop between FIUs and reporting entities to improve STR quality (Ogbeide et al. 2023 p. 9). Currently, entities often lack insight into outcomes of their reports, hindering refinement of detection systems. A robust feedback mechanism would enhance the utility of STRs and enable greater use of artificial intelligence (AI) and machine learning in AML frameworks.

3.2.2 *Geographic Risks in Financial Crime Literature*

The RBA became a cornerstone of AML frameworks following the FATF's 2003 recommendations. With further refinements in 2007 and 2013, it has since become embedded in transnational AML legal frameworks (Financial Action Task Force 2003, 2007, 2013; Ross & Hannan 2007 p. 107). Regulators continue issuing updated

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

guidance on how OEs and LEAs should address IFF risk (European Banking Authority 2021; European Commission 2022; European Union 2023; Financial Action Task Force 2022), and substantial fines have been imposed on OEs when automated red-flagging models failed (Turksen et al. 2024 pp. 373–374).

At the macroeconomic level, the International Monetary Fund (IMF) has employed machine learning and case study analysis to trace abnormal financial flows and assess national vulnerabilities – including around financial secrecy (Jackson et al. 2023). Regulatory impacts on money laundering routes have been documented empirically (e.g. Aldama-Navarrete 2021), and national risk assessments remain a major theme in AML scholarship (Ferwerda & Kleemans 2019; Grondona et al. 2025).

At the micro level, scholars have developed numerous models of AML risk assessments. Ross & Hannan (2007) defined essential conditions for risk-based decision-making to work effectively: shared definitions of risk, a quantifiable model, and feedback loops from outcomes. These principles remain pivotal in legal, criminological, and supervisory analyses. Although some scholars (Bello & Harvey 2017; de Koker 2009) critique FATF's vagueness, we align with those building upon its framework. For example, Savona et al. (2017 pp. 26–27) specify a function of risk consisting of two elements: the probability of an adverse event occurring, and the impact that would result if it did.

Risk models often consider at least three categories of risk, always inclusive of geographic risk (Alexandre & Balsa 2023 p. 2; AUSTRAC & Australian Government 2020; Sathye & Islam 2011 p. 172). FATF's guidance highlights geographic, customer, and product/service risk (Financial Action Task Force 2007 pp. 22–23) and the EU's 2024 AML package further specifies parameters within these categories (European Parliament and Council 2024b, Article 20 and Annex III).

Geographically determined levels of financial secrecy are widely used in both research and administrative practice. For example, Riccardi & Reuter (2024 pp. 341, 348–349) use financial secrecy in their conceptual framework to explain the level of sophistication of money laundering methods. Similarly, the models proposed by Hopkins and Shelton (2019, pp. 67–69), Savona et al. (2017, p. 162) or the research carried out by the Italian Central Bank (Cassetta et al. 2014) conceptualise jurisdictional financial secrecy as drivers of IFFs.

In administrative practice, financial secrecy is acknowledged to facilitate tax evasion (ECORYS 2021), money laundering, and the financing of terrorism (European Commission 2022; EUROPOL 2021; Savona et al. 2017). As the European Commission's 2022 Supra-National Risk Assessment states: 'Anonymity remains a critical vulnerability in the international financial system, [. . .] legal entities and arrangements are valued by criminals for their ability to enhance anonymity and conceal the identity of beneficial owners, as well as a means to carry out their illicit activities, for example by facilitating logistics or transport of illicit goods' (European Commission 2022 p. 10). In the EU, the regulatory

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

environment entering into force in 2027 explicitly requires the new Anti-Money Laundering Authority (AMLA) to issue guidelines defining money laundering (ML) risk factors (Article 32), including 'third countries identified by credible sources or pursuant to acknowledged processes as enabling financial secrecy' (European Parliament and Council 2024b, Annex III(3)(f)).

Empirical research on AML is severely constrained by data access limitations due to confidentiality of police files and STRs (Levi et al. 2018; Reuter & Riccardi 2024 p. 331). Data from OEs can be hard to access too, yet a body of research has been developed including by tapping into the 'pool' of innocent transactions to which red flagging is applied.

Computer science literature discusses technical innovations in red flagging and STR analysis, including through outlier detection, AI and machine learning models, and visualisation strategies (Jensen & Iosifidis 2023; Lebid & Veits 2020; Singh & Best 2019). The features a successful AML data analysis tool for flagging STRs should possess include 'data quality, detection accuracy, scalability, and reaction time' (Chen et al. 2018 p. 248).

Additionally, the literature discusses two persistent problems with accessible data on risk assessment models. First, criminological and legal literature has warned against racial bias and disproportionate exclusion embedded in AI tools (Turksen et al. 2024). In one documented case, ethnic minorities were systematically excluded from banking services by AI systems (Chen et al. 2018 p. 279). These tools can infringe fundamental procedural rights such as the right to a fair trial and the presumption of innocence (Sachoulidou 2023).

A second issue concerns geographic risk indicators themselves. The widespread use of so-called 'blacklists' – like FATF grey/blacklists or the EU's non-cooperative jurisdiction list – often reflects political biases rather than objective data. Research shows that countries with limited geopolitical power, especially from the Global South, are overrepresented on such lists, while powerful nations (e.g. the US) are omitted even though they are essentially displaying the same characteristics as the listed ones (Bello & Harvey 2017; de Koker 2024; Dolar & Shughart 2011; Meinzer 2016; Sharman 2010; Unger 2023). Even advanced systems struggle with concomitant oversimplification. For example, the risk models of the Spanish notary supervisory authority use binary categories such as domestic/foreign or inclusion in official high-risk country list (García Fresno 2022; Ministerio de Hacienda y Función Pública 2023), thereby missing the nuance of secrecy gradients. The European Parliament has noted that EU tax 'blacklists' may be politically motivated rather than being grounded in objective assessments (European Parliament 2023).

Against this background, we argue that a more robust, data-driven alternative is needed. Instead of dichotomous classifications, jurisdictions should be evaluated on a spectrum of financial secrecy, using independent, transparent, and verifiable data. This approach reflects growing consensus across disciplines and aligns with best practices for reducing discriminatory, politically biased, or overly simplistic assessments.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

3.2.3 *Research Gap and Contribution*

Since the publication of the IARM study of 2017 (Savona et al. 2017), a consensus is emerging in the literature on the need of more robust geographic risk assessment based on the levels of financial secrecy in AML. Riccardi and Reuter have conceptualised the AML environment money launderers are facing to a large extent in terms of geographically bound levels of financial secrecy. More specifically, they argue that low levels of banking and corporate transparency, coupled with the absence or weakness of cash regulations and asset recovery policies, attract money launderers, hence increasing the risk of ML (Riccardi & Reuter 2024 pp. 348–349). Yet, they remain silent on a data source or operationalisation of these levels of corporate and banking transparency. It is this gap we propose to fill with our approach.

At the level of computer science, we build on Jensen and Iosifidis who argue that 'banks face two principal data analysis problems in AML: (i) client risk profiling and (ii) suspicious behavior flagging' (Jensen & Iosifidis 2023 p. 8890). While our contribution lies in the second of those categories and more specifically at the transaction level, we argue that our model can be applied by both OE and LEAs. The data processing challenges faced by OE and LEAs are similar not least because the number of STRs continue to grow and for many countries surpass the mark of hundreds of thousands of STRs per year (Vedrenne 2023; Xue & Zhang 2016). The challenges encompass various dimensions, ranging from normative and legal (discrimination) to statistical challenges caused by data features of class imbalance and related challenges (Jensen & Iosifidis 2023). Both need scalable systems with real time processing capabilities that ensure accuracy while keeping a high detection rate. Our approach can be combined with existing statistical inference methods for the detection of crime, with the potential to ultimately reduce the ratio of false positive alarms while increasing STR effectiveness for OE and LEA alike.

We respond directly to calls for integrating transaction monitoring into dynamic risk assessment (Lannoo & Parlour 2021 p. 25) and to calls for a model that can operate with parsimonious data input, as opposed to possibly more complex models which have tended to fail to deliver robust results either because of their lack of transparency or because relevant data inputs have not been available consistently enough across time and space (Hopkins & Shelton 2019 pp. 66–67). The proposed method exploits geographic and transaction volume data found in STRs to produce unambiguous and dynamic prioritisation for further investigations or reporting and equips the OE and LEAs with relevant knowledge to inform their decision-making processes on filing an STR or opening further investigations, respectively. Beyond the technical efficiency of this geographic risk approach, a key operational advantage is its capacity to inform compliance officers and supervisors on the underlying risks related to the regulatory framework in place where the parties to a transaction are established. By drawing on an open-source repository of verifiable legal data,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

relevant information can be made available to investigators as need arises, showing overall scores, broad risk categories, or specific legal analysis. Thus, even without detailed knowledge of the regulatory particularities in each jurisdiction, investigators and OEs should be able to assess geographic risks in any given case and understand the nature of underlying vulnerabilities.

From a behavioural perspective, the proposed methodology hinders strategic manipulation in two ways. First, neither criminals in the case of OEs, nor OEs in the case of LEAs, can anticipate the outcome of their reporting with a view to potentially structure their transactions or filing of STRs with the intention to remain below certain thresholds or alarm levels. As they do not have access to the pool of transactions or STRs in which they are transacting or filing, respectively, they cannot know for certain if a specific transaction would be prioritised as high risk in the dynamic data pool. Second, criminals could decide to transfer activities to jurisdictions with lower Secrecy Scores, yet this would prove self-defeating in the longer term because stronger regulations would greatly increase the risk of detection and prosecution of illicit activity.

In comparison to other risk assessment methods, our approach avoids bias at two different levels. First, the FSI methodology employs a uniform standard across countries to avoid political bias, unlike inconsistent approaches such as the EU Code of Conduct and FATF listings, which often overlook high-risk financial activities in geopolitical allies (e.g. the US and Luxembourg) while disproportionately targeting adversarial jurisdictions (e.g. Iran and North Korea), which are routinely blacklisted (FATF-GAFI 2003). Such biases, including documented discrimination against Global South countries (Dean & Waris 2021), are heavily amplified when the output of risk assessments is a binary classification (high risk vs. low risk). The proposed approach assigns values from 0 (most transparent) to 100 (most secretive), enabling a more nuanced evaluation of secrecy risks (Janský et al. 2022). Second, the model's orientation toward regulatory context, rather than sender or recipient personal characteristics, ensures that assessments remain non-discriminatory. Scoring systems often used by OEs and LEAs run the risk of embedding bias through profiling, potentially resulting in systemic discrimination (Sciurba 2018).

Finally, the proposed geographic risk methodology can be considered forward-looking for different reasons. On the one hand, the evaluation of Secrecy Indicators using the 'weakest link' approach highlights loopholes available in jurisdictions even if these can be considered dormant, in the sense that there is no indication yet that they have been exploited by criminals. The capacity to account for potential (future) exploitation of regulatory loopholes provides a clear advantage over statistical methods that infer risks only on the basis of past criminal activity (see Lebid & Veits 2020). On the other hand, many FSI indicators have set early benchmarks that later influenced global standards. Indeed, while FATF recommendations are widely viewed as global AML standards, they emerge from slow-moving institutional

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

consensus, often shaped by self-regulatory ideology and the disproportionate lobbying power of certain member states, raising concerns about neutrality, effectiveness, and the influence of geopolitical interests. The FSI's ambitious benchmarks ensure that gaps are highlighted, even when media attention or policy priorities have not yet driven the establishment of stronger global regulations. For example, requiring beneficial owners of legal entities to be registered with a public authority – rather than with a private intermediary – has been an FSI standard since its inception in 2009 and only in recent years has been adopted in the EU and beyond (Ates et al. 2025b).

The proposed model thus intends to complement existing systems equipping both LEAs and OEs with a dynamic risk-assessment methodology that may serve as a basis for further analysis or be used as a cross-checking tool to make sure no high-risk transaction or STR is disregarded. The following section explains in detail how our assessment works and how it is applied to a dataset of STRs.

3.3 Modelling Geographic Risk in Financial Transactions

We estimate the geographic risk inherent to a transaction by combining three types of data, two of which are included in most transaction reports, including STRs: the amount as well as the jurisdiction of the sender/receiver of the transaction. We enrich this data with the levels of financial secrecy of the jurisdictions concerned in the transactions to arrive at a relative measure of risk.

3.3.1 *Data*

3.3.1.1 Suspicious Transaction Report (STR) Data

Legal research on STRs undertaken in the TRACE project compared reporting requirements across EU member states and evaluated the role of STR/SARs within AML investigative processes. Yet attempts to obtain anonymised STR data from EU authorities yielded a relatively small sample of twenty-one STRs from two EU member states. While this sample provided useful insights on STR reporting differences and opportunities for harmonisation, it was insufficient to showcase the effectiveness of our geographic risk assessment in providing a simple way to evaluate risk across large datasets and ultimately improve the allocation of investigative resources. For this reason, we use an extensive dataset of 534 STRs that includes more than 18,000 underlying transactions, made available by the ICIJ following the FinCEN leaks (ICIJ 2020).

The Financial Crimes Enforcement Network (FinCEN) is the FIU of the United States Treasury Department. It is responsible for collecting, analysing, and disseminating financial information related to investigations of illicit finance, including ML and terrorist financing (TF). In order to better exploit the STRs data that is filed

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

by reporting entities, FinCEN analysis of this data also includes the identification of emerging trends and techniques related to ML and other financial crimes, as specified in Article 31 USC 310(b)(2)(C) (US Congress 2024). This allows FinCEN to enhance its knowledge of methodologies, typologies, geographic patterns of activity, and systemic weaknesses pertaining to ML and TF (FATF-GAFI 2016 pp. 60–62). The analytical work is primarily focused on intricate cases where LEAs require support in identifying multiple individuals involved, mapping out criminal financial activities across extensive geographical regions, and establishing international connections that may not be immediately evident during initial investigations. FinCEN's analysts also generate threat assessments, industry reports, and technical guides that offer insights into financial transaction mechanisms (FATF-GAFI 2016). According to a FinCEN report published in 2024, the number of SARs filed by reporting entities to FinCEN in 2023 was approximately 4.6 million (FinCEN 2024).

The ICIJ investigation of the leaked FinCEN files was published in September 2020 and exposed vast amounts illicit transfers by banks. The investigation was based on a trove of classified documents, obtained and shared by BuzzFeed News. The documents included more than 2,100 SARs filed by global banks with FinCEN. This unprecedented data leak evidenced the movement of over USD 2 trillion in potentially illicit payments between 1999 and 2017, all of which were flagged by the banks themselves (ICIJ 2020). The leaked documents include numerous spreadsheets detailing the activities of financial institutions with clients under suspicion across more than 170 countries and territories.

Despite the various tools implemented by FinCEN to monitor typologies and geographic patterns of activity, the ICIJ found that in half of the FinCEN files reports, information was missing about at least one or more entities behind the transactions (ICIJ 2020). The data used for this study is a sub-sample of 534 SARs which represents approximately 25 per cent of the 2,100 SARs included in the leaked records. The sub-sample corresponds to the transactions for which ICIJ journalists were able to identify sufficient details on both the originator and beneficiary banks (ICIJ 2020) and represents approximately USD 35 billion (out of more than USD 2 trillion worth of transactions in the leaked files), or about 1.75 per cent. In our view, the fact that only a minor part of the leaked STRs actually included data on the countries from which the transactions were sent and in which they were received – let alone the actual identity of the originators and beneficiaries – provides a clear indication for a need to systematise and harmonise the way STRs are filed.

In the EU, the evolving regulatory environment exemplifies international initiatives to harmonise STR reporting. With regards to geographic information in STRs (i.e. the location of the transaction's sender and recipient), most reports accessed for this chapter present the information in a (semi-)standardised format. As mentioned above, we expect that minimal reporting requirements related to sender and recipient jurisdiction will be implemented in the near future, resulting from the interplay

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

between AMLR 2024/1620 (Articles 1(3), 5(5)(j) and Article 50) and AMLR 2024/1624 (Article 69) (European Parliament and Council 2024b 2024c). Geographical locations of sender and recipient are not only superior to other variables in terms of data availability, but they also represent transaction features that are hard to obfuscate and usually directly verifiable by OE and supervisors alike.

While certain jurisdictions may be ahead in terms of STR reporting systems and analysis, we expect that increased harmonisation at regional or global levels will gradually allow more systematic and evidence-based assessment of cross-border ML risks. Importantly, consolidation of STR data from multiple jurisdictions should clear the way for comprehensive research on anonymised STR data.

3.3.1.2 Financial Secrecy Index (FSI) Data

Our analysis incorporates data on financial secrecy laws and practice across multiple jurisdictions, drawing from official reports, datasets from international organisations and original legal assessments. Wherever feasible, the scoring incorporates the results of tests on how the regulatory framework is operating in practice. This data forms the basis of the FSI 2025 (Tax Justice Network 2025).

Since its inception in 2009, the FSI methodology has undergone eight revisions. The 2025 edition categorises twenty equally weighted Secrecy Indicators (SI) into four key dimensions to assess jurisdictional vulnerabilities to financial crime (see Table 3.1). Ownership registration (Indicators 1–6) evaluates banking secrecy, anonymous trusts/foundations, bearer shares and shell companies, real estate, and high-value assets, where absence of ownership registration enables exploitation for criminal purposes. Legal entity transparency (Indicators 7–11) focuses on corporate structures, measuring vulnerabilities from opaque limited liability partnerships, undisclosed company ownership, non-public accounts, and inadequate country-by-country reporting or Legal Entity Identifier (LEI) use – gaps that facilitate large-scale tax evasion and other financial crimes. Tax and regulatory integrity (Indicators 12–16) assesses enforcement weaknesses, including lax tax avoidance reporting, golden visa schemes, problematic personal and capital income tax policies, and non-disclosure of tax rulings or extractive contracts, which collectively foster tax avoidance and corruption. International cooperation (Indicators 17–20) scrutinises the adherence to FATF standards, automatic tax data exchange (CRS/MCAA), and treaty ratifications that provide concrete legal avenues for cooperation on financial crime investigation and prosecution. Together, these indicators provide a systematic, evidence-based approach to quantify how jurisdictional loopholes amplify vulnerabilities to IFFs (Tax Justice Network 2025).

The geographic risk data within Secrecy Scores builds on economic and criminological research, analysing behavioural shifts following regulatory changes and evolving *modi operandi* of financial crime. The selection of risk indicators (regulatory characteristics that affect the likelihood that activities in a jurisdiction are

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 3.1 *The twenty financial secrecy indicators underpinning the secrecy score*

1 Asset and ownership registration	Legal entity transparency	Integrity of tax and financial regulation	International standards and cooperation
1 Banking secrecy	7 Transparency of partnerships with limited liability	12 Tax compliance focus	17 Anti-money laundering
2 Beneficial ownership of trusts	8 Transparency of company ownership	13 Golden visas	18 Automatic exchange of information
3 Beneficial ownership of foundations	9 Transparency of company accounts	14 Foreign investment income	19 Exchange of information upon request
4 Beneficial ownership of companies	10 Public country-by-country reporting	15 Public statistics	20 International legal cooperation
5 Freeports ownership	11 Legal entity identifiers	16 Tax rulings and extractive industries' contracts	
6 Real estate ownership			

exploited for financial crime) has followed a combined inductive/deductive process. On the one hand, we reviewed databases with comparative data on country regulations (e.g. FATF, OECD, UN, IMF, IBFD, etc.) to determine whether any readily available data could be used to assess secrecy risks. For instance, we integrate FATF Recommendation ratings into three different indicators, in relation to banks and crypto intermediaries' ownership-registration obligations (SI 1) and more generally AML regulations (SI 17) and effectiveness of international cooperation (SI 20). Thus, an inductive process allowed for the identification of various risk components. On the other hand, expert publications from international organisations (IO), academia, and civil society were reviewed in order to determine what additional regulatory characteristics could be included in the risk assessment framework. For this purpose, we considered not only the direct relevance to the underlying threat (ML, TF, fraud, tax abuse), but also the available resources to undertake comparative research across jurisdictions. An important motivation to undertake this additional research is that FATF comparative assessments (ratings) are not specific enough to identify concrete regulatory loopholes, and often disregard vulnerabilities on the basis of subjective, non-verifiable assessments. This deductive process yields additional risk components that are combined with other relevant data from existing sources.

An important feature of FSI's Secrecy Scores is their resilience and methodological accountability. Since 2009, the FSI has been updated biennially, with all

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

indicators revised simultaneously to reflect regulatory developments. Beginning in 2025, the FSI has transitioned to a rolling update system, publishing revised data for selected indicators every few months within a three-year cycle. The new system ensures that any regulatory changes flagged by jurisdictions in annual consultation exercises are integrated, following a strict verification process. This shift to rolling updates enables the index to incorporate regulatory changes as they emerge, offering a more dynamic and timely assessment of jurisdictions' roles in financial secrecy and global tax abuse (Meinzer & Harari 2023). This is a significant advantage over FATF evaluations, some of which have taken almost a decade to reassess like Luxembourg (FATF n.d.) and the United States (FATF 2024). Thus, proposed geographic risk data secures resilience through continuous updates, and ensures accountability by transparently identifying all underlying sources and giving jurisdictions the opportunity to enrich or rectify assessments.

3.3.2 *Methodology*

We develop our risk assessment method on the basis that risk is a combination of the potential impact of an occurrence of financial crime, and the likelihood for that impact to materialise (Savona et al. 2017 pp. 26–28). Building on the FATF risk assessment framework (FATF 2013), we conceptualise risk as a combination of the probability or likelihood of financial crime (derived from underlying threats and vulnerabilities) with its potential impact (Savona et al. 2017). As for the likelihood of ML and other financial crimes to occur, we use aggregate data of secrecy features at the jurisdiction level that act as proxies of relative threats and/or vulnerabilities. The following example illustrates this conceptual framework.

Consider a corporate officer approving a transaction as a payment to a company supplier or service provider established in another jurisdiction. If such jurisdiction requires systematic registration, verification and online publication of the beneficial owners of legal entities established therein, the likelihood that the corporate officer is embezzling funds would be low, insofar as it is quite simple for anyone to check whether the corporate officer is a beneficial owner of the recipient company, and criminal activity would thus be easy to detect. If, however, the recipient jurisdiction does not require beneficial ownership (BO) registration, the likelihood that the individual embezzles funds is higher, given that the obfuscation of effective ownership and control can disguise the transaction as a legitimate payment to an independent third party (Cardao-Pito 2022). In the two situations, the potential impact of illicit activity would be the same transaction amount. Thus, *ceteris paribus*, combining the likelihood of illicit activity with its impact, the risk of the considered transaction will be higher in the latter situation. As we want to aim for a prioritisation of STRs, rather than for an estimate of expected damage, our numerical representations of risk are not meaningful in absolute terms. Rather, they are useful only insofar as they convey a relative understanding of risks among different occurrences.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Aligned with the two conceptual pillars, we combine two types of measures: (i) a quantitative measure of the economic value at stake in the assessed transaction(s), and (ii) a quantified measure of the opportunities for criminal activity offered by secrecy jurisdictions. Our approach produces a single and clearly defined risk score for each transaction on the basis of the widely established knowledge that IFFs follow weak regulations and secrecy, that is that large transactions between jurisdictions where money can be easily hidden have the highest IFF risk (Aldama-Navarrete 2021; Boyer & Kempf 2020; Cobham et al. 2015; Houston et al. 2012; Janský et al. 2022).

From a methodological perspective, optimal STR risk assessment should aim to integrate any relevant indicator and account for as many different types of risk as possible. However, the lack of relevant data across jurisdictions can make STRs difficult to compare on the basis of more complex frameworks. We claim that at a minimum, STR-based risk assessment should take into account the opportunities available in originator and recipient jurisdictions to hide or obfuscate the true nature of underlying economic activity. The present approach minimises STR data preconditions (amount, origin, destination), to then fully develop secrecy risks on the basis of jurisdictions' regulatory features.

3.3.3 *Risk Assessment Model*

Based on the determinations outlined above, we start with the following conceptualisation: *Risk=Likelihood x Impact*

Where:

- *Likelihood* is a function of threats and vulnerabilities, based on the opportunities of regulatory arbitrage allowed by financial secrecy.
- *Impact* is a function of the transaction volume recorded for an STR.

The next relevant definitions for our model concern these two functions, that is, the exact specification of Likelihood (Threat & Vulnerabilities) and Impact (transaction volume). We base these definitions on two considerations. First, we do not aim for an actual quantification of the expected damage, but only for an estimate that allows us to prioritise, that is, rank STRs according to the risk inherent in the reported transactions. Therefore, while the relative Likelihood and Impact of an STR should be commensurate across STRs, the resulting risk value does not need to have an economic interpretation. Second, the scaling of Likelihood and Impact needs to be such that both concepts contribute adequately to the overall risk score, without one of them entirely determining an STR's risk ranking. In this sense, transaction data is known to be highly right-skewed, with the vast majority of transactions being of relatively low value, and only a few transactions take very high values.

As shown in Figure 3.1, this skewing is apparent in the STRs from the FinCEN files. A simple product of our measures of Likelihood and Impact would thus assign

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

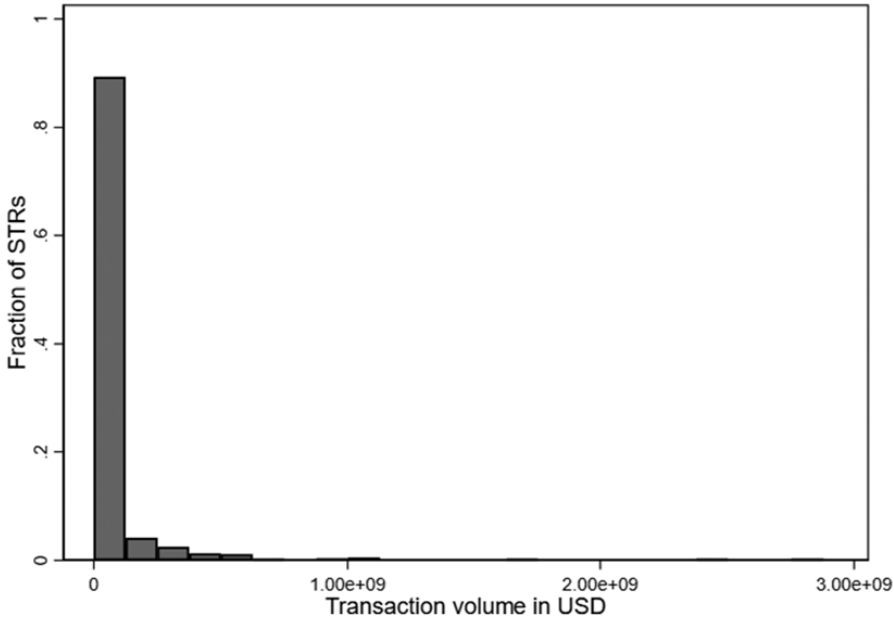

FIGURE 3.1 Distribution of transaction volumes in the FinCEN leaks dataset.

disproportional weight to large transactions, rendering the secrecy information irrelevant. To adjust for this pattern, we cube our likelihood measure and take the cube root of the transaction volume. This aggregation form has been reviewed by a study of the European Commission's Joint Research Center (JRC) (Becker & Saisana 2018). A useful alternative to the cube root function applied to transaction volumes is the logarithm function. For the model presented below, using the suggested cube root or the logarithm of transaction volume does not change the risk assessment of top-ranked transactions.

$$Risk = \left(\frac{SS_A + SS_B}{2}\right)^3 \times \sqrt[3]{transaction\ volume}$$

In order to assess the risk of a transaction from jurisdiction A to jurisdiction B, we determine the likelihood of illicit activity on the basis of the average of Secrecy Scores for the two jurisdictions involved. That average is then transformed through the cube function to derive the likelihood of illicit activity.

In our dataset, most STRs contain multiple transactions. This can be explained by the fact that a pattern of transactions is considered suspicious, rather than a specific unique transaction, and the obliged entity submits an STR to the FIU which includes all transactions considered potentially tainted by illicit activity. In order

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

to adjust our risk model to such situations, we calculate a weighted average of Secrecy Scores.

$$Likelihood = \left(\frac{\sum_i^n \left(\frac{SS_{Sender(i)} + SS_{Recipient(i)}}{2} \right) \times V_i}{\sum_i^n V_i} \right)^3$$

Where:

- n is the total number of transactions included within a STR report
- i designates sequentially each of the transactions in the STR report
- Vi corresponds to the transaction volume of the ith transaction
- $SS_{Sender(i)}$ reflects the Secrecy Score of the sender jurisdiction as applicable in the ith transaction
- $SS_{Recipient(i)}$ reflects the Secrecy Score of the recipient jurisdiction as applicable in the ith transaction

Thus, we can formalise a given STR's geographic risk with the following equation:

$$\text{Risk} = \left(\frac{\sum_i^n \left(\frac{SS_{Sender(i)} + SS_{Recipient(i)}}{2} \right) \times V_i}{\sum_i^n V_i} \right)^3 \times \sqrt[3]{\sum_i^n V_i}$$

In transactions where sender or receiver country information are missing, adjustments could be made to seamlessly include those in the model. For example, country-specific cash regulation scores could be used in case of cash deposits/withdrawals and for crypto-wallet senders and recipients, maximum secrecy could be assumed. This was not needed in the case of the FinCEN data because it lacks cash or cryptocurrency details.

3.3.4 *Limitations*

Despite the various advantages outlined above, the proposed geographic risk model is affected by several limitations.

First, some of the ML techniques relying on new and disruptive technologies can be effectively assessed with the proposed model of geographic risk assessment to the extent that they make use of front companies or bank accounts at some stage of the laundering process, such as 'transaction laundering' (Akartuna et al. 2023 p. 634). However, others prove more elusive to our approach since they lack a clearcut territorial 'location' for meaningful geographical risk attribution and necessitate further conceptual exploration and innovation for seamless integration into a baseline risk assessment model. For example, situations when a company established under the laws of country A has an account in country B, and carries on

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

a transaction with such account, both jurisdictions would be relevant for risk assessment. Optimally, standardised STR data would identify both jurisdictions, and risk indicators would account for threats and vulnerabilities alternatively with respect to country A (e.g. ownership registration) or B (e.g. banking-related AML regulations).

Second, our approach does not claim that automated geographic risk assessment methods are sufficient to identify the riskiest transactions, nor that human analysis of the facts and circumstances of each STR is redundant. Instead, the proposed method is conceived as complementary with other risk-assessment methods, notably those that take into account transaction features in relation to relevant parties' previous behaviour or expected behaviour in the context of transaction patterns across relevant economic sectors. There will always be an important for human agency in the design and evaluation of different risk-assessment outputs and techniques, and expert knowledge will continue to be particularly relevant in situations with potentially far-reaching legal consequences (Ogbeide et al. 2023 pp. 2–3).

Third, the proposed approach is focused on ML but may not accurately represent risks related to TF activities (Savona et al. 2017 pp. 26, 168). This is because in our model we approximate the harm or impact based on a quantitative monetary value, which does not capture the harm resulting from terrorist activities or other concrete predicate offences. Yet, in the realm of financial crimes, it is difficult or impossible to assess the underlying impact of a crime beyond the amount involved. Because all sorts of criminal actors use very similar financial secrecy tools, it can be very difficult to assess 'ex-ante' whether a given amount of funds results from relatively mild criminal activity (such as tax evasion) or from a particularly heinous type of crime (trafficking in human beings). Provided that standardised STR data can identify suspected predicate offences, FIUs may further develop risk-assessment models assigning different weights to transactions suspected of diverse predicate offences.

Finally, the effectiveness of the proposed method in identifying STRs that are relatively more useful in the investigation and prosecution of financial crimes could not be tested due to a lack of data on STR outcomes. The ultimate goal of any STR-based risk-assessment technique would be to single-out reports that are more likely to initiate a successful investigation or contribute to an existing one. This is what Europol refers as STR 'conversion': the fact that an STR filed by an obliged entity is further exploited by relevant authorities in the fight against financial crime (EUROPOL 2017 pp. 29–31). Without comprehensive analysis of large-scale STR datasets including the information on which reports have led to a criminal conviction, or have otherwise supported (ongoing) investigations, any risk analysis tool is arguably unable to demonstrate its effectiveness. Aiming to increase the historically low rate of STR conversion (EUROPOL 2017), international cooperation frameworks should ensure that conversion data is closely monitored in cross-border scenarios, and that comprehensive, anonymised, STR datasets are made available for academic research.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

3.4 RESULTS

Our model is designed for situations where so many different STRs need to be assessed that a manual prioritisation becomes overwhelming. In the following, we illustrate that our model can easily be applied to a large dataset, namely to all available STRs.

Table 3.2 presents the 15 STRs that have been ranked highest by our model out of the 534 STRs leaked in the FinCEN files. The large number of senders and recipients reported for most STRs reveals the high degree of complexity in the STR data of the FinCEN files. While Table 3.2 becomes close to unreadable due to complexity – even though it only includes the most relevant data fields, a slightly adapted version of our analysis[2] allows us to gain overview of the countries that contributed most to the IFF risk in the STRs from the FinCEN Files. As shown in Figure 3.2, transactions originating from or destined for Russia account for the largest share of overall risk (13.7 per cent), followed by those involving Latvia (13.1 per cent) and Switzerland (11.7 per cent).

The figure above illustrates the outputs that can be derived from a comprehensive geographic risk methodology. These outputs can not only be monitored in real time and allow the identification of the largest geographic risk exposures for further investigations or targeted supervisory measures, but also provide valuable input for National Risk Assessments (Grondona et al. 2025).

3.5 CONCLUSION AND POLICY RECOMMENDATIONS

Combating IFFs requires continuous innovation in AML methodologies, particularly as criminals exploit regulatory asymmetries across jurisdictions. This chapter contributes to this effort by developing a dynamic, evidence-based framework for geographic risk assessment that addresses critical gaps in current AML practices. Our approach builds on two decades of risk-based AML frameworks while challenging the limitations of politicised 'blacklisting'. By integrating minimal STR data with SI, we provide a scalable, transparent, and bias-resistant tool that enhances the detection and prioritisation of high-risk cross-border transactions. Unlike retrospective models that flag risks based on past criminal activity, our framework proactively identifies vulnerabilities in financial systems using the 'weakest link' approach. The FSI's rolling updates ensure that regulatory changes are promptly reflected, offering a dynamic alternative to slow-moving FATF evaluations. This forward-looking approach is critical for disrupting ML networks before they exploit weak regulations or enforcement.

[2] To estimate country-level risk contributions, we begin by calculating the risk for each individual transaction rather than for each STR, since a single STR can include multiple transactions. We then aggregate these transaction-level risks by summing all contributions associated with each country and report the country's contribution to overall risk.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CF15C048B4E80003C398D145

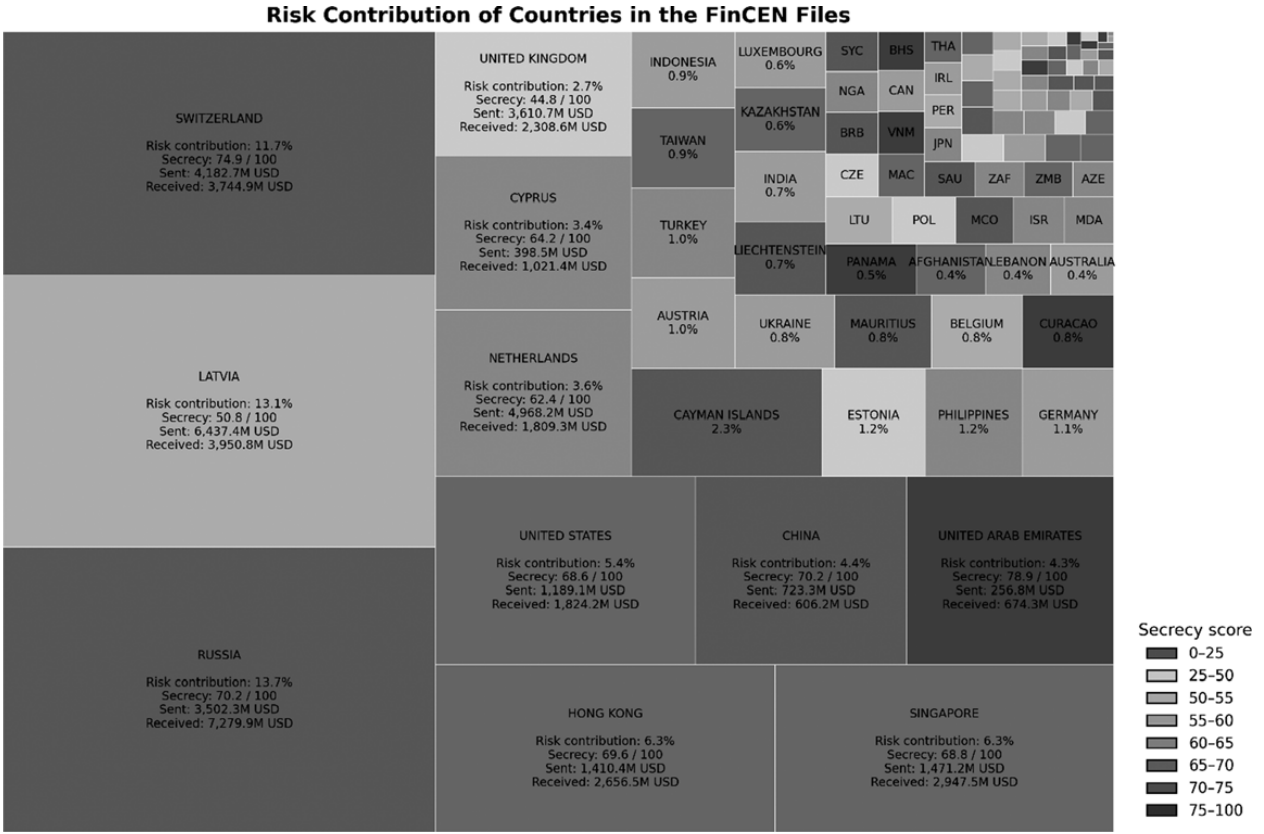

FIGURE 3.2 Risk contribution of different countries in the FinCEN files.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C04884E80003C398D145

TABLE 3.2 *Priority ranking of STRs in the FinCEN files*

Rank	STR Ref.	ISO sender	Secrecy Sender	ISO recipient	Secrecy Recipient	Secrecy STR	Volume (in US$)	Risk	Risk Contribution	Rank log model
1	2748	BEL, CHE, CYP (5), GBR (7), NLD, RUS (42), USA (11)	63	RUS (57), CHE (5), CYP (2), GBR (4)	70	66	2,878,948,864	416056000	1.17	4
2	2912	CYM (18), GBR (3), HKG (3)	63	HKG (6), USA (12), CYM (6)	72	67	1,658,486,016	357147904	1.00	7
3	2778	CHE (2), GBR, MCO (3), USA (2)	70	CHE (2), SGP (6)	70	70	1,070,848,064	353734144	0.99	2
4	2713	CHE (1), GBR (2), RUS (3)	73	USA (1), CHE (1), MUS (2), GBR (2)	67	70	953,490,048	333647968	0.94	6
5	3670	HKG (2), SGP	69	CHE, SGP (2)	70	70	921,257,600	332390272	0.93	5
6	2338	CHE (5), RUS (121), USA (12)	73	RUS (24), CHE (8), CYP (24), JPN (10), TUR (64), USA (8)	70	72	657,935,296	321726528	0.90	3
7	2266	CHE (12)	75	AUT, CHE (6), RUS (4), USA (1)	75	75	363,403,488	298272224	0.84	1
8	2729	CHE (5), CYP (6), RUS (7), USA	72	CHE (4), LTU, RUS (13), USA	72	72	274,660,960	246020496	0.69	8
9	2704	LVA (38), NLD (23)	57	LVA (23), NLD (38)	57	57	2,400,391,936	243103472	0.68	52
10	2859	LVA (8), RUS (2)	54	CHE (4), RUS (4), LVA (2)	69	61	1,094,978,432	235926608	0.66	30
11	3032	CYM, IRL, LUX, USA (7)	67	CYM (4), RUS, USA (5)	70	69	382,592,224	234950784	0.66	12
12	2322	CYP, GBR, MUS (4)	64	MUS (5), CYP	70	67	456,000,000	229099968	0.64	15
13	4069	CHN, HKG (4), SGP, THA	69	CHE, HKG (2), SGP (3), TWN	70	70	297,866,656	227654992	0.64	10
14	3789	SGP (14)	69	HKG (2), IND (4), SGP (8)	59	64	525,626,368	212822080	0.60	27
15	2380	CYP (4), NLD, RUS (12)	69	CYP (3), NLD (2), RUS (11), USA	68	69	258,861,840	205861328	0.58	16

Results highlight the ability to flag a reduced number of complex STRs often involving tens of underlying cross-border transactions, through the combination of transaction amounts and geographic regulatory data. We derive a calculation of risk associated with individual jurisdictions in the FinCEN dataset to map out broader secrecy risk exposures: Russia (13.7 per cent), Latvia (13.1 per cent), and Switzerland (11.7 per cent) are found to channel the most risk.

While geographic risk indicator selection and weighting is always open to debate, the FSI proposes a transparent methodology that integrates a variety of concrete regulatory characteristics. Availability of additional or alternative comparative data on financial regulation across a wide number of jurisdictions can allow expansion or adjustment of risk indicators, for instance, focusing on a specific type of ML (e.g. through real estate or high-value assets). Given appropriate resources and political will, methodologies such as the one presented in this chapter can allow targeted reduction of cross-border ML risks across specific categories of OEs. In the EU, expected but uncertain harmonisation of STR reporting and analysis may pave the way for robust, evidence-based, geographic risk assessment.

The implementation of a simple benchmark for STR-based risk assessments can help establish a minimum standard ensuring that no STRs above a certain threshold of risk are disregarded from thorough analysis. Further developments of the proposed risk assessment model could integrate non-public LEA data and calibrate risk indicators to maximise quantifiable policy goals (such as convictions or criminal funds recovered). This requires meticulous record keeping and monitoring of case developments, to ensure that the outcomes or use of each STR are systematically recorded, especially in cross-border scenarios. Furthermore, any successfully prosecuted financial crime case that did not trigger STR should also integrate tainted transactions into a dataset for risk model calibration. Arguably, a comprehensive evaluation of the effectiveness of current STR frameworks cannot be undertaken without analysing a large enough random sample of transactions that were not flagged by OEs. With DNFBPs and Virtual Asset Service Providers (VASPs) repeatedly showcased in vast financial crime cases, the extent of illicit activity in these sectors is a 'known unknown'. We shall question the effectiveness of STR frameworks in contexts where OEs are highly conflicted (business opportunity vs. STR) or directly controlled by criminal interests. In this sense, the development of mandatory transaction reporting systems to complement or replace STRs would be necessary.

In conclusion, this chapter underscores that combating financial crime requires not just technological innovation but also a commitment to transparency and equity in regulatory enforcement. By replacing opaque, politicised 'blacklists' with verifiable secrecy metrics, our framework advances a more just and effective AML ecosystem. The road ahead demands collaboration across academia, industry, and policy-, and lawmakers to refine risk tools, close data gaps, and ultimately disrupt the

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

financial architectures that enable IFFs. The promise of this approach lies not only in its analytical rigour but in its potential to reshape AML into a system that is as adaptive and resilient as the threats it seeks to counter.

REFERENCES

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2023) The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*, 36, pp.615–650. https://doi.org/10.1057/s41284-022-00356-z (Accessed 9 September 2025).

Aldama-Navarrete, D. (2021) Dark banking? Banks and illicit deposit flows, Federal Reserve Bank of Richmond. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811752 (Accessed 8 July 2025).

Alexandre, C. R., & Balsa, J. (2023) Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, **217**, 119500.

Ates, L., Knobel, A., Lorenzo, F., & Meinzer, M. (2025a) Competition and complementarity of EU and FATF beneficial ownership transparency orders. In I. J. Mosquera Valderrama, F. Heitmüller, J. Chaisse, & A. Christians, eds., *Redefining Global Governance*, Cham: Springer Nature Switzerland, pp.85–96.

Ates, L., Knobel, A., Lorenzo, F., & Meinzer, M. (2025b) The transnational legal ordering of beneficial ownership registration. *Transnational Legal Theory*, **16**, 451–476. www.tandfonline.com/doi/abs/10.1080/20414005.2025.2471184 (Accessed 8 July 2025).

AUSTRAC & Australian Government (2020) *Assessing ML-TF Risk*. www.austrac.gov.au/sites/default/files/2020-08/AUSTRAC%20Insights%20-%20Assessing%20-ML-TF%20Risk.pdf (Accessed 8 July 2025).

Becker, W., & Saisana, M. (2018) The JRC Statistical Audit of the Financial Secrecy Index 2018, Joint Research Centre of the European Commission. https://knowledge4policy.ec.europa.eu/sites/default/files/jrc_statistical_audit_of_the_financial_secrecy_index_2018.pdf (Accessed 9 September 2025).

Bello, A. U., & Harvey, J. (2017) From a risk-based to an uncertainty-based approach to anti-money laundering compliance. *Security Journal*, **30**(1), 24–38.

Borlini, L., & Montanaro, F. (2017) The evolution of the EU law against criminal finance: the 'hardening' of FATF standards within the EU. *Georgetown Journal of International Law*, **48** (4), 1009–1062.

Boyer, P. C., & Kempf, H. (2020) Regulatory arbitrage and the efficiency of banking regulation. *Journal of Financial Intermediation*, **41**, 100765.

Cardao-Pito, T. (2022) An embezzler test for norms, standards and regulations. *Journal of Financial Crime*, **29**(3), 878–889.

Cassetta, A., Pauselli, C., Rizzica, L., & Tonello, M. (2014) *Exploring Flows to Tax Havens Through Means of a Gravity Model: Evidence from Italy* (No. 236), Rome. https://papers.ssrn.com/abstract=2575647 (Accessed 8 July 2025).

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018) Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, **57**(2), 245–285.

Cobham, A., Janský, P., & Meinzer, M. (2015) The Financial Secrecy Index: shedding new light on the geography of secrecy. *Economic Geography*, **91**(3), 281–303.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Cusack, J. (2022, January 2) Financial Crime Bank Fines in the 21st Century. *Financial Crime News*. http://thefinancialcrimenews.com/financial-crime-bank-fines-in-the-21st-century-by-fcn/ (Accessed 8 July 2025).

Dalla Pellegrina, L., & Masciandaro, D. (2009) The risk-based approach in the new European anti-money laundering legislation: a law and economics view. *Review of Law and Economics*, **5**(2), 931–952.

de Koker, L. (2009) Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance. *Journal of Financial Crime*, **16**(4), 334–352.

de Koker, L. (2024) Editorial: FATF greylisting: time to revisit the approach. *Journal of Money Laundering Control*, **27**(4), 621–624.

Dean, S., & Waris, A. (2021) Ten truths about tax havens: inclusion and the 'Liberia' problem. *Emory Law Journal*, **70**(7). https://papers.ssrn.com/abstract=3822421 (Accessed 8 July 2025).

Dolar, B., & Shughart, W. F. (2011) Enforcement of the USA Patriot Act's anti-money laundering provisions: have regulators followed a risk-based approach? *Global Finance Journal*, **22**(1), 19–31.

ECORYS (2021) *Monitoring the amount of wealth hidden by individuals in international financial centres and impact of recent internationally agreed standards on tax transparency on the fight against tax evasion*, Brussels: European Commission DG TAXUD.

European Banking Authority (2021) Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/84. www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20–ML%20TF%20Risk%20Factors.pdf (Accessed 8 July 2025).

European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Pub. L. No. COM/2021/420 final (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420 (Accessed 8 July 2025).

European Commission (2022, October 27) Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554 (Accessed 8 July 2025).

European Council (2024, May 30) Anti-money laundering: Council adopts package of rules [Press Release]. www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/ (Accessed 8 July 2025).

European Parliament. (2023). *Lessons learnt from the Pandora Papers and other revelations* (Resolution No. P9_TA (2023)0249), Brussels, Belgium. www.europarl.europa.eu/doceo/document/TA-9-2023-0249_EN.pdf (Accessed 8 July 2025).

European Parliament and Council. (2024a) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), 2015/849. http://data.europa.eu/eli/dir/2015/849/2021-06-30/eng (Accessed 8 July 2025).

European Parliament and Council (2024b) Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

system for the purposes of money laundering or terrorist financing (Text with EEA relevance). http://data.europa.eu/eli/reg/2024/1624/oj/eng (Accessed 9 September 2025).
European Parliament and Council (2024c) Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2024/1620/oj (Accessed 8 July 2025).
European Union (2023) High risk third countries and the international context content of anti-money laundering and countering the financing of terrorism. https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en (Accessed 23 April 2026).
EUROPOL (2017) *From Suspicion to Action: Converting financial intelligence into greater operational impact*, EU. www.europol.europa.eu/cms/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf (Accessed 8 July 2025).
EUROPOL (2021) *Shadow Money: The International Networks of Illicit Finance*, EU. www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf (Accessed 8 July 2025).
FATF (1990) *The Forty Recommendations of the Financial Action Task Force on Money Laundering*, Paris: Financial Action Task Force (FATF). www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html (Accessed 8 July 2025).
FATF (2012) *The FATF Recommendations: International standards on combating money laundering and the financing of terrorism & proliferation*, Paris, France: Financial Action Task Force (FATF). www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (Accessed 8 July 2025).
FATF (2013) *National Money Laundering and Terrorist Financing Risk Assessment*, Financial Action Task Force (FATF). www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf (Accessed 8 July 2025).
FATF (2019) Anti-money laundering and counter-terrorist financing measures Turkey Mutual Evaluation Report. www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-Turkey-2019.pdf (Accessed 8 July 2025).
FATF (2024) FATF's assessment of the United States. www.fatf-gafi.org/en/countries/detail/United-States.html (Accessed 8 July 2025).
FATF (n.d.) FATF's assessment of Luxembourg. www.fatf-gafi.org/en/countries/detail/Luxembourg.html (Accessed 8 July 2025).
FATF-GAFI (2016) *Anti-money laundering and counter-terrorist financing measures – United States*, Fourth Round Mutual Evaluation Report, FATF, Paris (Accessed 8 July 2025).
FATF-GAFI (2022, April) Report on the State of Effectiveness and Compliance with the FATF Standards. www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html (Accessed 8 July 2025).
FATF-GAFI (2023, February) 'Black and grey' lists. www.fatf-gafi.org/en/countries/black-and-grey-lists.html (Accessed 8 July 2025).
F AT F (2003) *Financial Action Task Force on Money Laundering. The Forty Recommendations*. www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf (Accessed 8 July 2025).
FATF (2007) *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures*, FATF. www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html (Accessed 8 July 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

FATF (2013) *National Money Laundering and Terrorist Financing Risk Assessment*, FATF. www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf (Accessed 8 July 2025).

FATF (2022) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (2012 – Updated 2025)*, Paris. www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (Accessed 8 July 2025).

Ferwerda, J. and Kleemans, E.R. (2019) Estimating money laundering risks: An application to business sectors in the Netherlands, *European Journal on Criminal Policy and Research*, 25(1), pp. 45-62 (Accessed 8 July 2025).

FinCEN (2024) *FinCEN Year in Review for FY 2023*, US Treasury. www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf (Accessed 8 July 2025).

García Fresno, M. (2022) *Analiza, que no es poco: Herramientas para el Análisis de Operaciones de Blanqueo de Capitales y de Financiación del Terrorismo*. Madrid: Fundación Notariado. https://publicaciones.notariado.org/p/-papel-analiza-que-no-es-poco-2 (Accessed 8 July 2025).

Grondona, V., Meinzer, M., Monkam, N., Schultz, A., & Villanueva, G. (2025) Which money to follow? Evaluating country-specific vulnerabilities to illicit financial flows. *European Journal on Criminal Policy and Research*, **31**, 667–693. doi:10.1007/s10610-024-09610-z (Accessed 8 July 2025).

Halliday, T. C., & Shaffer, G. (Eds.). (2015) *Transnational Legal Orders*, Cambridge: Cambridge University Press. doi:10.1017/CBO9781107707092 (8 July 2025).

Hopkins, M., & Shelton, N. (2019) Identifying money laundering risk in the United Kingdom: observations from national risk assessments and a proposed alternative methodology. *European Journal on Criminal Policy and Research*, **25**(1), 63–82.

Houston, J. F., Lin, C., & Ma, Y. (2012) Regulatory arbitrage and international bank flows. *The Journal of Finance*, **67**(5), 1845–1895.

ICIJ (2020, September 20) Explore the FinCEN Files data. www.icij.org/investigations/fincen-files/explore-the-fincen-files-data/ (Accessed 8 July 2025).

Jackson, G., Markevych, M., Bardin, Pierre, … Thomas, I. (2023) *Nordic-Baltic Regional Technical Assistance Report. Financial Flows Analysis, AML/CFT Supervision, and Financial Stability*, Washington, DC: International Monetary Fund (IMF). www.imf.org/-/media/Files/Publications/CR/2023/English/1EUREA2023003.ashx (Accessed 8 July 2025).

Janský, P., Meinzer, M., & Palanský, M. (2022) Is Panama really your tax haven? Secrecy jurisdictions and the countries they harm. *Regulation & Governance*, **16**(3), 673–704.

Jensen, R. I. T., & Iosifidis, A. (2023) Fighting money laundering with statistics and machine learning. *IEEE Access*, **11**, 8889–8903.

Lando, S., & Landry, M. (2023) The production and use of financial intelligence to counter terrorism and terrorist financing. In C. A. El Khoury, ed., *Countering the Financing of Terrorism*. International Monetary Fund. pp.63-88. www.elibrary.imf.org/display/book/9798400204654/CH003.xml (Accessed 8 July 2025).

Lannoo, K., & Parlour, R. (2021) *Anti-Money Laundering in the EU – CEPS*. Brussels: CEPS. www.ceps.eu/ceps-publications/anti-money-laundering-in-the-eu/ (Accessed 8 July 2025).

Lebid, O., & Veits, O. (2020) Search for statistically approved criteria for identifying money laundering risk. *Banks and Bank Systems*, **15**(4), 150–163.

Levi, M., Reuter, P., & Halliday, T. (2018) Can the AML system be evaluated without better data? *Crime, Law and Social Change*, **69**(2), 307–328.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Meinzer, M. (2016) Towards a common yardstick to identify tax havens and to facilitate reform. In T. Rixen & P. Dietsch, eds., *Global Tax Governance: What is Wrong with it, and How to Fix it*. Colchester: ECPR Press, pp. 255–288.

Meinzer, M., & Harari, M. (2023, June 13) Transforming our flagship indexes to be even more responsive and timely. https://taxjustice.net/2023/06/13/transforming-our-flagship-indexes-to-be-even-more-responsive-and-timely/ (Accessed 8 July 2025).

Meinzer, M., Harari, M., Lorenzo, F., & Knobel, A. (2023) Comparative report on SWIFT data in the EU27. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4346192 (Accessed 8 July 2025).

Ministerio de Hacienda y Función Pública (2023) Orden HFP/115/2023, de 9 de febrero, por la que se determinan los países y territorios, así como los regímenes fiscales perjudiciales, que tienen la consideración de jurisdicciones no cooperativas, HFP/115/2023. www.boe.es/buscar/act.php?id=BOE-A-2023-3508 (Accessed 8 July 2025).

Nduka, B., Okenyebuno, E., & Sechap, G. (2021) Refocusing designated non-financial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance. *Journal of Money Laundering Control*, **24**(4), 693–711.

Ogbeide, H., Thomson, M. E., Gonul, M. S., Onkal, D., Bhowmick, S., & Bello, A. U. (2024) Rethinking experts' perceptions in money laundering risk assessment. *European Journal on Criminal Policy and Research*, **31**, 753–777. doi:10.1007/s10610-024-09586-w (Accessed 8 July 2025).

Ogbeide, H., Thomson, M. E., Gonul, M. S., Pollock, A. C., Bhowmick, S., & Bello, A. U. (2023) The anti-money laundering risk assessment: A probabilistic approach. *Journal of Business Research*, **162**, 113820.

Omar, N., & Johari, Z. A. (2015) An international analysis of FATF recommendations and compliance by DNFBPS. *Procedia Economics and Finance*, **28**, 14–23.

Panevski, D., Peráček, T., Rentková, K. (2021) Analysis of the Practices of Financial Intelligence Units (FIUs) and Other Anti-money Laundering Agencies Within EU. In Kryvinska, N., Poniszewska-Marańda, A. (eds) *Developments in Information & Knowledge Management for Business Applications*. Studies in Systems, Decision and Control, vol 376. Springer, Cham.

Ping, H. (2005) The suspicious transactions reporting system. *Journal of Money Laundering Control*, 8(3), 252–259.

Reuter, P., & Riccardi, M. (2024) Introduction to special issue on 'understanding money laundering: empirical and theoretical insights into offenders, typologies, and determinants of criminal behaviour'. *European Journal on Criminal Policy and Research*, **30**(3), 327–332.

Riccardi, M., & Reuter, P. (2024) The varieties of money laundering and the determinants of offender choices. *European Journal on Criminal Policy and Research*, **30**(3), 333–358.

Richardson, B., Williams, D., & Mikkelsen, D. (2019) *Network analytics and the fight against money laundering*, McKinsey. www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering (Accessed 8 July 2025).

Ross, S., & Hannan, M. (2007) Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, **10**(1), 106–115.

Sachoulidou, A. (2023) Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. doi:10.1007/s10506-023-09347-w (Accessed 8 July 2025).

Sathye, M., & Islam, J. (2011) Adopting a risk-based approach to AMLCTF compliance: the Australian case. *Journal of Financial Crime*, **18**(2), 169–182.

Savona, E. U., Riccardi, M., Shelton, N., & Kleemans, E. R. (2017) Assessing the risk of money laundering in Europe: final report of project IARM. www.academia.edu/33455865/

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Assessing_the_Risk_of_Money_Laundering_in_Europe_Final_Report_of_Project_IARM (Accessed 8 July 2025).
Sciurba, M. (2018) The heart of know your customer requirements: the discriminatory effect of AML and CTF policies in times of counter-terrorism in the UK. *European Journal of Crime, Criminal Law and Criminal Justice*, **26**(3), 222–235.
Sharman, J. C. (2010) Dysfunctional policy transfer in national tax blacklists. *Governance*, **23** (4), 623–639.
Shiel, F., & Starkman, D. (2020, September 19) About the FinCEN Files investigation – ICIJ. *International Consortium of Investigative Journalists (ICIJ)*. www.icij.org/investigations/fincen-files/about-the-fincen-files-investigation/ (Accessed 8 July 2025).
Singh, K., & Best, P. (2019). Anti-money laundering: using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, **34**, 100418.
Takáts, E. (2007). *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement*. Washington, DC: International Monetary Fund. www.imf.org/-/media/Websites/IMF/imported-full-text-pdf/external/pubs/ft/wp/2007/_wp0781.ashx (Accessed 8 July 2025).
Tax Justice Network (2025, June 3) Financial Secrecy Index: The world's biggest enablers of financial secrecy. https://fsi.taxjustice.net/ (Accessed 9 September 2025).
Turksen, U., Benson, V., & Adamyk, B. (2024) Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*, **25**, 359–377. doi:10.1057/s41261-024-00233-2 (Accessed 8 July 2025).
Unger, B. (2023) *Reforming EU blacklisting: how to increase the effectiveness and avoid politicisation of the EU list of high-risk jurisdictions for anti-money laundering and counter-terrorism financing: US experience and considerations for EU reform*, European Parliament Committee on Economic and Monetary Affairs (ECON). www.europarl.europa.eu/RegData/etudes/STUD/2023/740091/IPOL_STU(2023)740091_EN.pdf (Accessed 8 July 2025).
United Nations (n.d.) goAML: Anti-Money Laundering System. https://unite.un.org/goaml/ (Accessed 8 July 2025).
US Congress (2024) United States Code, 2018 Edition, Supplement 5, Title 31 – MONEY AND FINANCE, 31 USC 310 (2024). www.govinfo.gov/app/details/USCODE-2023-title31/USCODE-2023-title31-subtitleI-chap3-subchapI-sec310 (Accessed 8 July 2025).
Vedrenne, G. (2023, November 22) STR volumes rise again in Europe, Finland notwithstanding. *ACAMS Moneylaundering.Com*. www.moneylaundering.com/news/str-volumes-rise-again-in-europe-finland-notwithstanding/ (Accessed 8 July 2025).
Xue, Y.-W., & Zhang, Y.-H. (2016) Research on money laundering risk assessment of customers: based on the empirical research of China. *Journal of Money Laundering Control*, **19**(3), 249–263.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4

Use of AI in Law Enforcement: The Present and Future Prospects

Joachim Klerx, Lukas Vilim, Stefan Hopf, Thea Sogenbits and Umut Turksen

4.1 INTRODUCTION

AI has the potential to transform policing by performing certain tasks much faster than humans can, thereby giving the law enforcement agencies (LEAs) a critical advantage against criminals and pave the way for efficient, responsive and effective law enforcement at significant scale. Such tasks can include integration (Sarzaeim et al., 2023) and analysis of complex data sets (IBM, 2023) (e.g., illicit money flows, Suspicious Transaction Reports (STRs), electronic communications, images and video, etc.); prioritisation of most pressing threats and risks (Sarzaeim et al., 2023); translation of large documents; development of secure communication channels; and training platforms.

For the LEAs, in particular, any AI tool shall be underpinned by relevant legal provisions pertaining to data bias, fairness, and potential threats on privacy, data security, accountability, human rights protection and discrimination, to name a few. When the possibility of criminal conviction thus the depravation of liberty as a consequence increases, so should safeguards and principles if an AI is used in the criminal justice system. While plethora of studies have been conducted on the interrelation between predictive policing (Sarzaeim et al., 2023; European Council, 2024), AI and fundamental human rights (Council of Europe, n.d.) as well as the effects of AI on policing organisations (Sarzaeim et al., 2023), this chapter focuses on the use of AI in the investigation stage of policing where the crime in question has gone beyond mere suspicion and there is enough evidence to conduct the investigation and start procedures for seizure and confiscation of illicit proceeds of crime.

Accordingly, we focus on key potential areas of AI deployment that are relevant in several use cases, then present our horizon scanning results on AI tools for LEAs (what these tools can be in the future).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.2 USER REQUIREMENTS

The implementation of AI-supported and other new technological tools for investigation of financial crime is not straightforward. This is partly because LEAs often lack the necessary skills, appropriate basic training or further education (Dewald, 2022). Furthermore, LEAs often lack organisational capacities, such as legal, technical and financial resources to implement such tools easily and effectively (Tombul and Cakar, 2015).

In the TRACE project, the assessment of user and organisational needs for the implementation and use of AI-supported and other new technological tools for tracing illicit money flows (IMFs) was carried out via a mixed methods approach, including a quantitative survey, qualitative interviews and focus groups with employees of various law enforcement and judicial agencies. For the quantitative survey, a total of forty-two employees of various law enforcement agencies were contacted via an online questionnaire. Respondents were asked about their experiences in the tracing of IMFs, the usefulness and added value of digital investigation software in this context, and the challenges of cross-border police cooperation and information sharing. Table 4.1 provides an overview of the composition of the sample, which included eleven supervisors and thirty-one investigators with an average seniority of fourteen years.

For the qualitative data collection, a total of eight individual interviews were conducted with LEA personnel from Austria, Italy, Czech Republic, Germany,

TABLE 4.1 *Overview of quantitative sample*

Country	N	Unit	N
Austria	1	AML/CFT Supervision Unit	1
Belgium	4	Anti Terrorism Financing	2
Cyprus	1	Anti-Fraud	1
Czech Republic	7	Asset recovery	1
Estonia	3	Counter Terrorism	4
France	1	Cybercrime	2
Germany	6	Economic and Financial Crime	10
Guernsey	1	Financing terrorism/money laundering	1
Luxembourg	1	FIU	1
Netherlands	2	Internal affairs	1
Portugal	1	International Tax	1
United Kingdom	3	HMRC-Criminal Investigation	2
United States	4	Money laundering & Economic Crime	2
		Organised Crime	3
		Organised Crime & Economic Crime	1
		Tax Crime	2
n.a.	7	n.a.	7
Total			42

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Estonia, and two members of staff from international organisations, Europol and Eurojust. Interviewees were mid-level LEA/judicial staff who were still involved in investigations/prosecutions as senior officials, and as such were also taking on strategic and management functions. The participants had expertise in investigating organised crime, cybercrime, and economic and financial crime. These interviews were supplemented by one focus group with five employees of different Estonian law enforcement agencies. In a second data collection and evaluation phase, two workshops were conducted. In contrast to the initial interviews and focus group, these meetings primarily served to revisit, evaluate and refine the findings. These workshops involved nine participants (from Italy, the Czech Republic, Austria, and Spain). Table 4.2 provides an overview of the sample.

The following section provides the results of these two approaches. The results of the questionnaire are intended to show broad patterns of user needs, which are then fleshed out with more detailed accounts from the interviews. Regarding the quantitative sample size, a brief note is warranted. Although a sample size of forty-two is in principle very small, N 42 is reasonable considering that the sample includes qualified and experienced representatives of LEAs and thus organisational perspectives.

4.2.1 *Findings*

The challenge in tracing IMFs starts with the fact that most types of (organised) crime encompass illicit transactions. According to the responses, the scope of crimes ranges from money laundering and tax fraud to drugs, arms and human trafficking, to insurance fraud, espionage and kidnapping. Table 4.3 provides the respective overview. An understanding of this relation is important for the collection of user needs and the design of investigative tools, because even though there are, irrespective of the specific crime, some general investigative practices and tactics, different types of crime require different investigative techniques and tools. For example, crimes committed on the internet using crypto currencies demand different skills from investigators and their tools than traditional forms of tax fraud. Likewise, crimes that can be deeply interwoven with and covered up by (supposedly) legal business models make it more difficult to trace and prove the illegality of related money transactions. The situation becomes ever more complicated in cross-national cases as, for example, in the case of tax evasion, national states often differ in their respective legal provisions. This may result in a certain offence being subject to criminal penalties in one jurisdiction, while in another it merely constitutes an administrative offence (European Parliamentary Research Service, 2017).

Another significant challenge that the use of improved and AI-supported software could mitigate is the increased use of modern information and communication technology and cryptocurrencies to organise and commit crime. This development

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 4.2 *Overview of qualitative sample*

Participant Code	Number of Participants	Date	Country	Work experience	Area of expertise
lpl_Po_DE	1	07/02/2022	Germany	over 21 years	Organised Crime
lp2_Po_AT	1	08/03/2022	Austria	over 10 years	Organised Crime Financial & Economic Crime
lp3_Po_AT	1	16/07/2022	Germany	over 15 years	Financial & Economic Crime
lp4_Po_IT	1	19/07/2022	Italy	over 15 years	Organised Crime/Mafia
FGl_PO& Tax_EST	6	13/09/2020	Estonia	between 15 and 30 years	International Cooperation, Tax and Customs Crimes, Organised Crime
lp5_Po_EST	1	14/09/2022	Estonia	over 20 years	Organised Crime
lp6_Po_CZ	1	14/09/2022	Czech Republic	over 15 years	Cybercrime and Organised Crime
lp7_EuPo_EU	1	08/11/2022	EU	over 25 years	European Police Cooperation
lp3_EJ_EU	2	08/11/2022	EU	over 10 years	European Judicial Cooperation
E-FG_1	3	16/06/2023	Estonia, Czech Republic	n.a.	Internal Investigations
E-FG_2	6	18/09/2023	Austria, Italy, Spa in Czech Republic, Estonia	n.a.	Organised Crime, Financial & Economic Crime, Cybercrime, Public Prosecutor, Tax & Custom Crimes

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 4.3 *Types of crime and IMFs*

Crimes typically associated with IMF	Number of times mentioned (N = 41)	Per cent of cases
Money Laundering	40	96%
Tax Fraud	33	79%
Drug Trafficking	33	79%
Corruption/Bribery	32	76%
Bank Fraud	29	69%
Credit Card Fraud	23	56%
Human Trafficking	26	62%
Arms Trafficking	25	61%
Insurance Fraud	16	38%
Espionage	11	26%
Kidnapping	11	26%
Trade Mispricing	9	22%
Others (e.g., bankruptcy, benefit fraud, computer-related fraud, smuggling)	5	11%

poses new obstacles for investigators and has direct impact on their needs and the capabilities of potential tools (World Bank, 2016). To counter this technological-digital upgrade of criminals, LEAs in Europe and beyond are increasingly relying on digital and partly AI -based investigative software (Tombul and Cakar, 2015) as a tool to fight organised and financial crime (Gottschalk and Solli-Saether, 2010). This is also reflected in the responses from our sample. 21 per cent of respondents stated that the use of digital forensic software is 'very important' in cases involving IMFs, and a further 43 per cent indicated that it is 'important'. Consequently, many of the respondents also already use software such as rsCase (rsCase, n.d.), infoZoom (infoZoom, n.d.), Analyst's Notebook (i2 Analyst's Notebook, n.d.) and Cellebrite. (Cellebrite, n.d.). In this respect, 59 per cent of our respondents stated that they use digital forensic software 'very often' or 'often' and a further 26 per cent stated to use it, at least, 'rarely'. Thus, software-assisted investigation is already part of police practice and considered to be an important instrument.

However, as Table 4.4 also shows, a distinction must be made here between the use of general digital forensic software and AI-supported tools. According to the respondents, the latter are used less frequently. Only 21 per cent say that they use AI-based software very often or often, while 36 per cent say that they never use it. In comparison, only one respondent states that they never use simple digital forensic software. One reason for this, as stated by one of the interviewed German officers (Ip1_Po_DE), is the frequent lack of organisational capacity among LEAs to implement such technology. In particular, there is often a lack of appropriate technical infrastructure and investigators with the relevant expertise. According to some respondents, the latter is due to the high level of competition with the private labour

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 4.4 *Frequency of digital or AI-based/supported investigation software usage*

	Frequency of Digital Forensic/Investigation		Frequency of AI-Based/ Supported Software Use	
	N	Percentage	N	Percentage
Very Often	8	19	3	7
Often	17	40	6	14
Rare	11	26	8	19
Never	1	2	15	36
n.a.	5	12	10	24
Total	42	100	42	100

market, where IT specialists often find a significantly better remuneration scheme. This lack of technological and personnel capacity is especially evident, in the context of tracking IMFs involving cryptocurrencies. Almost all of the interviewed officers agreed that this is practically impossible at present and is usually not done, because the necessary technology and personnel expertise to do so is lacking.

Having established the context in which digital and an AI-based forensic investigation software are helpful and the frequency with which the software are already used, we will now address the specific user needs. Firstly, we identified the specific tasks for which improved software, potentially supported by AI, is perceived to improve workflows. Here, respondents primarily saw a need for software solutions that would improve automatic data and document extraction (68 per cent), data sorting (62 per cent), efficient term search and the extraction of names, phone numbers, bank details, all of which are functions and features that can already be successfully performed by powerful artificial intelligences. About half of the respondents (51 per cent) stated that improved software for exchanging information with other LEAs (across borders) would benefit their work. However, the results of the qualitative interviews also point to the risks of additional information exchange technology, as some participants reported that LEAs are already 'flooded' with information they received through the various EU-wide police information networks (Ip1_Po_DE). Hence, some participants argued that more important than new software would be a centralisation of existing communication channels (Ip4_Po_IT, Ip6_Po_CZ). The least important tasks for new software solutions are the linkage of information and knowledge between different parts of the organisation (44 per cent), linking data between different data bases (i.e., connecting silo-knowledge; 30 per cent) and the automatic authentication of documents (11 per cent).

Overall, the result of our study points out that LEAs particularly welcome special programmes for tasks that are becoming increasingly time-consuming and laborious due to the significant increase in data volumes. As demonstrated in Figure 4.1, fewer

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

respondents (51 per cent) regard analytical tasks, such as establishing links between suspect networks as important. One reason for this could be that analytical skills are considered to be the core competence of investigators. Therefore, outsourcing them to a 'machine' may be viewed with reservation (Gottschalk, 2010). However, in the interviews some participants suggested that (partially) automated pattern and relationship analysis ('connecting the dots: accounts, people, places' Ip2_Po_AT) software might be interesting for tracking and processing cash flows/financial flows.

A further area where improved technology is necessary, and which emerged in the interviews, is the encryption and decryption of communication technology. Here, participants reported an imbalance between the police and organised crime groups, with the latter having increased expertise in the protection (i.e., encryption) of their means of communication. For example, one of the German officers (Ip1_Po_De) mentioned that due to the market-driven competition between providers of encryption and decryption software, progress is extremely rapid. While before implementation LEAs have to go through security checks of such new software and more comprehensive set up and test phases, criminal organisations would adapt more quickly. As a result, LEAs would often lag behind technological developments. Another problem associated with communication technology is that, especially for cross-border cooperation, no communication tools are available that are suitable for everyday investigation work. Thus, according to the interviewees, investigators use applications like WhatsApp to informally and quickly share information relevant to operations and investigations.

To further differentiate the analysis, we compared differences in user needs according to different user groups. Therefore, we distinguished between 'frequent users' and 'non-users' based on the data on the frequency of use of digital forensic investigation software (Table 4.4, column 1). 'Frequent users' are participants who use digital forensic programs 'very often' or 'often', 'non-users' use such software

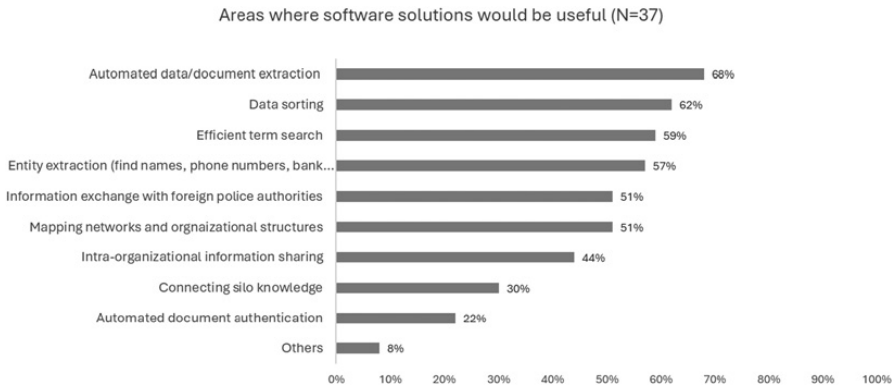

FIGURE 4.1 Work tasks requiring improved software solution.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

'rarely' or 'never'. The results primarily show overlaps in user needs between these two groups. Figure 4.2 and Figure 4.3 provide an overview. The most important user need for both groups is general usability (i.e., how smoothly and quickly the programme works and how efficiently tasks can be completed with it). The high priority given to usability is also illustrated by the high ranking of characteristics that we measured to substantiate the concept of usability (e.g., that the programmes should be self-explanatory, should have a simple interface design and should be accessible for IT novices). Less important for the respondents is that programmes have a wide range of functions, that they can be used across platforms, and/or are web-based applications.

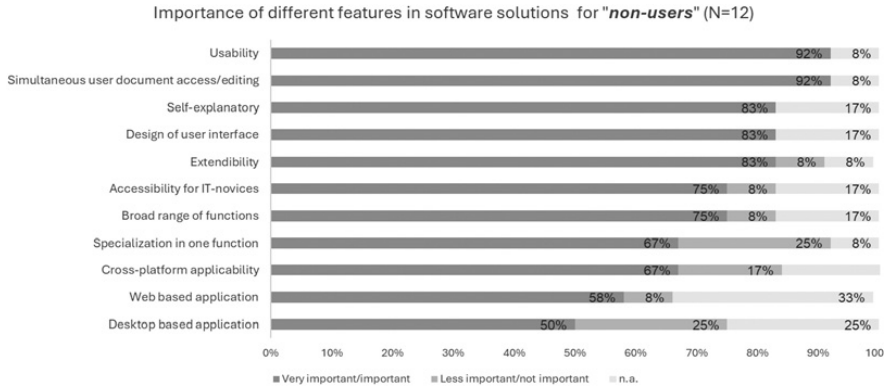

FIGURE 4.2 User needs of 'non-users'.

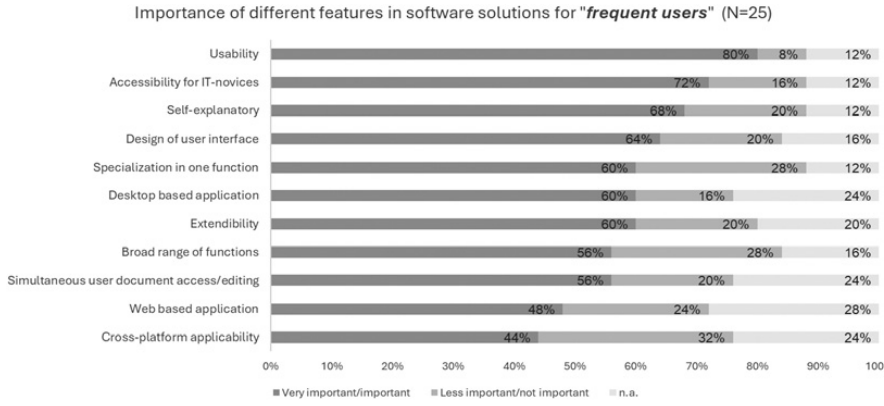

FIGURE 4.3 User needs of 'frequent users'.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Looking at the differences between the two groups, it is important to highlight that our analysis is purely descriptive. Therefore, no correlations or reasons can be given with regard to the differences. Nonetheless, we would like to highlight two points. First, that among 'frequent users', accessibility for IT novices is ranked higher than among 'non-users'. One possible reason for this could be that the former, due to their more frequent use, have had more negative experiences with the usability of programmes and, therefore, attach greater importance to low-threshold programmes. Second, the specialisation of programmes ranks higher among 'frequent users' than among 'non-users'. On the one hand, this preference could be related to the fact that programmes with many functions are more difficult to learn to use. On the other hand, this group could also have higher performance expectations for certain programmes. This is typically easier to achieve with specialised programmes.

Overall, the results of our study show that digital forensic software are seen as an important investigative tool and are also used as such. However, AI-supported solutions are rarely used at the national level of policing. One reason for this is the lack of organisational capacities in LEAs, such as insufficient infrastructure or a lack of technological expertise and corresponding training opportunities. More importantly, however, the qualitative data shows that, in terms of technological advancement, there are more pressing needs, such as the improvement decryption and decoding software or the development of internationally useable secure communication software for LEAs. Furthermore, it should not be overlooked that additional technology not only brings advantages, as the information overload mentioned in connection with communication technology shows. In terms of specific user needs, our data shows that investigators prefer software solutions that support targeted and automated data, search, extraction and sorting. Such software solutions should have a high level of usability, that is, be largely self-explanatory in use, have a simple user interface, and be accessible to people with little or no IT experience.

Having established the user needs and requirements, it is important to establish what types of AI tools and information analysis may be useful in financial crime investigations.

4.3 AI APPLICATIONS AND TOOLS IN POLICING

4.3.1 *Definition and Core Concepts of AI*

AI does not have a universally agreed definition. The EU AI Act provides a general and encompassing concept of AI and defines AI system as a software 'that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with' (European Council, 2024). Furthermore, it lists various categories of AI based on the purpose and risks they may pose when deployed.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Despite this relatively new definition of AI, the term AI was first coined by McCarthy in 1955 (Dick, 2019), and a number of commentators asserted that AI refers to 'machines or computers that mimic cognitive functions that humans associate with the human mind, such as learning and problem solving' (Russell and Norvig, 2018). Thus, it is envisaged that the future of this technology will be cognitive, not 'artificial' (Joseph and Turksen, 2022).

AI has been categorised into four types of activity or processes, namely: thinking humanly, acting humanly, thinking rationally, and acting rationally (Russell and Norvig, 2018). It would however not be entirely accurate to define the function of the AI as 'human thinking' because unlike the human cognition and decision-making, all AI systems rely on three essential components: computing capability (hardware), developing advanced algorithms (software), and access to relevant and reliable data to exploit. Currently, all these components are provided by people; thus, an AI system is also reliant on human input in general and in police investigations in particular. The second category of 'the thinking rationally' defines AI as 'the study of the computations that make it possible to perceive, reason, and act' (Charniak and McDermott, 1991) while the acting rationally category defines AI as 'the study of the design of intelligent agents' (Poole, Mackworth and Goebel, 1998).

While the term AI has existed for over fifty years, the access to and convergence of vast datasets (a common feature in cross-border financial crime investigations), powerful hardware and advanced algorithms have made application of AI in various contexts and in high-functioning robotics a reality only in the last decade. Accordingly, AI is categorised by first, second, and third generations. The first generation of AI tools are commonly installed in many devices which we use daily deal with finite number of tasks thus referred to as 'artificial narrow intelligence' (Poole, Mackworth and Goebel, 1998). Voice and face recognition, self-driving or autonomous vehicles are some of the examples of the first-generation AI systems. AI is also used to support several businesses needs inter alia, process automation, cognitive insight, and cognitive engagement (Joseph and Turksen, 2022; Davenport and Ronanki, 2018).

In recent years, we have seen the second-generation of AI, also referred to as 'artificial general intelligence' or AI agents, which are able to reason, plan, and solve problems autonomously for tasks they were never designed for (Gutowska, 2024).

If the AI technology develops at the same pace as it has been doing in the last decade, it is envisaged that there would be the third generation of AI, coined as 'artificial super intelligence', which would consist of self-aware and conscious systems that could, to a certain extent, make human thinking and decision-making redundant. If such technology is materialised, it would have very different characteristics from those attributed to the present AI tools, which inevitably would pose several technological, scientific, legal, ethical and societal challenges and opportunities, with different requirements for governance, policy, and law enforcement (UK Ministry of Defence, 2018). LEAs, therefore, need not only adopt new technologies

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

to counter financial crime but also be aware of emerging criminal activities enabled by AI. Virtually, all financial crimes involve dishonesty and laundering the proceeds of such crimes (NCA, 2025). Accordingly, LEAs need to reveal meaningful details (intelligence) among the multitude layers of legal and illicit activities and analyse complex sets of data in order to see the full picture of organised crimes whereby they can identify suspects (people and entities) as well as their proceeds of crime to seize and recover. Below are some of the examples of contexts (use cases) and methods which LEAs can leverage by utilising AI.

4.3.2 *Examples of Use Cases*

After consultation with several LEAs and in light of Europol's SOCA Report 2021 (EUROPOL, 2021), the following use cases containing various criminal activities and often involving IMFs were considered in regard to the deployment of AI in the investigation of such crimes:

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

These non-exhaustive lists of use cases were designed to be representative, though simplified, versions of potential real-life scenarios involving complex and organised crime schemes involving IMFs and typically entail electronic evidence. It was deemed that AI-driven tools could be deployed for investigating them.

4.3.2.1 Financing of Terrorism

Terrorist organisations operate more and more often in global, non-transparent company networks. To face and untangle these networks, it is necessary to deepen the understanding of the business model, structure, and characteristics of such global actors, to understand supply chains in these networks, to increase essentially corresponding data and to develop effective technical possibilities to link them.

In our use case, 'Financing of terrorism', LEAs look for businesses and financial footprints of terrorist activities. The supply chain networks of global terrorist organisations are typically part of hidden support networks of 'seemingly' legitimate businesses. Typically, four main relevant core services are involved: Financing of political campaigns (political support), financing religious infrastructure (religious support in the form of donations and/or misuse of zakat in the case of Islamic terrorism) (Chugani, 2008; Freeman and Ruehsen, 2013), banking services (external financial support), and media companies (knowledge sources/knowledge support).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Additional services, such as healthcare, travel agencies, or charities and donation are often (at least in a large part) legal networks, whereas essentials – like black markets – are anonymous networks (Council of Europe, n.d.). In particular, terrorist organisations face the challenge of buying illegal goods or selling to finance their racketeering. The 'www' (World Wide Web) has always been one of the most important ways of doing this. However, new technologies (such as blockchain) allow players on black markets and special online shops previously undreamed-of possibilities of fund raising. So, in this use case, LEAs should concentrate (as a first step) on supply chain networks of terrorism.

In this context, AI can offer a way to facilitate the compilation and analysis of the vast amounts of data that would be collected in such a scenario and create a knowledge graph to help identify connections between the primary suspect(s) and any other potentially relevant persons, who can then be investigated further to determine whether they serve a role in the larger organisation. See for an example Figure 4.4.

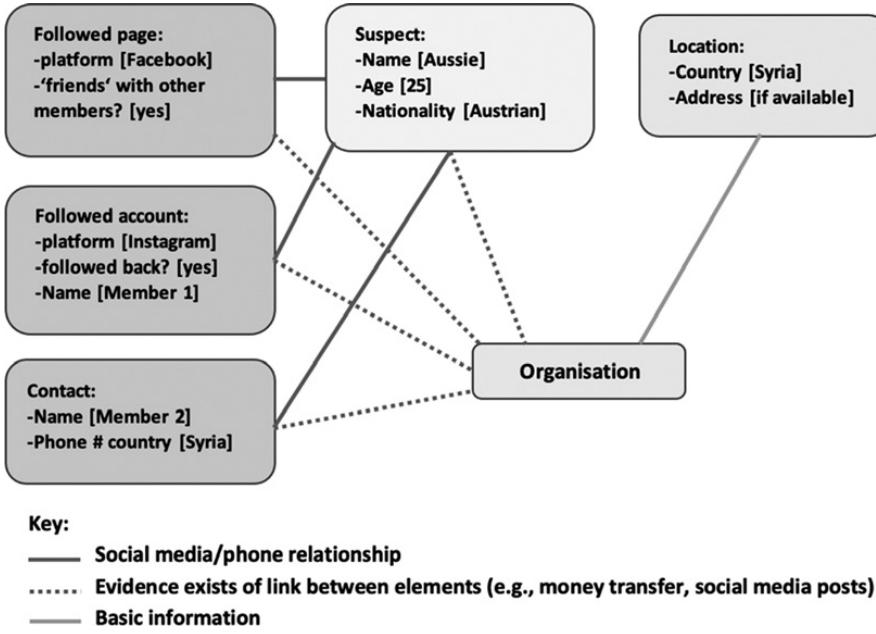

FIGURE 4.4 Example knowledge graph of Financing of Terrorism use case.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.3.2.2 Web Forensics for Tackling Terrorism Investigation

Digital forensics or web forensics is a process used by security analysts and investigators that often involves identifying, extracting, analysing and documenting digital evidence that can be used in investigations and admissible in court proceedings (Cobwebs, 2020). The nature of the work involved in web forensics includes complex and creative solutions and methods that are designed to identify, collate, and present critical information from digital sources, such as computers, smartphones, servers, and networks. Findings from these sources are then analysed for the value chain in investigations and as potentially substantive evidence for the purpose of crime prosecution. These analytics are seen as a useful tool that can help LEAs solve complex cases and trace digital footprints (CEPOL, 2019; Casey, 2011). AI-driven tools can enhance Web Intelligence (WEBINT) and Open-Source Intelligence (OSINT) solutions whereby they can provide Application Programming Interface (API) and/or data scraping from such sources to provide visually and analytically advanced investigation aids.

Many of the activities (financing, recruitment, planning of attacks, etc.) of terrorist organisations take place in the cyber space, thus can have global reach through a variety of online means from social media to dark web forums and sites. They can also receive direct donations and payments from their members or supporters. These new threats thus necessitate new investigative methods designed to collect and analyse the digital data to gather evidence against terrorist organisations and their members (Joseph and Turksen, 2022). Based on previous terrorism investigations, a typical set of data and objects (evidence) can include, inter alia:

- Passwords (e.g., BitLocker recovery key) to be found on another device.
- Communication channels used (analysis according to the following aspects, keyword-based and manually).
- Content hostile to the basic order of freedom and democracy.
- Content related to violent extremism and/or terrorism.
- (Organised) crime related content (Text in Document or Chat, Photos, Videos): weapon trafficking and/or drug dealing.
- Content related to blackmail/extortion.
- Content related to any suspicious activities that may be identified as money laundering activities.
- Content related to involvement in stores, events, concerts, etc.; relevant actors (i.e., keyword-based search for 'Thor's Thunder' and 'Germanica').
- Content related to membership fees.
- Content related to donations.
- Content related to rental, leases or trade with real estate and/or other goods.
- Persons (ordered by frequency of contact, incl. their nicknames, hosted websites, blogs, etc.).
- Organisations/Actors.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

- Financial transaction related content (non-official Agreements on financial matters, bank confirmations, IBANs, Money, CryptoC etc. in files, documents or chats) (FATF, 2019).

It is evident that such a scenario would involve vast amounts of data from a variety of sources that AI tools can help consolidate and analyse for connections and then create a visual representation of those established connections.

4.3.2.3 Property Market Transactions and Money Laundering

The property market has been a popular choice for criminals to invest in and/or to 'clean' their dirty money (Forbes, 2018). A recent EUROPOL (2020) Report confirms that emergence of an economic recession (caused by COVID-19) in the EU may lead to a reduction of prices for certain objects that are particularly favoured by criminal investors, which includes particularly real estate that lends itself to the investment of criminal profits (EUROPOL, 2020). The property and construction sectors have become attractive for money laundering both in terms of investment and as a justification for the movement of funds.

Furthermore, in recent years, we have seen an increased use of crypto currencies in the property market transactions (PwC, 2022). This poses numerous challenges for national economies, crime prevention and investigation as well as money laundering risks driven by serious crimes. For instance, establishing the source and legitimacy of the cryptocurrency funds can be particularly problematic owing to the anonymity and difficulty in tracing cryptocurrency transactions that may use Bitcoins (Bitcoin.org, n.d.), Dash (Dash.org, n.d.), Monero (GetMonero.org, n.d.) or other privacy coins stored in crypto-wallets. It is to be noted that Blockchain is the technology that enables the existence of cryptocurrency. Bitcoin is the name of the best-known cryptocurrency, the one for which blockchain technology was invented (PwC, 2022). Such transactions may not involve formal financial institutions (e.g., banks), establishing the identity of persons and conducting due diligence on them would be an onerous task. Without an analytical tool available to LEAs, investigation and gathering of evidence (e.g., mapping of connections of individuals and transactions) can be an onerous task.

The key features of money laundering in real estate can include:

- Discrepancy between the usual income and wealth of the owner and the property: in some cases, the most expensive properties in the city are owned by individuals with no income or wealth that would allow them to purchase such a property.
- An anonymous owner, as a result of recourse either to a third party or to companies, trusts or similar arrangements.
- A property's underestimated or overvalued price.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

- The indication by a country that there is a risk of money laundering by its citizens in another country (The Law Society, 2020).

All of the above typologies require LEA to analyse various data sets and connections between them.

4.3.2.4 Cyber Extortion

The global costs of the WannaCry cyber-attack have been estimated at £6.5 billion (Acronis, 2025). The cost of ransomware attacks, besides the ransom being paid in Bitcoins to the adversary, caused losses due to lost productivity (Fouche and Solsvik, 2019), the cost of business continuity, restoration of service (often, not only within the attacked entity, but also in the respective supply chain), loss of public confidence and reputation damage, and post-crisis disruption to the normal course of business. To investigate the ransom payments extorted by ransomware and identify ransomware-as -a-service (RaaS), a number of frameworks have been proposed but they rely on analysis of a wide range of data sources including ransomware knowledge base, ransomware removal guides, reports from Counter Threat Units, Incident Responses (IR), and Security Operations Centers (SOC), online forums where victims and researchers post Bitcoin addresses associated with the concerned ransomware; and secondary research databases to name just a few. With the proliferation of heterogeneous data sources as described above, a single platform-agnostic AI tool is needed to automate complex analytical tasks and visually present combined results. A knowledge graph tool such as the one developed by TRACE could enable such analysis and help close the gap in cyber extortion prosecution capabilities.

Once a cyber extortion is completed criminals move their illegal proceeds/funds in a variety of ways (Figure 4.5).

Based on well-known cases of cyber extortion, a number of techniques are identified that can help LEAs in investigating ransomware and, in particular, to identify criminals involved in ransomware attacks.

These may include:

- Analysis of records kept by the cybersecurity team within the victim organisation.
- Profiling criminals by the *modus operandi*.
- Forensic language analysis of the phishing email, the ransomware notice, communications with criminals, etc.
- Identification and attribution of the malware code and exploitation techniques.
- If there's exfiltration of data, trace the repositories (e.g., a google drive).
- OSINT, which includes:
  - Scanning the Dark Web for information about illegitimate business or users.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

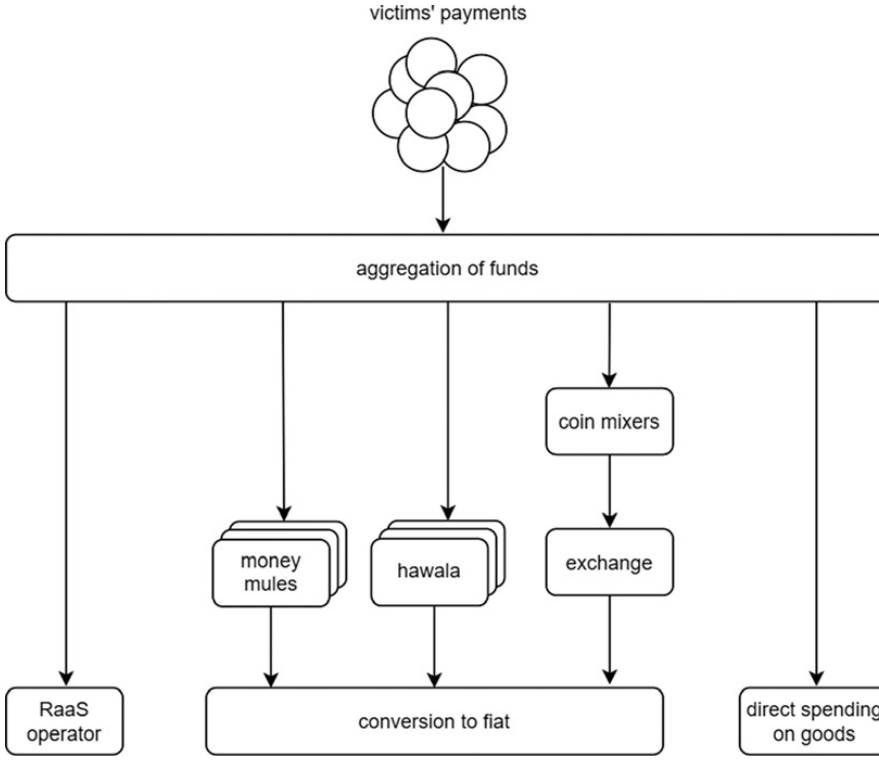

FIGURE 4.5 Ways of movements of illegal proceeds/funds.

- Cross-referencing information to build more complete pictures of the criminal activity.
- On-chain analysis of moving funds (Gertenbach et al., 2024).

While most of these tasks would be conducted by LEAs, the gathered data can be overwhelming for the human eye. Thus, AI can connect the dots (nods of information) and present a workable framework to hone in on perpetrators.

4.3.2.5 Money Laundering with Stolen Art and Antiquities

It is well established that arts and antiquities are used both for terrorist financing and laundering proceeds of crime (European Commission, 2017). It has been argued that the establishment of central databases of all stolen art would strengthen due diligence (Roodt and Benson, 2015), prevention of crime and law enforcement in the art trade, allowing all interested stakeholders to search and verify artworks, which would then lead to a 'fortification' of cultural and artistic

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

heritage against those with nefarious intentions. This is indeed a sensible suggestion, and in fact one that has been in operation for many years in various jurisdictions around the world; most notably the Scotland Yard database that has been in existence since 2008[1] as well as at least eighteen international databases that exist for stolen art (Yates, 2016).

In addition, there are a multitude of international databases that exist, cataloguing the collections of art held around the world, ostensibly within public collections, a prime example of which is the www.ArtUK.org website. In the absence of a national inventory of museum holdings and databases of stolen art and antiquities, law enforcement in respect of stolen art works becomes ever more complicated. Even if such databases of stolen art existed, what is even more challenging is that there is no technological tool to conduct a combined analysis of such art databases against, inter alia, individuals, their residence/s, business connections, money, and asset movements. An AI knowledge graph and/or a similar analytical tool can be used to fill this gap.

4.3.2.6 Online Gambling for Money Laundering

Money laundering through online gambling (Fiedler, 2014) is similar to the standard process of online gambling itself (De Sanctis, 2019). If anything, it is harder to detect because criminals can launder their whole stash through online gambling as a few bets to give a convincing veneer of legitimacy. They would lose only a few percentage points – a better rate than they would have to pay to traditional money launderers. The online gambling market is worth about US $53.7 billion a year (Grand View Research, 2019) and is expected to grow (European Commission, 2012). The following factors make it prone to financial crime including but not limited to fraud and money laundering: (1) virtuality of products; (2) virtuality of cash flows (EUROPOL, 2023); (3) internationality of cash flows; (4) complexity of payment processes; (5) non-harmonised legal frameworks (or legal uncertainty); (6) high pay-out percentages; and (7) tax-free winnings in many jurisdictions, such as Germany (European Council, 2022). The sources of online gambling and the formal headquarters are accumulated in a few tax-friendly legal orders, such as Malta (Fisher et al., 2025), and are formally headed by few specialists. Without an analytical tool available to LEAs, investigation, gathering of evidence (e.g., mapping of connections of individuals and transactions) of gambling proceeds as well as their assets can be an onerous task. AI-driven data analytics and knowledge graphs, which visualise national and EU-cross-border transactions, can address this challenge.

These use cases make it clear that AI tools can be deployed in several contexts in investigation of financial crime and asset recovery. These variety of contexts that are represented in financial crime investigations are further explained in the rest of this chapter.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.3.3 *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 (Browne et al., 2024).

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 (Browne et al., 2024).

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.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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 (Browne et al., 2024).

In addition to OSINT, data analytics can encompass NLP (Sarzaeim et al., 2023) and Large Language Models (LLMs) (IBM, 2023). NLP can be deployed to 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 (2024) 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, and 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 and analysed in complex financial crime cases.

4.3.4 *Cyber and Digital Forensics*

Cyber and digital forensics have existed well before AI became a publicly available tool. However, AI has catapulted the speed and efficiency of data detection, recovery, repair, and analysis. Common applications of AI in this realm include video monitoring, image classification, facial recognition, voice recognition, iris

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

scan, gait analysis, fingerprints, and pattern recognition. For example, an artefact search in a vast dataset of stolen or missing items by AI can take seconds rather hours if a human investigator were to conduct such search. In cases of deepfakes (AI-generated voices and images/videos) whereby criminal impersonate persons to phish personal information and commit fraud and/or spread false information, AI can be deployed to identify the integrity of such actions (Press, 2024). Furthermore, encrypted information, communication and access credentials of criminals can be obtained by advanced predictive capabilities that AI offers (Vurubindi and Narahari, 2024; Hayadi and Haryanto, 2022; Tan et al., 2022). While actual and potential deployments of AI in various contexts continue to expand and evolve (Vurubindi and Narahari, 2024; Hayadi and Haryanto, 2022; Tan et al., 2022) what has become clear is that for any AI to operate effectively and produce reliable results, it needs to have reliable and relevant data. Equally important is the fact that AI needs to be used according to fundamental legal and ethical safeguards. Without this integrity of policing, the use of AI in policing is dented. In Chapters 2, 5, and 8 of this book, ethical and legal standards that shall inform the use of AI are articulated in detail. Nevertheless, it is worth briefly mentioning these here.

4.4 SAFEGUARDS IN POLICING WITH AI

Data Privacy and Civil Liberties: One of the primary concerns surrounding AI in law enforcement is the potential for violations of privacy and civil liberties. AI systems rely heavily on data collection, raising questions about how this data is gathered, stored, and used. Without strict safeguards, there is a risk that surveillance technologies could infringe upon individuals' rights, leading to unwarranted scrutiny or profiling.

Algorithmic Bias and Fairness: AI algorithms are only as unbiased as the data used to train them. If historical data contains biases – whether related to race, gender, or socio-economic status – AI systems can perpetuate and even amplify these biases. This could lead to disproportionate targeting of certain communities, undermining public trust in law enforcement.

Complexity and Lack of Transparency: The complexity of AI systems can make it difficult for users to understand how decisions are reached. This 'black box' problem raises concerns about accountability, as officers may rely on AI-driven recommendations without fully understanding the underlying logic. Ensuring transparency in AI algorithms is crucial for maintaining trust and accountability.

Over-Reliance on Technology: While AI can enhance decision-making, over-reliance on technology could diminish critical thinking and investigative skills among officers. It is essential to strike a balance between human judgement and technological assistance, ensuring that AI serves as a tool rather than a replacement for law enforcement expertise.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Cybersecurity Threats: AI systems themselves can become targets for cyberattacks. Hackers could manipulate AI algorithms, corrupt datasets, or disable critical systems, compromising investigations and endangering public safety. Robust cybersecurity measures are essential to protect AI-powered platforms from malicious interference.

Legal and Ethical Uncertainty: The rapid advancement of AI technologies often outpaces the development of legal frameworks and ethical guidelines. Law enforcement agencies must navigate a complex landscape of regulations while ensuring that AI-driven practices align with fundamental rights and the rule of law.

By striking the right balance between innovation and responsibility, law enforcement agencies can harness the full potential of AI while maintaining public trust and accountability. As the TRACE project demonstrated (Sachoulidou et al., 2024) collaborative efforts, continuous evaluation, and adherence to ethical principles are key to ensuring that AI becomes a powerful ally in the pursuit of justice and safety.

4.5 FUTURE PROSPECTS AND EMERGING TRENDS

The current possibilities of the use of AI in policing are discussed above. As AI is a fast-evolving technology, it is also important to consider its potential future applications. Our horizon scanning has provided the following roadmap (Figure 4.6), summarising the state of the art and future scenarios including 2026 (near future), 2030–2035 (mid-term), and 2040 and beyond (long term). This roadmap synthesises the insights gathered from various sources, including publication data, internet data, and community detection analyses, to present a holistic view of the future of AI in countering financial crime in general and money laundering in particular. It anticipates the integration of emerging technologies, the refinement of algorithms, and the strengthening of global cooperation, setting the stage for a more effective and intelligent approach to policing and countering financial crime.

The roadmap contains six different knowledge objects:

Weak Signals: These are subtle, early indicators of potential changes or emerging trends that are not yet widely recognised or understood. Weak signals are often overlooked but can be harbingers of significant shifts in social behaviour, economic patterns, or technological advancements. These weak signals could indicate changes in trends, disruptive events, threats or innovation (European Union, 2024).

Trends: Trends are patterns or shifts in behaviour, attitudes, or conditions that develop over time and point to a general direction in which a particular aspect of society, technology, or the market is moving.

Disruptive Events: Disruptive events are occurrences that significantly alter the status quo or even a system change. These can be sudden and unexpected, causing a major impact on societies, economies, or ecosystems, and they often require substantial adaptation or response.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

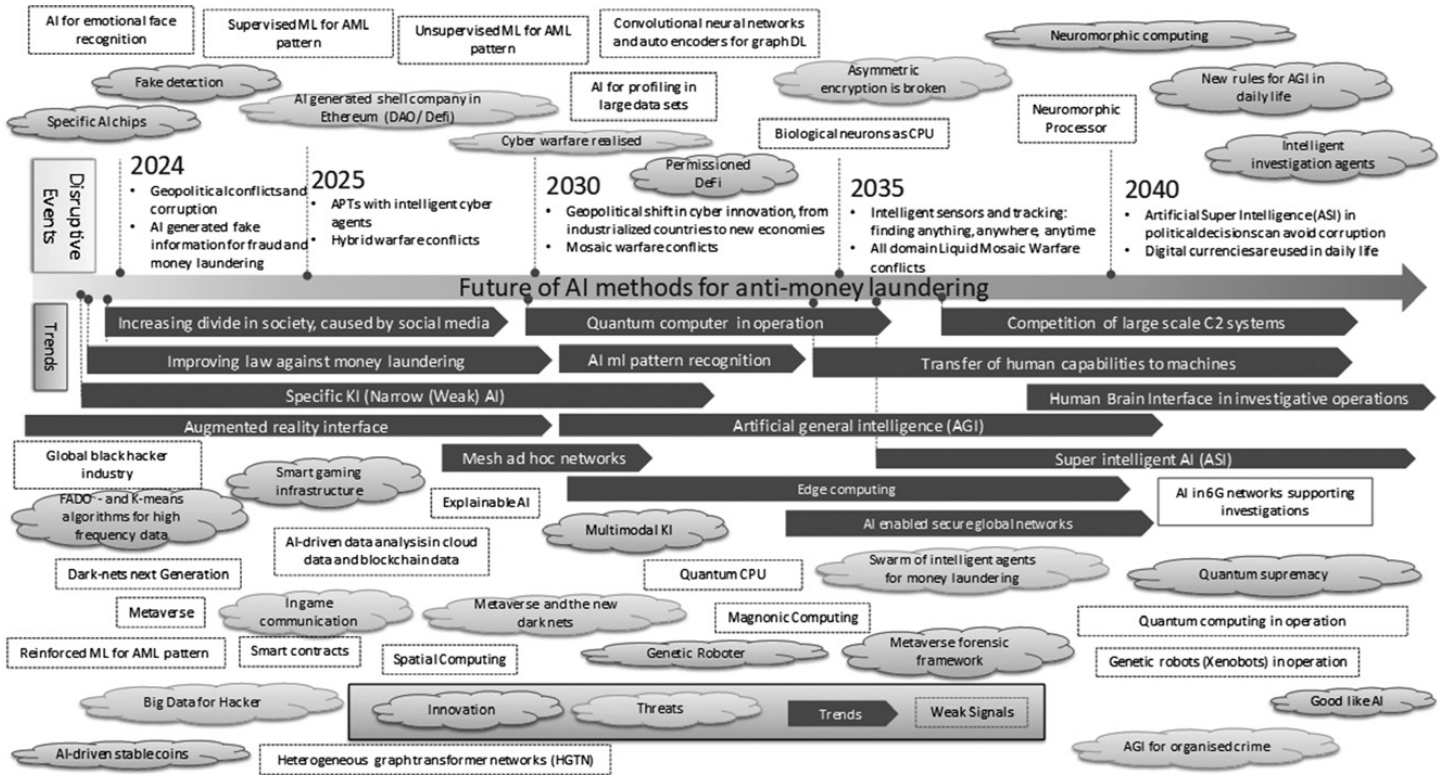

FIGURE 4.6 Roadmap of future AI developments to counter financial crime.
Source: Authors' compilation.

Threats: Threats are factors or circumstances that have the potential to cause harm or adverse effects. In the context of financial crime, these are perceived challenges or dangers that could undermine performance, stability, integrity of the economy and/or particular sectors that are important in a given economy.

Innovation: Innovation refers to the creation or adoption of new ideas, methods, products, or services in the context of countering financial crime. It involves thinking creatively and differently to develop solutions that are novel and effective, often improving efficiency, solving problems, or meeting the needs of individuals or organisation.

Below is the explanation of the roadmap in different time periods.

4.5.1 *The State of the Art: 2025*

4.5.1.1 Weak Signals

AI for Emotional Face Recognition: This technology signifies a subtle yet growing interest in enhancing AI's understanding of human emotions through facial cues. As a weak signal, its potential use in AML could be groundbreaking. It might enable systems to detect suspicious behaviours or stress during transactions, which are often subtle indicators of fraudulent activities. However, its emergence could raise ethical questions about privacy and consent and will most likely not be accepted within the EU if the AI tools are not in compliance with the AI Act (European Union, 2024).

Global Black Hacker Industry: The rise of a sophisticated hacker industry, working on a global scale for profit and power reflection, represents a weak signal with significant implications for financial crime. This burgeoning shadow industry can pioneer methods to circumvent traditional security measures, necessitating advanced AI tools for early detection and prevention of such threats in financial transactions. State-sponsored hacker groups have been involved in every recent conflict (CSIS, 2024; UK National Cyber Security Centre, 2024) and are becoming more professional and more powerful.

4.5.1.2 Trends

Augmented Reality Interface: AR interfaces are increasingly attracting public attention, transforming user interaction with digital systems. In AML, such interfaces could enable investigators to visualise complex transaction networks or to identify risks within immersive data representations, enhancing analysis and decision-making capabilities. However, AR environments, like proprietary metaverse implementations, are searchable only for the owner. Thus, searching for pattern of ML becomes more difficult.

Specific AI (Narrow AI): The trend towards developing AI with specialised capabilities – or Narrow AI – is significant for AML. Tailored AI systems can be more effectively trained on specific types of financial crime, resulting in higher

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

precision in anomaly detection and regulatory compliance. Artificial general intelligence (AGI) systems are only on the horizon.

Improving Law Against Money Laundering: There is a discernible trend towards strengthening legal frameworks against money laundering. AI can play a role in this by providing regulatory bodies with tools for monitoring compliance and flagging deviations more efficiently (Joseph and Turksen, 2022).

Increasing Divide in Society Caused by Social Media: The trend of social media exacerbating societal divides can indirectly impact AML efforts. It can influence the political and regulatory environment surrounding technology adoption and privacy laws, which in turn affect how AI is implemented in AML processes. The weak and poor in the society are becoming less protected, as they might get involved in illegal groups, without the attention of LEAs and mass media.

4.5.1.3 Disruptive Events

Geopolitical Conflicts and Corruption: These events can drastically change the AML landscape by shifting the focus and resources to emerging hotspots of financial crime. The actual formation of BRICS (BRICS, 2025) as opponent to NATO might lead to different groups of nations, involved in a sanctions regime and thus avoiding exchanging AML information. AI systems may need to adapt rapidly to new patterns of money laundering that arise as a result of such disruptions.

AI-Generated Fake Information for Fraud and Money Laundering: The potential of AI to create convincing fake information could be a disruptive event, challenging existing AML mechanisms. This necessitates the development of sophisticated AI that can distinguish between genuine and AI-generated fraudulent information.

4.5.1.4 Threats

Big Data for Hackers: The availability of large, leaked data sets could empower hackers and posing a threat by enabling them to devise new methods for committing financial crimes. In response, AML systems powered by AI will have to evolve to outsmart such threats, perhaps by using the same data for predictive analytics and defence mechanisms.

4.5.1.5 Innovation

Fake Detection: Innovations in detecting fakes, such as deep fakes or doctored documents, are crucial for AML. By leveraging AI's pattern recognition capabilities, these systems can identify discrepancies or anomalies that human analysts might miss.

Specific AI Chips: The development of AI chips designed specifically for AI AML tasks could greatly enhance processing capabilities. These chips could accelerate data

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

analysis, pattern detection, and real-time monitoring, thus significantly strengthening the technological infrastructure against money laundering activities.

Each of these elements highlights the dynamic interplay between the evolving capabilities of AI and the persistent adaptations of money laundering tactics in the years around 2025 and are considered state of the art. The future of countering financial crime and AML starting from 2026 will likely be characterised by a technological arms race, with both sides (criminals and public authorities) wielding AI as either a tool for perpetration or prevention. The challenge will be in developing AI that not only keeps pace with these changes but also anticipates and mitigates potential risks before they materialise (Hutter and Hutter, 2021).

4.5.2 2026 (Near Future)

In 2026, the application of AI in AML will continue to evolve, responding to new weak signals, disruptive events, threats, and innovations. Here is an exploration of these elements.

4.5.2.1 Weak Signals

Supervised ML for AML Pattern Identification: Although such an AI is in use right now, quality improvements could be expected. The use of supervised ML to detect known money laundering patterns, for example, will continue to refine the accuracy of predictive models. These models will be trained on historical data to identify transactions that closely resemble known money laundering cases, increasing detection rates.

Unsupervised ML for AML pattern identification: Similar to supervised ML, quality improvements and advancements in this sphere could be expected. Unsupervised ML approaches will play a significant role in discovering new, previously unidentified patterns in money laundering. By analysing data without pre-labelled outcomes, these models can unearth subtle correlations and anomalies that humans and supervised models may miss.

AI-driven data analysis in cloud data and blockchain data: As more financial transactions move to the cloud and blockchain, AI-driven analytics will become paramount in monitoring these platforms for signs of money laundering and other malfeasant activities. The decentralised nature of blockchain and the vast amount of cloud-stored data present unique challenges that AI is well-equipped to manage.

Smart Contracts (SC): Smart contracts will diffuse in all corners of business, in particular everyday business to business activities. SC on blockchain platforms will be scrutinised through AI to ensure they are not coded to facilitate money laundering. For instance, AI could potentially be used to analyse the terms of these contracts to identify those designed to obfuscate the origin of funds.

Heterogeneous Graph Transformer Networks (HGTN): These advanced neural network architectures will be capable of analysing data from various sources and

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

types, providing a more holistic view of existing financial networks and forecast future networks. Their ability to handle heterogeneous data will make them particularly effective in AML applications.

Spatial Computing: This technology, which enables the interaction of computers with the three-dimensional space, as presented by Apple (Apple, 2025) and other technology firms, could be used to visualise and analyse the geography of financial transactions, potentially revealing high-risk zones for money laundering activities. There is a potential overlap with AR/VR and metaverse technologies, named by different bands differently. The future needs to decide, whether special computing is different from metaverse, as Apple did claim (Euronews, 2024).

4.5.2.2 Trends

There are no new trends, compared to 2025, which indicate that the developments established in the previous year could continue to mature and become mainstream practices in AML efforts (Financial Conduct Authority, 2025).

4.5.2.3 Disruptive Events

APTs with Intelligent Cyber Agents: Advanced Persistent Threats (APTs) employing intelligent cyber agents could significantly disrupt financial cybersecurity. These agents could autonomously adapt and evolve to bypass security measures, requiring AI-driven defence systems to be equally adaptive. It is very likely, that these systems are in development (Mutalib et al., 2024; Shami and Rohatgi, 2024). The next step would be to see such a system in operation. Machine learning could be a component in these systems, which tactically prepare for cyber operations.

Hybrid Warfare Conflicts: The use of cyber warfare tactics alongside conventional warfare could impact global financial stability. AI will be crucial in detecting and responding to financial attacks that form part of these hybrid warfare strategies. Machine learning and AML might get part of non-conventual conflicts and countries need to prepare for this.

4.5.2.4 Threats

In-game Communication: As video games have become more social, they have been exploited for covert communication between criminals and terrorist. It is very likely that money launderers are offering their services and organising their customer relations in these closed systems. Monitoring these platforms for suspicious activities without infringing on privacy will be a delicate and yet unsolved challenge for AI-driven AML solutions.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.5.2.5 Innovation

AI-generated Shell Company in Ethereum (DAO/DeFi): The creation of decentralised autonomous organisations (DAOs) and decentralised finance applications (DeFi) on the Ethereum blockchain as shell companies for money laundering is a potential avenue for OC groups. To address this innovation, AI would need to differentiate between legitimate and AI-generated DAOs used for illicit purposes.

Smart Gaming Infrastructure: Gaming platforms might implement smart technologies to prevent their misuse for money laundering. AI innovations could monitor transaction patterns within games for suspicious financial activities, integrating AML mechanisms within the gaming industry's infrastructure.

By 2026, AI's role in AML will have expanded significantly, not only in detecting and preventing traditional forms of money laundering but also in adapting to the newer modalities that technology and innovation bring forth. AI's versatility and learning capabilities will be central to maintaining the integrity of increasingly digital financial systems (Basu and Tetteh, 2024; Leitner et al., 2024).

4.5.3 2030 *(Mid-term 1)*

Looking towards 2030, the landscape of AML is expected to be significantly shaped by advancements in AI technologies and changing global dynamics. Here is an exploration based on the collected information.

4.5.3.1 Weak Signals

Convolutional Neural Networks and Autoencoders for Graph Deep Learning: The application of these sophisticated AI models will likely advance the detection of complex money laundering schemes embedded in financial networks. Their ability to process and learn from graph-structured data will enhance the mapping and understanding of transaction flows.

AI for Profiling in Large Data Sets: Profiling within large datasets will become more nuanced with AI, allowing for the identification of risky profiles and behaviours with greater accuracy. This will enhance due diligence and ongoing monitoring efforts.

Explainable AI (XAI): As AI systems become more integral to AML, the need for transparency in AI decision-making processes will grow. XAI will be critical for gaining the trust of regulators and users by providing understandable explanations for AI's conclusions and actions. Future AML AI systems will highly likely be based on XAI concepts.

4.5.3.2 Trends

Quantum Computer in Operation: The deployment of quantum computing will revolutionise AML efforts by exponentially increasing the speed and capacity to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

analyse complex datasets and recognise patterns that are beyond the scope of classical computing. However, this will only work on very specific and hard to solve solutions such as decrypting asymmetric encryption.

AI ML Pattern Recognition: Pattern recognition capabilities of AI will not disappear because of AGI models. Instead, they are highly likely to evolve, becoming adept at sifting through noise to detect the subtlest signs of illicit activities, because of XAI.

AGI: If achieved, AGI will represent a monumental shift in AI capabilities, potentially outperforming human intelligence in AML tasks, and being capable of solving complex problems with little to no human intervention. However, it is highly likely, that the AGI models will use XAI and AI ML to improve the efficiency, transparency, and reliability.

Mesh Ad Hoc Networks: As decentralised, self-configuring networks become more prevalent in hacker communities, AML systems will need to adapt to monitor transactions in these less centralised environments. However, this is an unclear trend, as it might highly likely be, that comfort is prioritised against security. In combination with many devices, mesh networks seem to have an advantage, but it remains open, whether cryptocurrency exchange could go via network devices, by direct concept. This would make a cryptocurrency very equal to cash.

4.5.3.3 Disruptive Events

Geopolitical Shifts in Cyber Innovation from Industrialised Countries to New Economies: The shift of technological innovation to emerging economies may alter the AML landscape by introducing new technologies and methodologies at a rapid pace. It is very difficult to forecast geopolitical trends until 2030, but as it looks today, it is likely that we will be in a multi polar world, with different aggressions appearing and disappearing until we have a clear balance of power.

4.5.3.4 Threats

Cyber Warfare Realised: It is likely that by 2030 the first cyber warfare operations will become visible. By 2025 there have been a lot of hacking and other cyberattacks (World Economic Forum, 2023). However, these are single activities and not embedded in a military concept. Arguably, Stuxnet was the first military cyber operation, (Knapp and Langill, 2015) yet this was to avoid a war, not to win a war. It is likely that the use of unconventional nonmilitary organisations (e.g., state-sponsored and contracted independent hacker groups/cyber mercenaries) will become more important in military operations. AML strategies will need to become more sophisticated to combat state-sponsored and highly organised cybercrime syndicates.

Metaverse and the New Dark Nets: The emergence of extensive virtual environments like the metaverse may create new avenues for financial crime and money laundering, similar to the darknet, but with potentially greater complexity and scale.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

In 2030 the landscape of metaverse providers is likely to be more diverse, than of 2025. These different proprietary platforms offer good opportunities for AML, without being detected.

4.5.3.5 Innovation

Multimodal AI: AI capable of processing and interpreting multiple types of data simultaneously (e.g., text, images, and sensor data) could provide a holistic view of financial activities for better monitoring and detection of illicit actions.

Quantum CPU Operational: Once available with the relevant number of qubits, quantum processors will bring about breakthrough capabilities in data processing for AML, possibly enabling the cracking of previously unbreakable encryption methods used in financial crimes.

Genetic Robots: While not directly related to AML, the development of robots that can interact with genetic material may influence cybersecurity if such technology is applied to biometric security measures. If used on cash, it might be possible to use xenobots as marker for cash in 2030.

By 2030, AML efforts will have to contend with an increasingly complex and interconnected technological environment. Advancements in AI will offer unparalleled tools for financial security, while also introducing new challenges that will need to be addressed to keep illicit activities in check. Quantum computing, AGI, and multimodal AI will be at the forefront of detecting and preventing sophisticated money laundering operations, necessitating a proactive and innovative approach to AML policy and practice.

4.5.4 2035 *(Mid-term 2)*

By 2035, the landscape of AML efforts will continue to be profoundly influenced by advanced technological developments and shifts in the geopolitical and cyber landscape. Not surprisingly, technology will be faster, more precise, and more intelligent. Here is an exploration based on the collected information:

4.5.4.1 Weak Signals

Biological Neurons as CPU: This groundbreaking development indicates a fusion of biological components with computing technology, leading to a new era of processing capabilities, by using brain cells to form a neuronal network. First results have been surprisingly successful (Khullar, 2025; Reuters, 2024). For AML in 2035, this could mean unparalleled data processing and pattern recognition abilities, allowing for real-time analysis of complex financial networks with a level of nuance and adaptability that mimics the human brain.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.5.4.2 Trends

Competition of different Geopolitical Large-Scale C2 (Command and Control) Systems: The very different approaches and sometimes the rivalry among countries to develop superior command and control systems for surveillance, data analysis, and cyber operations will significantly impact global efforts to counter financial crime and money laundering. The effectiveness of AML measures will be closely tied to the capabilities of these systems, influencing how quickly and efficiently illicit financial activities can be detected and countered.

Transfer of Human Capabilities to Machines: The trend of endowing machines with skills and decision-making processes that were traditionally human will redefine AML strategies. AI systems in AML will not only analyse data but also make complex decisions about the risk associated with various transactions and entities, incorporating ethical and legal considerations in the future.

4.5.4.3 Disruptive Events

Intelligent Sensors and Tracking, Finding Anything, Anywhere, Anytime: The ubiquity of intelligent sensors from any smart device, capable of tracking financial transactions and assets across the globe will make it exceedingly difficult for money laundering activities to go undetected. However, this also raises significant privacy and surveillance concerns that will need to be addressed.

All Domain Liquid Mosaic Warfare Conflicts: This new form of warfare, characterised by highly fluid and adaptive strategies across multiple domains (not just land, sea, air, cyber, and space, but also cognitive domain, information, and psychology), in addition to hybrid tactics, will pose unique challenges to AML efforts. Financial systems might become targets or tools within these conflicts, necessitating AI-driven systems that are as adaptive and multifaceted as the warfare strategies themselves.

4.5.4.4 Threats

Asymmetric Encryption is Broken: If the foundational security mechanism of asymmetric encryption is compromised, for example, by an operational quantum computer, or by a biological computer, the integrity of all digital financial transactions could be at risk. AML strategies will need to evolve to counter the heightened risk of financial data breaches and fraudulent transactions.

Swarm of Intelligent Agents for Money Laundering Working Effectively in Different Metaverses: The use of coordinated, intelligent agents operating across various digital realms in the metaverse to launder money will challenge traditional AML frameworks. These agents, capable of executing complex laundering schemes across multiple platforms, will require equally sophisticated AI-driven countermeasures.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.5.4.5 Innovation

Metaverse Forensic Framework: In response to the new challenges posed by digital universes, an innovative forensic framework will be developed for the metaverse. This will enable the tracking, analysis, and investigation of financial crimes within these expansive digital spaces, leveraging AI to navigate and make sense of the complex, immersive environments.

By 2035, AML efforts will need to be highly adaptive, leveraging cutting-edge AI to keep pace with rapidly evolving financial crime strategies. The intersection of AI, biocomputing, and new digital frontiers will redefine the battleground for financial security, requiring a balance between innovation, privacy, and regulatory oversight.

4.5.5 2040 *(Long-Term Future)*

The long-term foresight is particularly challenging. For epistemic reasons it is not possible to produce a precise technology forecast and by definition, it is not possible to capture unexpected disruptive innovation. Nevertheless, it is possible to extend existing technology trends and to develop scenarios, based on the interdependence of existing basic research results and possible future technology innovation, which is based on existing knowledge and future needs, which can be derived from reliable trends like demographic trends, environmental trends, trends in future use of resources trends in societal challenges and possible innovations, based on these scenarios. Given these trends, by 2040, the landscape of AML will be profoundly influenced by advanced AI technologies and significant shifts in the global technological infrastructure. Following is an overview of these developments, as far as possible.

4.5.5.1 Weak Signals

Genetic Robots (Xenobots) in Operation: The emergence of xenobots, robots designed with biological materials, signifies a blurring of the lines between biological and artificial systems. From today's perspective, these xenobots might be used to imitate biological marker. However, if these bots could be used to parallelise calculations of AML algorithms or other threat detection systems. In the far future these xenobots could be deployed for tasks that require a physical presence, such as inspecting physical assets or locations involved in financial transactions. However, this is highly speculative.

Quantum Computer in Operation: The operational use of quantum computers will offer unprecedented computational power in selected algorithm (Bravyi et al., 2022). This could enable the processing of complex AML algorithms and large datasets at speeds unattainable by classical computers and enhance pattern recognition and anomaly detection in financial transactions.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

AI in 6G Networks Supporting Investigations: The integration of AI into 6G networks will facilitate faster, more reliable communication and data analysis capabilities (Chataut, Nankya and Akl, 2024). This could be used to support real-time AML investigations and enhancing cross-border collaboration.

4.5.5.2 Trends

Artificial Super Intelligence (ASI) to Avoid Corruption in Political Decisions: The involvement of ASI in political decision-making could lead to more transparent and corruption-resistant governance structures, supporting AML and counter financial crime efforts by reducing the opportunities for dishonesty crimes. However, it is not clear whether a society would accept this.

Digital Currencies Used in Daily Life: The widespread adoption of digital currencies will necessitate advanced AML measures to monitor and secure digital financial ecosystems against money laundering activities.

Human-Brain Interface in Investigative Operations: The use of human-brain interfaces in investigations could revolutionise data analysis and decision-making processes, enabling investigators to interact directly with AI systems for deeper insights and intuitive understanding of complex patterns.

Transfer of Human Capabilities to Machines: The ongoing trend of endowing machines with human-like capabilities will enhance AI's effectiveness in identifying and adapting to new money laundering tactics, offering a more nuanced and adaptable approach to AML.

4.5.5.3 Potential Disruptive Events

ASI in Political Decisions Can Avoid Corruption: The integration of ASI in governance could disrupt traditional power structures and decision-making processes, potentially eliminating many of the systemic vulnerabilities that money launderers exploit.

Digital Currencies Used in Daily Life: The normalisation of digital currencies will disrupt traditional financial systems, requiring a complete re-evaluation and redesign of AML strategies to address the unique challenges posed by digital/crypto and decentralised financial systems.

4.5.5.4 Threats

AGI for Organised Crime: The use of AGI or even ASI by organised crime groups could escalate the sophistication of money laundering schemes, presenting complex challenges for AML systems to identify and counteract such advanced threats.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

4.5.5.5 Innovation

New Rules for AGI in Daily Life: The establishment of new regulatory frameworks for AGI's role in society will be crucial in ensuring these systems are used ethically and responsibly, particularly in sensitive areas like AML.

Intelligent Investigation Agents: The development of AI-powered agents specialised in investigations will transform AML processes, enabling proactive and highly nuanced analysis of financial activities.

Neuromorphic Computing: This innovation, which involves designing computer chips that mimic the human brain's structure, will provide AI systems with enhanced learning and processing capabilities, ideal for the complex demands of AML.

God-like AI: The concept of AI with God-like capabilities (Werner, 2024; Uyar, 2024), in terms of intelligence and decision-making, raises both opportunities and challenges for AML, as it could either be a powerful tool in combating financial crimes or a formidable adversary if misused.

Quantum Supremacy: Achieving quantum supremacy, where quantum computers can perform tasks beyond the reach of classical computers, will revolutionise AML by enabling the analysis of encrypted data and complex networks at an unprecedented scale and speed.

By 2040, the integration of these advanced technologies into AML efforts will necessitate a paradigm shift in how financial security is maintained, requiring innovative approaches to harness these capabilities responsibly and effectively while safeguarding against their potential misuse.

This roadmap is indicative of a projected evolution of AI capabilities in relation to societal changes and challenges, particularly focusing on countering financial crime and money laundering. It suggests a progressive integration of AI with various systems and societal structures, hinting at significant technological advancements and possible geopolitical events that could impact the development of AI in this compiled context.

4.6 RECOMMENDATIONS AND CONCLUSION

The confluence of rapidly evolving AI technologies and shifting geopolitical landscapes presents both unprecedented opportunities and challenges. As we stand on the cusp of significant technological breakthroughs, from quantum computing to AGI, the need for a robust, dynamic, and forward-thinking approach to countering financial crime and money laundering cannot be overstated. Based on the analysis of how AI can be leveraged in financial crime investigation and where the AI technology may be heading in the future, the following recommendations are put forward. The key aim behind these recommendations is to equip LEAs with the strategic

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

foresight and agility required to harness the benefits of AI advancements while mitigating associated risks.

While doing the horizon scanning exercise, it became obvious that the intricate interplay of technological innovation, regulatory adaptation, and international cooperation is essential for countering financial crime and money laundering effectively. The landscape is characterised by the emergence of sophisticated AI applications capable of enhancing AML efforts but also by the potential for these same technologies to be co-opted for nefarious purposes. Thus, any country's approach must be holistic, encompassing not only the enhancement of AI capabilities in AML efforts but also the ethical, legal, and societal implications of such technologies.

It is important to recognise that the path forward requires a concerted effort across multiple fronts. This includes strengthening regulatory frameworks, fostering ethical AI development, enhancing international collaboration, and investing in future-ready technologies and training of law enforcement staff. The ultimate goal should be to create an AML ecosystem that is not only resilient in the face of emerging threats but also conducive to ethical and sustainable technological advancement.

Based on the roadmap with a comprehensive overview of the anticipated developments in AI against money laundering up to 2040, drawing on the trends, weak signals, disruptive events, threats, and innovations outlined, here are several recommendations:

Enhance Regulatory Frameworks: Given the fast pace of AI development and its applications in countering financial crime and AML, LEAs should continuously update and enhance its regulatory frameworks to ensure they remain effective and relevant. This includes privacy, data protection, and AI ethics, particularly in light of emerging technologies such as emotional face recognition and the use of AI in financial transaction monitoring.

Promote Ethical AI Use: There needs to be clear guidelines and standards for the ethical use of AI, balancing technological advancement with fundamental rights and freedoms. This includes considerations around consent, transparency, and accountability, particularly with technologies like AI-driven emotional recognition, predictive decision-making, and unsupervised ML for AML patterns.

Establish AI Ethics and Governance Bodies: There should be dedicated authorities for overseeing AI ethics and governance, particularly in sensitive areas of AML and AI. These would be responsible for setting standards, conducting audits, and ensuring compliance with ethical AI use in AML. This would help address concerns related to privacy, bias, and accountability in AI systems used for AML purposes.

Foster International Cooperation: The global nature of financial crime necessitates international collaboration. Countries should lead, support and participate in global initiatives to standardise AML practices, share intelligence, and harmonise regulatory environments, especially in light of geopolitical shifts and the potential fragmentation of AML efforts.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Strengthen Cybersecurity Measures: With the increasing sophistication of cyber threats, the authorities should prioritise the development and implementation of advanced cybersecurity measures to protect financial systems. This includes preparing for the potential threats posed by quantum computing to encryption standards.

Develop Skills and Expertise: There is an urgent need to build a skilled workforce capable of designing, implementing, and managing advanced AI systems in the AML domain. This includes education and training programmes in AI, cybersecurity, and financial regulations.

Encourage Responsible Innovation: While promoting innovation in AML strategies, new technologies shall be developed and implemented responsibly, with due consideration for potential social, ethical, and privacy implications.

Adapt to New Financial Ecosystems: As digital and decentralised financial systems become more prevalent, AML strategies must adapt to these new environments. This includes understanding and regulating emerging technologies such as blockchain-based SC, crypto currencies and non-fungible tokens.

Prepare for Geopolitical Shifts: There is need to remain agile and responsive to geopolitical shifts that could impact AML efforts, including the rise of new economic powers and the potential for cyber warfare. This includes developing contingency plans and strategic alliances.

Invest in Research and Development: To stay ahead of sophisticated financial crime schemes and money laundering tactics, LEAs should invest in R&D for advanced AI technologies, including quantum computing, AGI, and multimodal AI. This should include public-private partnerships to drive innovation in AML strategies.

Enhance Data Sharing Mechanisms: As the relevant information and evidence related to cross- border crimes are captured in different jurisdictions, there is a need to develop secure and efficient data sharing mechanisms to facilitate the exchange of information related to AML between different stakeholders, including financial institutions, regulatory bodies, and international partners. This would improve the detection and prevention of money laundering by leveraging collective intelligence and resources.

These recommendations can create a robust, dynamic, and responsive policy that leverages AI's potential while addressing the challenges and risks associated with rapid technological advancements.

REFERENCES

Acronis (2025) *Understanding the true, hidden costs of ransomware attacks on the business*. Available at: www.acronis.com/en-gb/blog/posts/costs-of-ransomware-attacks/ (Accessed 28 March 2025).

Apple (2025) *Apple's first spatial computer*. Available at: www.apple.com/uk/newsroom/2023/06/introducing-apple-vision-pro/ (Accessed 1 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Basu, D. and Tetteh, G. K. (2024) Using Automation and AI to Combat Money Laundering, Financial Regulation Innovation Lab. Available at: www.strath.ac.uk/media/departments/accountingfinance/fril/whitepapers/Using_Automation_and_AI_to_Combat_Money_Laundering.pdf (Accessed 22 May 2025).

Banks, J. (2014) *Online Gambling and Crime: Causes, Controls and Controversies*. 1st ed. London: Routledge. Available at: https://doi.org/10.4324/9781315598918.

Bitcoin.org (n.d.) *Bitcoin – Open source P2P money*. Available at: https://bitcoin.org/en/ (Accessed 13 April 2025).

Bravyi, S. et al. (2022) The future of quantum computing with superconducting qubits. *Journal of Applied Physics*, 132(6).

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*. Available at: https://infobrics.org (Accessed 1 April 2025).

Browne, T. O., Abedin, M. and Chowdhury, M. J. M. (2024) A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, 23, pp. 2911–2938.

Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Waltham: Academic Press.

Cellebrite, n.d. *Cellebrite – Digital Intelligence for a Safer World*. Available at: www.cellebrite.com (Accessed 13 April 2025).

CEPOL (2019) Digital data - Now and tomorrow. European Union Agency for Law Enforcement Training, 9 July. Available at: www.cepol.europa.eu/newsroom/partners-news/digital-data-now-and-tomorrow (Accessed 23 April 2026).

Charniak, E. and McDermott, D. (1991) *Introduction to Artificial Intelligence*. Reading, Mass.: Addison-Wesley.

Chataut, R., Nankya, M. and Akl, R. (2024) 6G networks and the AI revolution: Exploring technologies, applications, and emerging challenges. *Sensors*, 24, p. 1888. https://doi.org/10.3390/s24061888 (Accessed 1 April 2025).

Chugani, S. H. (2008) Benevolent blood money: Terrorist exploitation of Zakat and its complications in the war on terror. *North Carolina Journal of International Law and Commercial Regulation*, 34, p. 601.

Cobwebs (2020) *Web Forensics for Tackling Terrorism Investigation*. Available at: www.cobwebs.com/wp-content/uploads/2020/01/Web-Forensics-for-Tackling-Terrorism-Investigation-White-Paper.pdf (Accessed 26 March 2025).

Council of Europe (n.d.) *Financing of terrorism*. Available at: www.coe.int/en/web/moneyval/implementation/financing-terrorism (Accessed 24 June 2022).

CSIS (2024) *Significant Cyber Incidents*. Available at: www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Accessed 1 April 2025).

Cyber Management Alliance (2025) *Top 10 Biggest Cyber Attacks of 2024 & 25*, 20 January. Available at: https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about (Accessed 02 April 2025).

Davenport, T. and Ronanki, R. (2018) Artificial Intelligence for the real world. *Harvard Business Review*, January–February. Available at: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world (Accessed 18 March 2025).

Dash.org, n.d. *Dash – Digital Cash*. Available at: www.dash.org/ (Accessed 13 April 2025).

De Sanctis, F. M. (2019) *Technology-Enhanced Methods of Money Laundering: Internet as Criminal Means*. Cham: Springer.

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

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Dick, S. (2019) Artificial intelligence. *Harvard Data Science Review*, 1(1). https://doi.org/10.1162/99608f92.92fe150c (Accessed 18 March 2025).
Dixon, A. and Birks, D. (2021) 'Improving Policing with Natural Language Processing', in *Proceedings of the 1st Workshop on NLP for Positive Impact*, pp. 115–124. Available at: https://aclanthology.org/2021.nlp4posimpact-1.13.pdf (Accessed 28 March 2025).
Euronews (2024) 'What is "spatial computing" and why is Apple pushing the new buzzword?'. Available at: www.euronews.com/next/2024/02/05/what-is-spatial-computing-and-why-is-apple-pushing-the-new-buzzword (Accessed 22 May 2025).
European Commission (2012) *Online gambling in the Internal Market*, SWD (2012) 345 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0345&from=EN (Accessed 28 March 2025).
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. Available at: https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax (Accessed 24 June 2022).
European Council (2023) *Council adopts EU laws on better access to electronic evidence*. Press Release. Available at: www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/ (Accessed 19 March 2025).
European Council (2024) *Better access to e-evidence to fight crime*, 11 January. Available at: www.consilium.europa.eu/en/policies/e-evidence/ (Accessed 19 March 2025).
European Council (n.d.) *Taxes in Europe Database v2*. Available at: https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax (Accessed 24 June 2022).
European Parliamentary Research Service (2017) *Die Kapazität der Mitgliedstaaten zur Bekämpfung von Steuerstraftaten: Ex post Folgenabschätzung*. Available at: https://data.europa.eu/doi/10.2861/9432 (Accessed 10 May 2022).
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 …. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (Accessed 18 March 2025).
EUROPOL (2020) Beyond the pandemic: how COVID-19 will shape the serious and organised crime landscape in the EU. Available at: www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know (Accessed 27 March 2025).
EUROPOL (2021) Serious and Organised Crime Threat Assessment (SOCTA). Available at: www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Accessed 19 March 2025).
EUROPOL (2023) Internet Organised Crime Threat Assessment (IOCTA). Available at: www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment (Accessed 28 March 2025).
EUROPOL (2024) AI and policing: The benefits and challenges of artificial intelligence for law enforcement. ISBN 978-92-95220-92-8.
Financial Action Task Force (FATF) (2019) Terrorist Financing Risk Assessment Guidance. Available at: www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf (Accessed 22 May 2025).
Financial Conduct Authority (2025) Assessing and reducing the risk of Money Laundering Through the Markets (MLTM). Available at: www.fca.org.uk/publication/corporate/money-laundering-through-markets-review-january-2025.pdf (Accessed 22 May 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Fiedler, I. (2014) Online gambling as a game changer to money laundering? in Ötsch, W.O. et al. (eds.) *The Political Economy of Offshore Jurisdictions*. Marburg: Metropolis Verlag, pp. 79–98.

Fiedler, I. et al. (2017) *Das Geldwäscherisiko verschiedener Glücksspielarten*. Wiesbaden: Springer. Available at: http://link.springer.com/10.1007/978-3-658-16625-0 (Accessed 28 March 2025).

Fiedler, I. et al. (2020) *Regulierung von Onlineglücksspielen*. Wiesbaden: Springer. Available at: https://doi.org/10.1007/978-3-658-29846-3 (Accessed 28 March 2025).

Financial Times (2019) London properties worth £80 m targeted in 'dirty money' probe, 29 May. Available at: www.ft.com/content/9b1a3e7a-814d-11e9-b592-5fe435b57a3b (Accessed 24 June 2022).

Fisher M. L. et al. (2025) Legal and regulatory responses to online gambling harms: A scoping review of evidence, *Harm Reduction Journal*, Oct 8;22(1):163.

Forbes (2018) Criminals are using your dream home to clean dirty money, 21 November. Available at: www.forbes.com/sites/vishalmarria/2018/11/21/criminals-are-filling-your-dream-home-with-dirty-money (Accessed 24 June 2022).

Forbes (2024) Detecting deepfakes: Fighting AI with AI, 6 August. Available at: www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/ (Accessed 31 March 2024).

Fouche, G. and Solsvik, T. (2019) Aluminum maker Hydro battles to contain ransomware attack. Reuters, 19 March. Available at: www.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUSKCN1R00NJ (Accessed 28 March 2025).

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

Gertenbach, W., Botha, J. and Leenen, L. (2024) A proposed high-level methodology on how OSINT is applied in blockchain investigations, in Van Niekerk, B. 19th International Conference on Cyber Warfare and Security: ICCWS 2024. Available at: https://books.google.co.uk/books?hl=en&id=WxAXEQAAQBAJ&pg=PA75 (Accessed 22 May 2025).

GetMonero.org (n.d.) Monero – Private Digital Currency. Available at: www.getmonero.org/ (Accessed 13 April 2025).

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

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

Grand View Research (2019) Online gambling market size, share & trends analysis report. Available at: www.grandviewresearch.com/industry-analysis/online-gambling-market (Accessed 28 March 2025).

Gutowska, A. (2024) *What are AI Agents*. IBM, 3 July. Available at: www.ibm.com/think/topics/ai-agents (Accessed 18 March 2025).

Hodgson, G. S. and Jiang, S. (2021) *Online Money Laundering: Methods and Countermeasures*. Cheltenham, UK: Edward Elgar Publishing.

Home Office (2018) *UK anti-corruption strategy: 2017 to 2022*. Available at: www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022 (Accessed 25 March 2025).

Hutter, R. and Hutter, M. (2021) Chances and risks of artificial intelligence: A concept of developing and exploiting machine intelligence for future societies. *Applied System Innovation*, 4(2), 37.

i2 Analyst's Notebook (n.d.) *IBM i2 Analyst's Notebook*. Available at: www.ibm.com/products/i2-analysts-notebook (Accessed 13 April 2025).

IBM (2023) *What are large language models (LLMs)?* 2 November. Available at: www.ibm.com/think/topics/large-language-models (Accessed 30 March 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

IMF (2022) *Global Financial Stability Report: Navigating the High-Inflation Environment*. International Monetary Fund. Available at: www.imf.org/en/Publications/GFSR (Accessed 22 March 2025).

InfoZoom (n.d.) *InfoZoom – Data Analysis and Visualization Software*. Available at: www.infozoom.com/en/ (Accessed 13 April 2025).

Interpol (2023) *Digital Forensics in Combating Cybercrime*. Available at: www.interpol.int/en/Crimes/Cybercrime/Digital-forensics (Accessed: 26 March 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.

Kethineni, S., Cao, Y. and Dodge, C. (2017) Use of cryptocurrency in money laundering: Examining Bitcoin transactions. *International Criminal Justice Review*, 27(4), pp. 355–372. https://doi.org/10.1177/1057567717738263 (Accessed 6 April 2025).

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

Knapp, E. D. and Langill, J. T. (2015) *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. 2nd ed. Syngress Media.

KPMG (2023) *2023 Fraud Outlook Report*. Available at: https://home.kpmg/xx/en/home/insights/2023/01/kpmg-2023-fraud-outlook.html (Accessed 30 March 2025).

Leitner, G., Singh, J., van der Kraaij, A. and Zsámboki, B. (2024) *The rise of artificial intelligence: benefits and risks for financial stability*. European Central Bank – Financial Stability Review. Available at: www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html (Accessed 22 May 2025).

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

Littler, A. (2020) How the EU's regulatory approach to gambling is failing. *Maastricht Journal of European and Comparative Law*, 27(1), pp. 56–72. https://doi.org/10.1177/1023263X19888997 (Accessed 6 April 2025).

Lugo, G. and Faiella, G. (2020) *Cryptocurrencies and money laundering: An overview*, Bank of Italy Occasional Paper No. 559. Available at: www.bancaditalia.it/pubblicazioni/qef/2020-0559/QEF_559_20.pdf (Accessed 25 March 2025).'

MI5 (2023) *Threats to the UK: espionage, cyber attacks and terrorism*. Available at: www.mi5.gov.uk/threats-to-the-uk (Accessed 20 March 2025).

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, p. 297.

National Crime Agency (NCA) (2021) *National Strategic Assessment of Serious and Organised Crime 2021*. Available at: https://nationalcrimeagency.gov.uk/who-we-are/publications/539-national-strategic-assessment-of-serious-and-organised-crime-2021/file (Accessed 18 March 2025).

National Crime Agency (NCA) (2025) *Money Laundering and Illicit Finance*. Available at: www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance (Accessed 22 May 2025).

OECD (2022) *Tax Crime Investigation Maturity Model*. Available at: www.oecd.org/tax/crime/tax-crime-investigation-maturity-model.htm (Accessed 10 May 2022).

Palmer, C. (2021) *Digital Forensics: The Fascinating World of Forensic Science*. New York: Rosen Publishing.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

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

Press, G. (2024) Detecting deepfakes: Fighting AI with AI. *Forbes*, 6 August. Available at: www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/ (Accessed 31 March 2024).

PwC (2022) *Bitcoin, cryptocurrency, blockchain . . . So what does it all mean?* Available at: www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (Accessed 28 March 2025).

PwC (2023) *Global Economic Crime and Fraud Survey 2023*. Available at: www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (Accessed 30 March 2025).

Reuters (2024) *Elon Musk's Neuralink implants brain chip in first human*. Reuters, 30 January. Available at: www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/ (Accessed 6 April 2025).

Roodt, C. and Benson, B. (2015) 'Databases for stolen art', *SA Crime Quarterly*, June, No. 52: 5–14.

RsCase (n.d.) *rsCase – Investigation Case Management Software*. Available at: www.rstech.de/en/products/rscase/ (Accessed 13 April 2025).

Russell, S. and Norvig, P. (2016) *Artificial Intelligence: A Modern Approach*. Upper Saddle River: Pearson.

Sachoulidou, A., Rego Oliveira, C., Kordoni, A., Hughes, J., Nidhi Shiji, A. and Nathan, C. (2024) *D8.2 – The project's ethical, data protection and societal impact assessment*. TRACE project. Available at: https://cordis.europa.eu/project/id/101022004/results (Accessed 22 May 2025).

Sandotra, N. and Arora, B. (2024) A comprehensive evaluation of feature-based AI techniques for deepfake detection. *Neural Computing & Applications*, 36, pp. 3859–3887. https://doi.org/10.1007/s00542-024-06491-x (Accessed 6 April 2025).

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

Shami, S. and Rohatgi, S. (2024) Understanding and mitigating advanced persistent threats in a dynamic cyber landscape in Shrivastava, G. 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), pp. 9637.

The Law Society (2020) *Warning signs of money laundering*. Available at: www.lawsociety.org.uk/topics/anti-money-laundering/money-laundering-warning-signs (Accessed 22 May 2025).

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

UK Ministry of Defence (2018) Human-Machine Teaming, Joint Concept Note 1/18, p. 11. (online) Available at: www.gov.uk/government/publications/human-machine-teaming-jcn-118 (Accessed 9 June 2025).

UK National Cyber Security Centre (2024) *Heightened threat of state-aligned groups against western critical national infrastructure*, 1 January. Available at: www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups (Accessed 1 April 2025).

Uyar, T. (2024) *ASI as the New God: Technocratic Theocracy*. *Computers and Society*, 23 March. Available at: https://arxiv.org/abs/2406.08492 (Accessed 8 April 2025).

Van Duyne, P. C. (2016) Money laundering: estimates in fog. *Trends in Organized Crime*, 19, pp. 199–213. https://doi.org/10.1007/s12117-016-9282-3 (Accessed 25 March 2025).

Vurubindi, P. and Narahari, S. C. (2024) 'Encryption and Decryption Algorithms in Private AI', in Maheswari, U. V. and Aluvalu, R. (eds.), *Sustainable Development Using Private AI: Security Models and Applications*. Boca Raton: CRC Press.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Werner, J. (2024) God-like AI and the decentralized internet. *Forbes*, 19 June. Available at: www.forbes.com/sites/johnwerner/2024/06/19/god-like-ai-and-the-decentralized-internet/ (Accessed 8 April 2025).

World Bank (2016) *Do Digital Technologies Facilitate Illicit Financial Flows?* Available at: http://hdl.handle.net/10986/23803 (Accessed 10 May 2022).

World Economic Forum (2023) *Global Cybersecurity Outlook 2023*. Available at: www.weforum.org/reports/global-cybersecurity-outlook-2023 (Accessed 1 April 2025).

Yates, D. (2016) Soft control and the illicit trade in antiquities. *Trafficking Culture*, 21 April. Available at: http://traffickingculture.org/ (Accessed 28 March 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

5

The Interplay between Socio-Ethical, Legal and Technological Standards in Developing Automated Law Enforcement Systems: The Case of AI-Enabled Crime Analytics

Anastasia Kordoni, Athina Sachoulidou and Cristina Rego de Oliveira

5.1 INTRODUCTION

Before national, regional and international legislators considered regulating automation in response to emerging technologies, including artificial intelligence (AI), debates had already emerged about its role in *critical* areas of public governance, such as law enforcement. While automation is not new for the purposes of crime control (Sommerer, 2022), modern AI systems serve multiple law enforcement purposes, ranging from crime detection and investigation to crime prediction (Europol, 2025). However, their use in criminal proceedings raises concerns about fundamental rights, especially when AI-generated insights appear to influence decisions beyond human oversight (Straus, 2021). Notably, the capacity of AI systems to operate automatically and at scale (Yeung, Howes and Pogrebna, 2020) coupled with a higher degree of epistemic opacity (Buihsman, Klenk and van den Hoven, 2025; Burrell, 2016) challenge significantly the responsible use of such systems, particularly given the severity of the consequences for the affected individuals (see Section 5.2).

This chapter contributes to a multi-disciplinary approach to automated law enforcement, examining the example of AI tools intended to be employed for crime analytics purposes. As the cyber-element penetrates even traditional forms of criminal activity and data-driven police investigations grow more complex, law enforcement authorities (LEAs) leverage AI tools to analyse large datasets, identify patterns, uncover hidden relationships and unveil unknown patterns or discover hidden relationships in the data (for the respective definition see Commission, 2021, Annex III, point 6, lit. g). These tools may offer services like translation, entity extraction, video transcription, social media analysis, and relationship mapping through filtering and visualisation, and, thus, may consist of one or more respective components. The ultimate goal of their use is tackling crime more effectively. LEAs may use their output to establish or confirm suspicion, guide investigations, compile

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

prosecution files, determine key details of criminal conduct, and support prosecutors in initiating criminal proceedings.

This chapter explores the impact of AI-powered crime analytics on fundamental rights, focusing on defence rights through the lens of the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (CFR) (Section 5.2). It then critically examines the stance of Regulation (EU) 2024/1689, commonly known as the EU AI Act (AIA) on such AI systems, analysing key provisions within its risk-based approach to AI (Section 5.3). Given that crime-analytics tools as such have been largely excluded from high-risk classification in the AIA, it explores alternative safeguards advocating for a fundamental rights-by-design approach to their development (Section 5.4). Finally, this chapter concludes with a socio-ethical account on bias detection and mitigation tailored to the interconnectedness of micro (technical, individual), meso (organisational), and macro (social) challenges associated with AI-enabled crime analytics (Section 5.5).[1]

5.2 THE IMPACT OF AI-DRIVEN CRIME ANALYTICS TOOLS ON DEFENCE RIGHTS

The compatibility of AI with fundamental rights has been the focus of intense debates at national, regional, and international levels (Lane, 2022), aiming to promote human-centric AI. The affected rights span privacy, data protection, freedom of expression and association, non-discrimination, effective remedy, and fair trial rights (see, for instance, Council of Europe, 2017; González Fuster, 2020). Although some rights and risk parameters have received more attention than others, the EU legislators adopted a *holistic* approach to mitigate AI's adverse impacts across public and private fields of action. Given the particular features of crime analytics tools, the following analysis focuses on defence rights (see also Sachoulidou, 2026).

The EU Member States shall abide by the fair trial principle and the rights that arise therefrom as enshrined in the ECHR (Article 6) and the CFR (Articles 47–48). According to the jurisprudence of the European Court of Human Rights (ECtHR), one has to evaluate the *overall fairness* of *criminal* proceedings (ECtHR, 2024, paragraphs 2–3) – with the concept of '*criminal* charge' having a meaning that is independent of the categorisations employed by national legislators (ECtHR, 2024, paragraphs 15–16). Next, the notion of charge is defined as the 'the official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence' and includes the test of whether the suspect's situation has been affected substantially (ECtHR, 2024, paragraph 18). The fair trial guarantees, ranging from the right to a fair and public hearing to the right to equality of arms and adversarial hearings and the right to be presumed innocent,

[1] The analysis is based on the research findings of the TRACE H2020 project (Grant agreement no. 101022004). The respective research results have been included in deliverable 8.2 'The project's ethical, data protection and social impact assessment' (Sachoulidou *et al.*, 2024).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

apply *throughout the entire criminal procedure*, encompassing the pre-trial and the trial stage as well as the appeal proceedings.

AI systems used at pre-charge stages, such as those assessing the likelihood of future offending, will typically fall outside the scope of fair trial protections (Sachoulidou, 2023). Conversely, AI-based crime analytics systems may be introduced during criminal proceedings and their output, depending on the applicable national rules on evidence admissibility, may be treated as evidence. As such, their use must align with fair trial guarantees *throughout all procedural stages* (cf. Palmiotto, 2021). The affected individuals should be able to exercise their right to equality of arms and an adversarial hearing. Equality of arms presupposes that each party is given a reasonable opportunity to present their case under conditions that do not place them at a disadvantage vis-à-vis their opponent (ECtHR, 2024, paragraph 171). Similarly, the right to an adversarial hearing is respected when the parties are able to have knowledge of and comment on all evidence adduced or observations filed *with a view to influencing the court's decision*, without having to determine that the failure to access a certain piece of evidence has caused them any prejudice (ECtHR, 2024, paragraph 172). This suggests that the defendant shall be able to challenge evidence that arise from the use of AI-powered crime analytics tools effectively. This presupposes, however, a certain level of *transparency* regarding the algorithmic output as well as the inner workings of the algorithm.

Further ECtHR guidance supports this approach. Taking the example of expert findings, the Court has stressed that the failure of the prosecution to disclose the technical details an expert report has been based upon may compromise the defence's ability to challenge the report and, thus, raise an issue of equality of arms (ECtHR, 2024, paragraph 184). Limited access to the case file or other documents on public-interest grounds may have a similar effect – with the Court finding that respect for defence rights requires that access limitations shall not prevent the evidence from being made available to the defendant before the trial and the latter from commenting on it (ECtHR, 2024, paragraphs 185–186). However, the right to disclosure of relevant evidence is not absolute as competing interests, such as police secrecy, shall be taken into consideration and be weighed against the rights of the accused. In such cases, only such measures restricting defence rights which are *strictly necessary* are permissible under Article 6(1) ECHR, and such restrictions should be sufficiently counterbalanced by the procedures followed by the judicial authorities (ECtHR, 2024, paragraph 191). The importance of the undisclosed material and its use in the trial remains of central importance to assess whether defence rights have been violated (ECtHR, 2024, paragraphs 193–194). As regards cases where the prosecution files include electronic data, the defence shall be able to be involved in the laying down of the criteria for determining what may be relevant for disclosure. Moreover, the refusal to allow the defence to have further searches of identified or tagged data may violate the right to be provided with adequate facilities for the preparation of the defence. Finally, the defence must be able to assess the

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

integrity and *reliability* of the evidence presented in court (cf. Oerlemans and Royer, 2023; Stoykova, 2023; Kipker and Bruns, 2022). If this is not possible, the burden falls even more heavily on national authorities to subject such evidence to the highest level of scrutiny (ECtHR, 2024, paragraph 195).

The lack of sufficient knowledge and resources to confront evidence against oneself may impact adversely on the right to examine witnesses (Article 6 (3) lit. d ECHR). The term 'witness' shall encompass *any* evidence that is used in criminal proceedings and can support a conviction. In this sense, AI-generated output that supports a criminal investigation and arrives in the courtroom falls into the scope of this definition (cf. Gless, 2020; Palmiotto, 2021). The ability to challenge evidence can also be analysed through the lens of the presumption of innocence (PoI) (Article 6(2) ECHR, 48 CFR). Even if the prosecution or the court formally bears the burden of proof, the defence must be able to contest any (indirect) shifting of this burden, especially in cases where EU secondary law, in line with ECtHR jurisprudence (ECtHR, 2024, paragraphs 409–411), allows for legal and factual presumptions of criminal liability (recital 22 Directive (EU) 2016/343). When such evidence or presumptions stem from an AI system, the primary barrier to meeting the protection standards required by PoI is algorithmic opacity (Sachoulidou, 2023). This opacity may arise from multiple sources: deliberate corporate or institutional self-protection and concealment, including police secrecy; lack of technical expertise among the judiciary and defence to assess AI-generated evidence; a fundamental mismatch between the complexity of AI-driven decision-making and human cognitive capacities (Burrell, 2016).

Next, the fair trial principle includes the right to a reasoned judicial decision, ensuring that parties have been meaningfully heard. This requires judges to base their reasoning on objective arguments and uphold defence rights (ECtHR, 2024, paragraph 198). Moreover, reasoned decisions are essential for safeguarding the right to appeal. This remains just as critical when AI-generated evidence is admitted in criminal proceedings (Palmiotto, 2021; Franssen and Berrendorf, 2021) – with the lack of sufficient knowledge of the inner workings of such systems posing a significant obstacle to compliance with this rule-of-law principle.

Lastly, reliance on AI-generated evidence may challenge compliance with the *in dubio pro reo* principle (Article 6 (2) ECHR, 48 CFR). This principle is considered to have been violated when a judicial decision is not sufficiently reasoned as well as when the defence faces an extreme and unattainable burden of proof depriving them of the slightest prospect of success (ECtHR, 2024, paragraph 407). This is particularly relevant for AI-powered crime analytics systems, as their use in criminal proceedings may distort legal reasoning and impose overwhelming challenges on the defence, particularly in terms of the resources needed to contest AI-supported conclusions.

Moreover, the *in dubio pro reo* principle is put under strain in an environment where AI outputs create the illusion of certainty and objectivity, seemingly surpassing the fallibility of human judgement (cf. Peršak, 2021). Even when doubt persists

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

(for instance, in cases where the error rate of an AI system is disclosed), it remains unclear how much doubt is required to override the algorithmic output and exonerate a defendant (Sachoulidou, 2023).

5.3 AI-POWERED CRIME ANALYTICS TOOLS: THE NORMATIVE CONTEXT

At the EU level, the development and use of AI-powered crime analytics tools should be placed in the normative context shaped by the AIA, as complemented by the EU fundamental rights legislation and the EU data protection *acquis*. The AIA seeks to balance between innovation and effective protection of health, safety and fundamental rights (Article 1(1) AIA). In this context, it includes a definition of AI systems, confirming that AI is best understood as a socio-technical concept (Barabas, 2020). More specifically, AI systems are defined as 'machine-based system(s) designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infer, from the input (they) receive, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' (Article 3(1) AIA). Crime analytics tools may fall into the scope of this definition, provided they are not limited to following predefined, explicit instructions or operations, or they are solely intended for descriptive analysis, hypothesis testing, and visualisation, *but rather learn, reason or model at any stage of their lifecycle* (European Commission, 2025a, p. 9).

Next, the AIA stands out for its top-down approach to risk regulation (De Gregorio and Dunn, 2022) that presents varying levels of density (Ebers, 2022). At the core of this approach is the assessment of an AI system's impact on health, safety, and fundamental rights (recitals 7 and 46 AIA). The AIA categorises AI systems into the following risk categories (for an analysis focused on automated law enforcement see Sachoulidou and Vavoula, 2025):

1. *Unacceptable risk* leads to a prohibition that may be waived under certain conditions (Article 5 AIA; see European Commission, 2025b). In the area of law enforcement, this category includes AI systems that are employed for 'making risk assessments of natural persons in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics' (Article 5(1) lit. d AIA) and 'real-time' remote biometric identification systems employed in publicly accessible spaces (Article 5(1) lit. h AIA).
2. *High risk* results in a series of minimum requirements for providers, deployers and third parties (Articles 8–49 AIA). This includes AI systems that have a 'significant harmful impact on the health, safety and fundamental rights' (recital 46 AIA). Such AI systems may be intended to be used as a safety component of a product or may be products themselves and, as such, are required to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

undergo a third-party conformity assessment with a view to their placement on the market or being put into service (Article 6(1) AIA). Besides this, this category encompasses stand-alone AI systems deployed in the areas of activities listed in Annex III to AIA (Article 6(2) AIA). In the area of law enforcement, point 6 of Annex III to the AIA explicitly classifies as high-risk *only* those AI systems which are intended to be used to: assess a natural person's risk of becoming the victim of criminal offences; serve as polygraphs or similar tools; evaluate evidence reliability; assess the likelihood of a natural person of (re-)offending not solely based on profiling of natural persons as referred to in Article 3(4) of the Directive (EU) 2016/680 (Law Enforcement Directive (LED)), or personality traits and characteristics or past criminal behaviour of natural persons or groups; profile natural persons as referred to in Article 3(4) LED in the course of crime detection, investigation, or prosecution.

3. AI systems intended to interact directly with natural persons pose a *limited risk* and, as such, should comply with transparency requirements (Article 50 AIA); that is, the natural persons concerned should be informed that they are interacting with AI. This does not apply to 'AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, ... unless those systems are available for the public to report a criminal offence' (Article 50(1) AIA).
4. The deployers of AI systems that present a *minimal risk* should create codes of conduct, including related governance mechanisms, to promote the *voluntary* application of some or all the mandatory requirements applicable to high-risk AI systems (Article 95 AIA).

In the light of these categorisations, AI-supported crime analytics tools, which do not serve any additional purpose out of the above-mentioned ones, nor fall into the scope of point 8 of Annex III to AIA ('AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts [...]'), will be governed by flexible standards, an outcome that prioritises an effectiveness-focused approach to automated law enforcement (cf. European Police Chiefs, 2022). Notably, the Council of the EU (2022) edited out Annex III point 6 lit. g AIA, introducing an exception for crime analytics that is meant to address contemporary investigative needs. Despite the disagreement at the level of the European Parliament (2023), this exception was preserved in the final text of the AIA.

Additionally, Article 6(3) AIA introduces exceptions to the automatic classification of AI systems deployed in designated high-risk areas. The primary rationale is that such systems do not necessarily have a significant impact on decision-making, nor they harm substantially health, safety or fundamental rights (recital 53 AIA). This exception encompasses cases where an AI system is intended to: (1) perform a narrow procedural task; (2) improve the result of a previously completed human activity; (3) detect decision-making patterns or deviations from prior decision-making patterns, without replacing or influencing the previously completed human assessment,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

without proper human review; or (4) perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. This *appears to* be the case with crime analytics tools that perform 'merely' narrow procedural tasks, such as translation or entity extraction, and 'only' preparatory tasks to the ultimate law enforcement and judicial decision-making.

This stance conflicts, however, with the data-intensive processes involved in developing and training AI-powered crime analytics tools. The accuracy and reliability of their output (to the extent that the latter is not merely a visualisation of a certain dataset) can be significantly compromised when such systems are developed/trained on low-quality, biased or otherwise non-representative data (see, for instance, Mittelstadt et al., 2016; Ryan, et al., 2019; FRA, 2020), leading to unjust identification of individuals (rather than patterns) (cf. recital 59 AIA). Next, given that crime analytics tools are meant to facilitate complex criminal investigations and, accordingly, inform criminal proceedings, opacity coupled with lack of documentation may significantly undermine the exercise of fundamental procedural rights, particularly if the algorithmic output is admitted as evidence.

Moreover, crime analytics systems will fall outside the protective scope of Article 86 AIA, which grants a right to clear and meaningful explanation *only for decisions based on high-risk AI outputs*. As a result, affected individuals will have to rely on general legal frameworks for remedies. This is particularly concerning when AI has the potential to influence criminal proceedings. Notably, recital 59 AIA already stresses 'the difficulty in obtaining meaningful information on the functioning of (AI) systems (employed for law enforcement purposes) and the resulting difficulty in challenging their results in court, in particular by natural persons under investigation' – *but only with regards to high-risk AI systems*.

Lastly, the editing out of crime analytics systems does not take into consideration the risk of their (reasonably foreseeable) misuse (cf. Article 3 nr. 13 AIA) in operational settings. Such misuse may take the form of repurposing a crime analytics tool for profiling purposes. Besides this, an even more usual case would be to incorporate crime analytics tools into other existing AI systems; the latter may be high-risk and, thus, higher standards will apply to their development. Yet, crime analytics tools would be originally developed without similar restrictions. Additionally, the crime analytics exception fails to consider the power imbalance that is inherent into the law enforcement environment, even though power imbalance has been listed among the criteria that may be used for the purposes of adding or modifying use cases of high-risk AI systems pursuant to Article 7 AIA.

5.4 HOW TO MERGE SOCIO-ETHICAL, LEGAL, AND TECHNICAL STANDARDS: THE MATCHING EXERCISE

A risk-based approach is crucial for regulating AI, as reflected in the AIA's focus on protecting fundamental rights, though its limited guidance as to how to conduct an

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

impact assessment (Mantelero and Marí, 2025) and the complexity of AI systems necessitate diverse, tailored assessment methodologies integrating socio-ethical, legal, and technical standards. Given the special features of AI-powered crime analytics tools and considering that the law enforcement context is not, nor should be, exempted from (public) scrutiny (Mantelero and Fanucci, 2024), this section presents a model-template, called 'matching exercise' (ME) for ensuring a fundamental rights-by-design approach to AI in law enforcement settings. This assessment framework consists of a set of questions designed to address socio-ethical and legal implications of the development and use of AI in the law enforcement environment, combining different methodologies: an Ethical Impact Assessment (EIA), Social Impact Assessment (SIA), and Human Rights Impact Assessment (HRIA). In this way, it aims to enable a holistic approach to AI impact.

An EIA provides a methodological framework to ensure that the development of AI systems 'align(s) with the promotion and protection of human rights and human dignity, environmental sustainability, fairness, inclusion, and gender equality' (UNESCO, 2023, p. 5). It includes an *ex ante* assessment of the development phase of an AI system and an *ex post* assessment of the commercialisation phase, covering its entire lifecycle. In this context, ethics serves as a complement to legal standards. Given that the profound societal impact of AI cannot be fully mitigated by human rights laws alone, it often requires a nuanced approach that considers both community choices and individual autonomy, thereby pointing to the need of an analysis of socio-ethical values in context (Mantelero, 2022, p. 93). This means an EIA relies significantly on stakeholder engagement, ethical perceptions, and real experiences of those involved (UNESCO, 2023), which requires a context-sensitive and participative analysis of community values where the AI solutions are to be implemented (Mantelero, 2022, p. 93).

Another dimension that complements ethical accounts for human protection consists of the societal consequences of developing AI tools. A SIA encompasses 'processes of analysing, monitoring and managing the intended and unintended social consequences, both positive and negative, of planned interventions (policies, programmes, plans, projects) and any social change processes invoked by those interventions' (IAIA, 2015, p. 1). It typically relies on local knowledge and participatory processes to assess the concerns of interested and affected parties (Vanclay, 2003, p. 6), bringing together different stakeholders to monitor the social impact of a planned intervention and analyse its alternatives. The challenge consists of defining comprehensively what qualifies as social impact or social risk as 'all issues that affect people, directly or indirectly, are pertinent to (SIA)' (Vanclay, 2003, p. 8). In the AI context, a SIA should assess technical features that may be inaccessible to the public, professionals, or vulnerable groups affected by an AI system. Moreover, an AI system may have the potential to affect an undefined geographical community or population, making it impossible to determine which concrete stakeholders should participate in SIA procedures.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Alternatively, one may deploy a 'conceptual and procedural framework (that) guarantees the promotion and protection of human rights in policies, programs, plans and projects' (IAIA, 2015, p. 6). An HRIA can be defined as 'a process for identifying, understanding, assessing, and addressing the adverse effects of a project or activities on the human rights enjoyment of impacted right-holders' (The Danish Institute for Human Rights, 2020, p. 7). Employing an HRIA means: (a) placing human rights and the principles arising therefrom at the centre of attention; (b) requiring accountability and transparency on the part of duty-bearers towards right-holders; (c) fostering empowerment of right-holders and capacity building; (d) ensuring that the meaningful participation of right-holders in development processes and planned interventions is recognised as an intrinsic right; (e) facilitating the non-discriminatory engagement of right-holders and prioritising vulnerable or marginalised individuals or groups (The Danish Institute for Human Rights, 2020, p. 7).

To effectively implement an HRIA in an AI system under development, there are *five* steps to follow: (1) plan and define the scope of the system under evaluation; (2) collect data and develop a baseline; (3) analyse impact considering the risks pointed out; (4) mitigate and manage risks; (5) report and evaluate (The Danish Institute for Human Rights, 2020, p. 7; cf. Mantelero and Marí, 2025). Additionally, any assessment model should develop a self-assessment tool (questionnaire) to 'identify values, rights and freedoms at risk, as well as relevant groups of rights-holders involved' (Mantelero and Fanucci, 2024, p. 7), as well as 'an *ad hoc* expert committee' (Mantelero, 2018, p. 758) to guarantee an independent review of the design choices, the contents of the questionnaire, the appropriateness and clarity of the questions, and propose improvements.

The ME serves as a self-assessment tool for developers and providers of AI-powered crime analytics tools. The development of such a tool requires determining: the relevant variables or risks that should be taken into account; the methods used to assess them and to develop risk indices; the contribution of standard questionnaires to this process along with their limitations; and the importance of expert-based evaluation in conducting the assessment (Mantelero and Marí, 2025, p. 6). Driven by this, the *first step* in designing the ME is to identify the *variables* (or risk definition on the grounds) to be tested based on the AIA's minimum requirements for high-risk AI systems (Articles 9–15 AIA), given the criticism expressed above as to the editing out of AI-enabled crime analytics from Annex III (see Section 5.3).

These requirements are used as the basis for designing a set of *questions* in the form of an *AIA compliance test*, which assesses risk management (Article 9), data governance (Article 10), technical documentation (Article 11), record-keeping (Article 12), transparency (Article 13), human oversight (Article 14), accuracy, robustness, and cybersecurity (Article 15) (for an example see Table 5.1). Additionally, socio-ethical considerations, including human rights principles arising from key legal frameworks,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CF15C048B4E80003C398D145

TABLE 5.1 *AIA compliance test (example)*

Matching Exercise (ME)					
	Essential requirements				
EU AIA	Risk Management System (art 9)	Questions	AI Tool's Features	Project Deliverable	Observations
Art 9 (1)	Definition of the risk assessment system	Does the AI system have a risk assessment system to be established, implemented, documented and maintained for the system's entire lifecycle? Does the AI system have a technical document informing the system's intended purpose and any potential misuse that could be reasonably foreseen? Does the AI system identify possible threats (design faults, technical faults, environmental threats) and possible consequences thereof? Does the AI system inform the end-user of existing or potential risks? If yes, how?			

such as the ECHR and the CFR, are integrated into the ME design. Questions within these components of the ME are associated with the detection of privacy threats, the impact of false positives and false negatives, and a detailed focus on bias detection and mitigation (see Section 5.5), which can be critical due to their direct social and legal implications in AI-enabled crime analytics.

To turn the ME into a 'user-friendly' assessment tool, a glossary with terms and concepts can be added, including definitions of technical terms and examples as to how to address the questions.

In the *second stage*, oriented to data collection, this participatory approach implies that the ME should be shared with potentially affected groups or their representatives, partners of the building system (technical, legal), and relevant stakeholders (community, advisers, and so on), who should be selected based on their involvement in the development of the AI system in question and their familiarity with AI as a general concept. Additionally, a meaningful impact assessment should include transparency guidelines that 'promote multi-stakeholder participation to bridge the gap between ethical principles and concrete practices of developers' (Mantelero and Fanucci, 2024, p. 1).

The *third stage* involves a qualitative analysis of the responses to assess the potential impact of the system's features and decisions, and identify risk mitigation measures. To generate such insights, deductive and inductive approaches can be useful (Creswell and Tashakkori, 2007). A deductive approach involves checking existing patterns and requirements against the data in a top-down fashion. This 'top-down' method helps to assess if the system aligns with existing standards or norms. An inductive approach works from the 'bottom up'. It can be adopted to identify, analyse, and organise raw data into unified themes of information that indicate the AI system's potential impact. Combining these approaches over an interpretive textual analysis can help understand contextual specifics of the responses contributing to better tailored measures to mitigate risks and impacts across the different development stages of an AI system. This can be done by analysing the likelihood and severity of an adverse impact to construct a risk index, as identifying the level of risk both prior to and following the application of preventive or corrective actions is necessary to show that the risk has been clearly and effectively managed (Mantelero and Marí, 2025).

The *last stage* involves a report, or a set of recommendations based on the impact assessment's results that should be public, promoting transparency and facilitating future revision of the assessment tool and the measures adopted (Mantelero, 2025).

5.5 ETHICS AND FUNDAMENTAL RIGHTS-BY-DESIGN: IDENTIFYING BIAS DETECTION AND MITIGATION MEASURES FOR FAIRER OUTCOMES

AI-enabled crime analytics systems are prone to various biases that influence algorithmic and human decision-making processes and data interpretation. While the

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

sources of such biases are widely debated, biases associated with AI-enabled law enforcement tools are generally characterised by two dimensions: *inaccuracy* – where predictions deviate from reality, and *undesirability* – where AI-generated outcomes reinforce harmful or unfair effects (Zajko, 2021). These dimensions may overlap but should not be conflated, as an AI system's output can be factually accurate while still leading to undesirable social consequences. This points to the complexities of biases in AI systems which can perpetuate their own biases exacerbating inequalities (FRA, 2022) and flawed decision-making in policing. To mitigate these risks, the AIA mandates strict bias detection and mitigation measures for high-risk AI systems. Article 10 (2) lit. f–g AIA requires developers to assess and address biases to prevent adverse effects on fundamental rights, health, and safety, while Article 10 (5) lit. a–f AIA imposes strict controls on sensitive data processing to balance bias mitigation with privacy protection.

Yet, challenges remain in effectively addressing bias in AI-enabled law enforcement tools manifested in two ways: first, existing bias mitigation measures may be inadequate, as solutions are not yet sufficiently developed to account for the complexities of bias detection and mitigation in these systems. Second, even targeted mitigation efforts may fall short if they fail to consider the broader socio-technical context in which such AI tools operate, including their interdependencies, and human dynamics. Overlooking this context can influence the classification of crime analytics tools, potentially allowing biases to persist and leading to discriminatory outcomes. Moreover, such oversight may compromise the integrity and reliability of evidence derived from these systems in criminal proceedings (see Section 5.2). Therefore, understanding the nature of biases imposed on AI-enabled crime analytics tools and developing robust mitigation measures are necessary to safeguard against discriminatory practices and promote responsible and ethical innovation and governance in the law enforcement environment.

This section explores the complexities of bias in AI-enabled crime analytics tools, and provides a knowledge base for self-assessment tools, such as the ME (see Section 5.4). It identifies the types of biases detected in such AI tools and existing mitigation measures to inform relevant risk management and policy decisions. It builds on results from a scoping review conducted for AI-enabled crime analytics tools within the TRACE project (see Sachoulidou et al., 2024). The results indicated a broad spectrum of biases in AI-enabled crime analytics tools across their lifecycle, including both pre-development (ideation) and post-deployment (governance) phases: individual biases, societal biases, and algorithmic biases. These biases tend to be horizontally applicable across different types of AI tools intended to be used for law enforcement purposes.

Socio-cognitive biases can be induced by police officers' use of AI systems, which influence their decision-making. Automation bias occurs when officers overly rely on automated suggestions, disregarding external evidence (Alon-Barkat and Busuioc, 2023). Police officers are more susceptible to confirmation

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

bias – favouring information that supports preferred conclusions, leading to selective and biased information processing, as well as anchoring bias – a cognitive bias that influences decision-making towards information that appears to match (or amplify) their subjective arbitrary reference points (Datta, Whitmore and Nwankpa, 2021). Officers tend to trust AI recommendations that align with their professional knowledge (Selten, Robeer, and Grimmelikhuijsen, 2023), reinforcing existing stereotypes and creating a feedback loop where biased AI predictions perpetuate biased law enforcement practices (Alon-Barkat and Busuioc, 2023). This consequence is observed in digital forensics related to the construction or reconstruction of (chain of) evidence that is at the core of AI-enabled crime analytics (Leone, 2021).

On a social level, AI biases can stem from broader structural inequalities embedded in institutions and social norms. In AI ethics, much attention is given to discrimination against protected categories such as race, gender, and disability (Zajko, 2021) – often termed 'discrimination bias'. However, in policing, these biases tend to be examined separately. For instance, racial bias as a byproduct of racial profiling has been found embedded in AI-driven law enforcement tools leading to wrongful identification of marginalised communities (Gentzel, 2021). Data used in crime analytics, such as report filing (Davis et al., 2022) can reinforce such a bias. Gender bias, often intertwined with racial bias, reflects the practice of assigning specific attributes or roles based on gender (OHCHR, 2020). Gender classification algorithms have been shown to perform less accurately for women than men, reflecting biases in police training data (Xiang, 2022). They can lead to fairness biases, which reflect historical inequalities embedded in AI policing tools (Cardenas and Vallejo-Cardenas, 2019), financial crime analytics (Moldovan, 2023), and anti-corruption technologies (Odilla, 2023).

Biases linked to specific social categories often manifest as algorithmic biases, emerging at various AI system stages, including design, data collection, training, testing, and deployment. Pre-existing bias in training data stems from inherent dataset biases. Crime analytics tools, for instance, may rely on legal datasets that introduce algorithmic biases, as historical inequalities in court data and variations in legal rule programming can produce discriminatory outcomes (Grosso et al., 2014). This negative legacy bias is further compounded by representation bias, where underrepresentation of certain groups leads to poor generalisation and skewed results (Yan, Kao and Ferrara, 2020). In AI tools using large language models, such as crime analytics, framing bias influences causal interpretations and moral evaluations, leading to misclassification or inappropriate semantic categorisation (Zola et al., 2022). Aggregation bias arises when distinct groups requiring separate treatment are processed uniformly, distorting outcomes, and can be worsened by contaminated data or adversarial manipulation. Consequently, flawed data representation, contextual loss, or oversimplified modelling and evaluation metrics contribute to systematic prediction errors.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

When AI-enabled crime analytics tools are applied to real-life conditions, a deployment bias can occur as real-life conditions diverge from training environments, leading to unfair or inaccurate outcomes (Hutiri and Ding, 2022). As AI-enabled crime analytics systems start interacting with multiple users, unintended discriminatory patterns may be reinforced, leading to emergent biases. From a governance perspective, biases have been identified in ethical impact assessments used alongside crime analytics tools, particularly in population composition assessments (Guo and Kennedy, 2023), financial decision-making, and algorithmic risk assessments in the criminal justice system (Zilka et al., 2023), making them prone to biases both independently and through their interconnectedness within law enforcement socio-technical systems (Purves, 2022).

Mitigation measures align with this perspective, addressing *micro-* (algorithmic, developer, and user biases), *meso-* (organisational culture), and *macro-* (socio-cultural implementation) levels, therefore contributing to a holistic mapping of diverse dimensions to be integrated in relevant assessment tools. At the micro level, no concrete strategies are identified to directly mitigate individual biases. Instead, emphasis is placed on the role of technology developers, highlighting the need for interdisciplinary learning as a prerequisite to understand how race, gender, and systemic inequalities are embedded in society. This ontological engagement is considered critical for developing classification models, which are often tasked with categorising race, gender, and behavioural traits for investigative purposes without necessarily examining how these categories intersect with social hierarchies and historical discrimination (Zajko, 2021). Self-assessments of AI tools could encourage such an engagement in law enforcement settings.

Yet, the focus lies upon algorithmic interventions to bias mitigation, including data pre-processing, in-processing interventions, post-processing adjustments, and fairness-aware algorithm design that primarily target biased training data, model assumptions, and feedback loops. Although a bias-free AI tool cannot be suggested, bias-aware data analytics can aid bias mitigation of AI-enabled crime analytics, and more broadly policing tools through ecologically valid datasets (Hutiri and Ding, 2022), dataset augmentation, as well as re-sampling for diversity (Amini et al., 2019). In crime analytics tools that use natural language processing (NLP) techniques, mitigation strategies can include modifying word embeddings for gender neutrality or augmenting language corpora to break biased associations, albeit indirect discrimination (i.e., discrimination by proxy) may still occur (Fosch-Villaronga et al., 2021). Fairness-aware model design emphasises integrating fairness into training rather than relying on *post hoc* corrections. For example, Wang et al. (2019) proposed replacing explicit fairness metrics with a secondary classifier trained on human judgements. For real-world applicability, AI models were recommended to be assessed using social-minded quality measures to reduce the reinforcement of societal biases (Du et al., 2020), aspects that may be overlooked if rigorous assessment standards do not apply.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

That is, technical solutions alone may not suffice; ethical considerations need to be embedded in crime analytics tools. Yet defining 'fairness' remains a key ethical challenge (Silva and Kenney, 2019). Participatory design methods that engage stakeholders can help build trust between data collectors and impacted communities (Xiang, 2022) and promote a better understanding of what constitutes 'fair treatment'. For example, AI-enabled policing tools analysing social media data without community input can exacerbate discrimination by misinterpreting cultural and linguistic nuances (Frey et al., 2020). Beyond fairness, adhering to human-centric principles – transparency, accountability, data integrity, and autonomy – is central to effective mitigation (Hung and Yen, 2021). This necessitates socio-technical approaches which enable human interaction with and correction of biased AI outputs as a systematic, normative practice.

Audits can serve as a critical mechanism towards socially responsible AI-enabled investigative tools. Effective audits extend beyond technical evaluations of data and algorithms to interrogate the theoretical assumptions embedded in model design and their broader social impact (Ugwudike, 2022). Internal and external audits have increasingly been recognised as essential accountability measures, helping to identify conduits of bias, embed ethical principles in AI systems, and prevent potential harms before deployment (Ugwudike, 2022). Transparency tools, such as model cards, facilitate collaboration between AI developers, policymakers, and end-users, integrating diverse perspectives into bias assessments (Akter et al., 2021). Psychological audits have been proposed to assess AI-driven predictions of human traits and behaviours impartially (Landers and Behrend, 2023), while interactive tools like D-BIAS enable human-in-the-loop interventions to visualise and modify causal structures in datasets (Ghai and Mueller, 2022). As AI continues to shape law enforcement decision-making, robust auditing frameworks need to be introduced to mitigate bias in crime analytics tools.

However valuable their contributions to bias mitigation, these measures can only partially influence the outcomes of AI-enabled law enforcement tools. This is because these tools operate within a broader socio-technical system of policing that is not independent from human dynamics. In this sense, establishing appropriate organisational safeguards (meso-level) is crucial when implementing AI in law enforcement (Grimmelikhuijsen and Meijer, 2022), a dimension that has not been properly examined and integrated in relevant regulatory frameworks. Organisational self-monitoring, preparing algorithmic impact statements relative to organisational culture, increasing gender diversity within law enforcement and inter-agency collaboration (Zilka, Sargeant and Weller, 2022) have been proposed to counteract biases in AI design and oversight. In combination, this evidence suggested that institutional and bureaucratic reforms, standardised operating procedures, transparency in procurement processes, analysing governance limitations, and establishing *ex post* mechanisms for accountability and redressal can be increasingly needed to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

mitigate systemic biases in AI-driven law enforcement decision-making, including in the use of crime analytics tools.

On a macro level, bias mitigation measures focus on systemic, legal, and societal interventions to address structural inequalities. A key strategy involves enhancing policing technological capabilities to be inclusive and remain responsive to evolving societal conditions, such as dynamic changes in the people, types and locations of crimes without undermining regulatory constraints (Fosch-Villaronga et al., 2021). This necessitates treating AI-enabled law enforcement as a socio-political, rather than purely technical issue, where interdisciplinary approaches engage with historical and social contexts to transform unjust social structures and drive meaningful change (Zajko, 2021). Moving beyond simply identifying bias to evaluate which AI system's uses are harmful, to whom, and why, points to the social justice implications of algorithmic decision-making (Drage and Frabetti, 2024) and a key dimension for future self-assessment frameworks.

5.6 CONCLUSIONS AND RECOMMENDATIONS

The use of AI-enabled crime analytics tools can pose concerns for fundamental rights, fairness, and justice, highlighting the need for a multidimensional regulatory approach, informing the current AIA's approach to them (Sachoulidou, 2024). Legislatively, there is an urgent need for specific rules governing automated law enforcement, focusing on complaint and redress mechanisms, greater transparency, and clear evidentiary standards in criminal proceedings where the algorithmic output may be admitted as evidence. Such measures should be complemented by procurement guidelines for AI use in law enforcement settings (European Parliament, 2021, paragraph 17). Soft-law measures, including impact assessments and mandatory periodic audits of their results (European Parliament, 2021, paragraph 18), can help implement a fundamental rights-by-design approach, even where such an assessment is not mandatory (cf. Article 27 AIA). Promoting AI literacy among developers and deployers is essential – not just to understand the technology, but also its ethical risks and limitations (European Parliament, 2021, paragraphs 22–23). This is evident in measures to address bias that require action at the individual (micro), organisational (meso), and societal (macro) levels.

REFERENCES

Akter S., McCarthy G., Sajib S., Michael K., Dwivedi Y. K., D'Ambra J., & Shen K. N. (2021) Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management*, 60, 102387.

Alon-Barkat S. and Busuioc M. (2023) Human–AI interactions in public sector decision making: 'automation bias' and 'selective adherence' to algorithmic advice. *Journal of Public Administration Research and Theory*, 33(1), pp. 153–169.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Amini A., Soleimany A.P., Schwarting W., Bhatia S.N., and Rus D. (2019) Uncovering and mitigating algorithmic bias through learned latent structure. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 289–295.

Barabas C. (2020) Beyond bias: 'Ethical AI' in criminal law. In Dubber M., Pasquale F. and Das S. eds., *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press, pp. 737–753.

Buijsman S., Klenk M., and van den Hoven J. (2025) Toward a 'design for values' approach. In Smuha N. ed., *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge: Cambridge University Press, pp. 59–78.

Burrell J. (2016) How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society* 3(1), pp. 1–12.

Cardenas S. and Vallejo-Cardenas S. F. (2019) Continuing the conversation on how structural racial and ethnic inequalities affect AI biases. In *2019 IEEE International Symposium on Technology and Society (ISTAS)*, pp. 1–7.

Council of Europe (2017) *Algorithms and Human Rights. Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications*. Study prepared by the Committee of Experts on Internet Intermediaries (MSI-NET). Available at: https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html (Accessed 25 August 2025).

Council of the EU (2022) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach. Available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf (Accessed 25 August 2025).

Creswell J. W. and Tashakkori A. (2007) Differing perspectives on mixed methods research. *Journal of Mixed Methods Research* 1(4), pp. 303–308.

Datta P., Whitmore M., and Nwankpa J. K. (2021) A perfect storm: social media news, psychological biases, and AI. *Digital Threats: Research and Practice* 2(2), pp.1–21.

Davis J., Purves D., Gilbert J., and Sturm S. (2022) Five ethical challenges facing data-driven policing. *AI and Ethics* 2(1), pp. 185–198.

De Gregorio G. and Dunn P. (2022) The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review* 59(2), pp. 473–500.

Drage E. and Frabetti F. (2024) The performativity of AI-powered event detection: How AI creates a racialized protest and why looking for bias is not a solution. *Science, Technology, & Human Values* 49(5), pp. 1045–1072.

Du X., Hargreaves C., Sheppard J., Anda F., Sayakkara A., Le-Khac N. A., and Scanlon, M. (2020) SoK: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In *Proceedings of the 15th ARES International Conference on Availability, Reliability and Security*, pp. 1–10. Available at: https://arxiv.org/abs/2012.01987 (Accessed 23 April 2026).

Ebers M. (2022) Standardizing AI: The case of the European Commission's proposal for an 'Artificial Intelligence Act'. In Di Matteo L. A., Poncibò C. and Cannarsa M. eds., *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge: Cambridge University Press, pp. 321–344.

European Union Agency for Fundamental Rights (FRA) (2020) *Getting the Future Right. Artificial Intelligence and Fundamental Rights*. Available at: https://fra.europa.eu/en/publication/2020/artificialintelligence-and-fundamental-rights (Accessed 25 August 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

European Agency for Fundamental Rights (FRA) (2022) *The Fundamental Rights Report 2022*. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/FRA-2022-Fundamental-Rights-Report-2022-opinions_en.pdf (Accessed 25 August 2025).

European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM (2021) 206 final. 2021/0106 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (Accessed 25 August 2025).

European Commission (2025a) Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission – Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act). C (2025) 924 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (Accessed 25 August 2025).

European Commission (2025b) Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). C (2025) 884 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (Accessed 25 August 2025).

European Police Chiefs (2022) Joint Declaration on the AI Act (as approved by the European Police Chiefs during their informal meeting in Berlin on 24 May 2022). Available at: www.europol.europa.eu/cms/sites/default/files/documents/EPC%20Joint-Declaration%20on%20the%20AI%20Act.pdf (Accessed 25 August 2025).

European Court of Human Rights (ECtHR) (2024) Guide on Article 6 of the European Convention on Human Rights. Right to a fair trial (criminal limb). Available at: https://ks.echr.coe.int/web/echr-ks/all-case-law-guides (Accessed 25 August 2025).

European Parliament (2021) Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2021(INI)). Available at: www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (Accessed 25 August 2025).

European Parliament (2023) Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 2021/0106 (COD)). Available at: www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf (Accessed 25 August 2025).

Europol (2025) *Assessing Technologies in Law Enforcement: A Method for Ethical Decision-Making*. Luxembourg: Publications Office of the European Union.

Ferrer X., Van Nuenen T., Such J. M., Coté M., and Criado N. (2021) Bias and discrimination in AI: A cross-disciplinary perspective. *IEEE Technology and Society Magazine* 40(2), pp.72–80.

Fosch-Villaronga E., Poulsen A., Søraa R. A., and Custers B. H. M. (2021) A little bird told me your gender: Gender inferences in social media. *Information Processing & Management*, 58(3), 102541.

Franssen V. and Berrendorf A. (2021) The use of AI tools in criminal courts: Justice done and seen to be done? In Vermeulen G., Peršak N. and Recchia N. eds., *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*. Antwerp: Maklu, pp. 199–224.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Frey W. R., Patton D. U., Gaskell M. B., and McGregor K. A. (2020) Artificial intelligence and inclusion: Formerly gang-involved youth as domain experts for analysing unstructured twitter data. *Social Science Computer Review* 38(1), pp. 42–56.

Gentzel M. (2021) Biased face recognition technology used by government: A problem for liberal democracy. *Philosophy & Technology* 34(4), pp. 1639–1663.

Ghai B. and Mueller K. (2022) D-bias: A causality-based human-in-the-loop system for tackling algorithmic bias. *IEEE Transactions on Visualization and Computer Graphics* 29(1), pp. 473–482.

Gless S. (2020) AI in the courtroom: A comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law* 51(2), pp. 195–253.

González Fuster G. (2020) Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. Study requesttheby the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)656295 (Accessed 25 August 2025).

Grimmelikhuijsen S. and Meijer A. (2022) Legitimacy of algorithmic decision-making: Six threats and the need for a calibrated institutional response. *Perspectives on Public Management and Governance* 5(3), pp. 232–242.

Grosso C. M., O'Brien B., Taylor A., and Woodworth G. (2014) Race discrimination and the death penalty: An empirical and legal overview. In Lanier C. S., Bohm R., and Acker J. eds., *America's Experiment with Capital Punishment* (3rd ed.). Durham, NC: Carolina Academic Press, pp. 525–576.

Guo Z. and Kennedy L. (2023) Policing based on automatic facial recognition. *Artificial Intelligence and Law* 31(2), pp. 397–443.

Hung T. W. and Yen C. P. (2021) On the person-based predictive policing of AI. *Ethics and Information Technology* 23, pp. 165–176.

Hutiri W. T. and Ding A. Y. (2022) Bias in automated speaker recognition. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency*, pp. 230–247.

Kipker D.-K. and Bruns H. (2022) Encrochat und die 'Chain of Custody'. Digitale Ermittlungen alsBewährungsprobe für ein Recht auf faires Verfahren? *MMR* 5, pp. 363–368.

International Association for Impact Assessment (IAIA) (2015) *Social Impact Assessment. Guidance for assessing and managing the social impacts of projects*. Available at: www.iaia.org/news-details.php?ID=3 (Accessed 25 August 2025).

Landers R. N. and Behrend T. S. (2023) Auditing the AI auditors: A framework for evaluating fairness and bias in high stakes AI predictive models. *American Psychologist*, 78(1), pp. 36–49.

Lane L. (2022) Clarifying human rights standards through artificial intelligence initiatives. *International and Comparative Law Quarterly* 71(4), pp. 915–944.

Leone M. (2021) From fingers to faces: Visual semiotics and digital forensics. *International Journal for the Semiotics of Law-Revue internationale de sémiotique juridique* 34(2), pp. 579–599.

Mantelero A. (2018) AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review* 34, pp. 754–772.

Mantelero A. (2022) *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI. Information Technology and Law Series*. The Hague: Springer.

Mantelero A. and Marí. J. (2025) *FRIA model: Guide and use cases. FRIA methodology for AI design and development. DPD in Xarxa, Barcelona*. Available at: https://digimed.polito.it/2025/02/22/fria-model-guide-and-use-cases-fria-methodology-for-ai-design-and-development-barceclona-28-january-2025/. (Accessed 25 August 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Mantelero A. and Fanucci, F. (2024) *Governing AI: From Principles to Implementation in a Global World. Task Force 05 – Inclusive Digital Transformation. Policy Briefs. G20 – Brazil*. Available at: www.t20brasil.org/en/pbs?nucleo_id=5 (Accessed 25 August 2025).

Mittelstadt B. D., Allo P., Taddeo D., Wachter S. and Floridi L. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society*, pp. 1–21.

Moldovan, D. (2023) Algorithmic decision making methods for fair credit scoring. *IEEE Access* 11, pp. 59729–59743.

Odilla, F. (2023) Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime, Law and Social Change* 80(4), pp. 353–396.

Oerlemans J.-J. and Royer S. (2023) The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 14(4), pp. 434–458.

OHCHR (2020) *UN Human Rights Report* 2020. Available at: www.ohchr.org/en/publications/annual-report/ohchr-report-2020 (Accessed 25 August 2025).

Palmiotto F. (2021) The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings. In Ebers M., Cantero Gamito M. eds., *Algorithmic Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law*. Cham: Springer, pp. 49–70.

Peršak N. (2021) Automated justice and its limits: Irreplaceable human(e) dimensions of criminal justice. In Vermeulen G., Peršak N. and Recchia N. eds., *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*. Antwerp: Maklu, pp. 225–241.

Purves D. (2022) Fairness in algorithmic policing. *Journal of the American Philosophical Association* 8(4), pp. 741–761.

Ryan M., Brey P., Machnish K., Hatzakis T., King O., Maas J., Haasjes R., Fernandez A., Martorana S., Oluoch I., Eren S., and Van Der Puil R. (2019) D1.4 – *Report on ethical tensions and social impacts*. SHERPA project. Available at: https://doi.org/10.21253/DMU.8397134 (Accessed 25 August 2025).

Sommerer L. (2022) *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control: A Study of Person-Based Predictive Policing and the Algorithmic Turn*. Baden-Baden: Nomos.

Sachoulidou A. (2023) Going beyond the 'common suspects': To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. Available at: https://link.springer.com/article/10.1007/s10506-023-09347-w (Accessed 25 August 2025).

Sachoulidou A. (2024) Harnessing AI for law enforcement: Solutions and boundaries from the forthcoming AI Act. *New Journal of European Criminal Law* 15(2), pp. 117–125.

Sachoulidou A., Rego Oliveira C., Kordoni A., Hughes J., Nidhi Shiji A., and Nathan C. (2024) *D8.2 – The project's ethical, data protection and societal impact assessment*. TRACE project. Available at: https://cordis.europa.eu/project/id/101022004/results (Accessed 25 August 2025).

Sachoulidou A. and Vavoula N. (2025) Artificial intelligence and surveillance. In Lucarelli S. and Sperling J. eds., *Handbook of European Union Governance*. Cheltenham: Edward Elgar, pp. 156–170.

Sachoulidou A. (2026) A Typology of Automated Law Enforcement Systems Under EU Law: What Standards for Defence Rights? *European Papers* 11(1), pp. 595–630.

Selten F., Robeer M. and Grimmelikhuijsen S. (2023) 'Just like I thought': Street-level bureaucrats trust AI recommendations if they confirm their professional judgment. *Public Administration Review* 83(2), pp. 263–278.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Silva S. and Kenney M. (2019) Algorithms, platforms, and ethnic bias. *Communications of the ACM* 62(11), pp. 37–39.

Stoykova R. (2023) Encrochat: The hacker with a warrant and fair trials? *Forensic Science International: Digital Investigation* 46, 301602.

Straus J. (2021) Artificial intelligence: Challenges and chances for Europe. *European Review* 29(1), pp. 142–158.

The Danish Institute for Human Rights (2020) *Human Rights Impact Assessment Guidance and Toolbox*. Available at: www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox (Accessed 25 August 2025).

Ugwudike P. (2022) AI audits for assessing design logics and building ethical systems: The case of predictive policing algorithms. *AI and Ethics* 2(1), pp. 199–208.

UNESCO (2023) *Ethical Impact Assessment. A tool of the Recommendation on the Ethics of Artificial Intelligence*. Available at: www.unesco.org/en/articles/ethical-impact-assessment-tool-recommendation-ethics-artificial-intelligence (Accessed 25 August 2025).

Vanclay F. (2003) International principles for social impact assessment. *Impact Assessment and Project Appraisal* 21(1), pp. 5–12.

Wang T., Zhao J., Yatskar M., Chang K. W., and Ordonez V. (2019) Balanced datasets are not enough: Estimating and mitigating gender bias in deep image representations. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pp. 5310–5319.

Xiang A. (2022) Being 'seen' versus 'mis-seen': Tensions between privacy and fairness in computer vision. *Harvard Journal of Law & Technology* 36(1), pp. 1–60.

Yan S., Kao H. T., and Ferrara E. (2020) Fair class balancing: Enhancing model fairness without observing sensitive attributes. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*. New York: Association for Computing Machinery, pp.1715–1724.

Yeung K., Howes A., and Pogrebna G. (2020) AI governance by human rights-centered design, deliberation, and oversight: An end to ethics washing. In Dubber M., Pasquale F. and Das S. eds., *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press, pp. 76–106.

Zajko, M. (2021) Conservative AI and social inequality: Conceptualizing alternatives to bias through social theory. *AI & Society* 36(3), pp. 1047–1056.

Zilka M., Fogliato R., Hron J., Butcher B., Ashurst C., and Weller A. (2023). The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. New York: Association for Computing Machinery, pp. 1553–1569.

Zilka M., Sargeant H., and Weller A. (2022) Transparency, governance and regulation of algorithmic tools deployed in the criminal justice system: A UK case study. In *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*. New York: Association for Computing Machinery, pp. 880–889.

Zola F., Segurola-Gil L., Bruse J. L., Galar M., and Orduna-Urrutia R. (2022) Attacking Bitcoin anonymity: generative adversarial networks for improving Bitcoin entity classification. *Applied Intelligence* 52(15), pp. 17289–17314.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

6

Cross-Border Investigation of Financial Crime Empowered by AI

Adam Abukari, Dimitrios Kafteranis, Stefan Hopf, and Thea Sogenbits

6.1 INTRODUCTION

In today's interconnected world, the landscape of financial crime has significantly evolved. This is facilitated by fast advancements in technology and globalisation. As a result, it has never been easier to commit cross-border financial crime and to do so in many EU countries at the same time (Liu, Tian, and Shao, 2022; Rebovich, Kim, and Layne, 2021). For instance, financial transactions and communications now transcend borders of EU Member States with a lot of ease thanks to the integrated Single Market of the EU, which offers freedom of movement for assets, people, companies, goods, and services (European Commission, 2025). This poses significant challenges for law enforcement agencies (LEAs) charged with combating financial crimes. In Chapter 6, we seek to explore the transformative power and potential of artificial intelligence (AI) in harnessing cross-border investigations, providing a critical analysis on how AI technologies intersect with the pursuit of justice in relation to cross-border investigation of financial crime.

Although the digital revolution has facilitated the lives of many people and organisations significantly, it has also contributed to the sophistication and mutation of financial crimes such as money laundering and cyber enabled financial crimes. Criminals often take advantage of digital technologies to carry out their activities with impunity, by exploiting the seamless flow of information and the ease of digital transactions. The evolving landscape of financial crime and technological advancements requires LEAs to develop capabilities and strategies to address these emerging threats.

AI is a pivotal tool in enhancing the efficiency and effectiveness of investigations. AI technologies such as predictive analytics, natural language processing, and machine learning algorithms have transformed the identification, tracking, and prosecution of financial criminals across the EU (Europol, 2024; Europol, 2020). These technologies provide LEAs with the capability to unravel complex financial transactions, predict suspicious activities, and analyse vast datasets for patterns that indicate financial crime. Thus, despite significant benefits in cross-border

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

corporation and use of AI, challenges remain. These include variations in resource allocation and investigative capabilities across EU Member States, differing interpretations of EU law, fragmented digital evidence, and the increasing complexity of transnational crime, notably cybercrime and organised crime, which necessitate innovative cross-border strategies and collaboration (Europol, 2024; Europol, 2020).

This chapter explores how AI is reshaping and can revolutionise cross-border financial crime investigation in the EU. It addresses key technological advancements, financial crime landscape, cross-border regulatory challenges, and trust-based collaboration dynamics. In this regard, in the following four sections, we first elaborate on the evolving nature of cross-border financial crime and AI. We argue that cross-border cooperation is needed more than ever before. Second, we present key LEA cooperation arrangements in the EU and elaborate on general problems in law enforcement cooperation. Understanding these arrangements and general challenges is important because technology is only one element in a cooperative relationship. Third, we critically discuss how technology can harness or hinder cooperation, while the fourth section concludes the chapter.

6.2 EVOLVING NATURE OF CROSS-BORDER FINANCIAL CRIME AND AI

Crime evolves as society evolves. The nature of crime has been in a constant state of flux, reflecting the ever-changing social, economic, and technological landscape of our world. Technology has always, since its emergence and by extension its use in the functioning of societies, played a predominant role in traditional crimes and has continued to enhance and constitute a key driver in the creation of new forms of crime.

As borders become increasingly permeable and digital technologies advance, criminal activities have taken on an unmistakably cross-border character (Burton et al., 2025). The rise of transnational organised crime groups, coupled with the ease of moving funds and information across jurisdictions, has significantly challenged LEAs. Major stakeholders such as Europol and the Federal Bureau of Investigation (FBI) have warned about the spike in AI crime from 2022 onwards (Europol, 2025; FBI, 2024). This has also been confirmed by research such as the Alan Turing Institute and Centre for Emerging Technology and Security report on AI and serious online crime warning about the alarming rise in AI-driven crime (Burton et al., 2025).

Today's crime landscape is not only geographically unbound but is also evolving at the speed of technological innovation. Digital connectivity allows criminal actors to operate from anywhere in the world, executing illicit activities in multiple jurisdictions without ever leaving their country of origin (Europol, 2025). This global reach, combined with the instantaneous nature of digital communication, has compressed the timeline of criminal operations, allowing crimes to be planned, launched, and executed at unprecedented speeds and from several different places

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

around the globe. Organised crime previously was concentrated to one place or area, but nowadays we see that this is challenged by new technologies. Emerging technologies are not only used for communication purposes among criminals but also to commit relevant crimes.

Emerging technologies, particularly AI, have profoundly transformed both the methods and scale of criminal enterprise (Europol, 2025). Criminals not only rely on AI but also on other emerging technologies such as blockchain and quantum computing which enable them to accelerate their criminal activities (Europol, 2025). AI-enabled tools have opened new avenues for criminal exploitation beyond traditional cybercrime. Technologies such as deepfake generation, algorithmic profiling, autonomous botnets, and automated hacking tools now empower criminals to engage in identity theft, large-scale fraud, and sophisticated scams with minimal human effort (Burton et al., 2025). These AI-driven innovations not only scale up existing crimes but are also spawning entirely novel forms of digital transgressions that exploit gaps in regulatory and enforcement frameworks.

One particularly alarming consequence is the immense expansion in the number of potential victims. AI-generated phishing emails, fake customer service bots, and deepfake impersonations can target millions of individuals simultaneously. In addition, social media play a major part in people's everyday life where most of the victims are targeted (King et al., 2019). People spend more time online as it was the case some years ago. Although the financial damage to any single victim may be minor, the aggregate profits for criminals can be enormous, while the dispersed harm reduces incentives for victims to report incidents to LEAs, hampering detection and prosecution efforts.

Anonymity further compounds the challenge. Criminals can mask their identities more effectively than ever before, using encrypted communication channels, anonymisation networks, and AI-generated digital personas (FBI, 2024). For instance, encrypted communication technologies which were originally designed for cybersecurity, protection of personal data and privacy, are now major tool for criminal networks (Europol, 2025). Moreover, the rise of cryptocurrencies and decentralised financial products has made the traceability of illicit assets increasingly difficult (Carlisle, 2023). Transactions can be rapidly executed, fragmented, and laundered across multiple platforms, eroding the traditional tools LEAs rely on for tracking and seizing criminal proceeds.

The barrier to entry for engaging in AI-assisted crime has also fallen dramatically. The increasing low-threshold accessibility and usability of sophisticated technologies mean that criminals no longer need advanced technical expertise. User-friendly AI platforms, readily available malware-as-a-service offerings, and preconfigured hacking toolkits have democratised access to powerful criminal capabilities, enabling even low-skilled individuals to participate in complex illicit networks. Criminals have also resources to facilitate money laundering and to participate in

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

corruption both at local and international levels. These criminal activities happen online, and the advent of AI can only accelerate these phenomena (Europol, 2025).

On the other side, LEAs and regulatory bodies are racing to integrate AI into policing and investigative processes, deploying algorithmic surveillance, predictive analytics, and AI-driven cyber agents (Burton et al., 2024). However, the co-evolutionary nature of AI-enabled crime and AI-assisted law enforcement demands constant innovation. Criminals rapidly adapt, develop countermeasures, and exploit emerging technologies faster than legal systems can respond (Nerantzi and Sartor, 2024).

As the criminal landscape continues to evolve at pace, it is imperative that policymakers, law enforcement, and the public develop strategies that match the borderless, AI-driven dimensions of crime. International collaboration, robust regulatory frameworks, continuous investment in cutting-edge technology, and a deep understanding of the intricate interplay between criminal innovation and enforcement responses will be crucial to navigating this new era of technologically accelerated, globally dispersed criminality.

6.3 CROSS-BORDER COOPERATION BETWEEN LEAS IN THE EU

European police cooperation has undergone a dramatic transformation since its inception, evolving from largely bilateral arrangements to a complex system of multilateral frameworks and legal instruments designed to combat transnational crime and terrorism. Early cooperation faced significant obstacles, including diverse national legal systems, differing priorities, and limited information sharing mechanisms. The establishment of Europol in 1992, based on the Treaty on European Union (TEU), marked a pivotal shift towards a more coordinated approach, providing a central platform for information exchange, operational support, and strategic analysis. However, Europol's authority and effectiveness have been a subject of continuous debate, particularly concerning data protection under the Charter of Fundamental Rights of the European Union, 2000, and the delicate balance between national sovereignty and supranational policing powers.

Key instruments that underpin cooperation include the Prüm Treaty 2008, which facilitates the rapid exchange of DNA profiles, fingerprints, and vehicle registration data between participating Member States (European Union, n.d.). This Treaty, while not directly establishing a new EU body, has significantly enhanced practical cross-border investigations (FDFA, 2025). To further enhance cross-border cooperation in matters covered by Part III, Title V, Chapters 4 and 5 of the Treaty on the Functioning of the European Union (TFEU), the EU has promulgated the Prüm II Regulation (i.e., Regulation (EU) 2024/982 on the automated search and exchange of data for police cooperation).

The Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

JHA as well as subsequent framework decisions on specific crime areas have further harmonised legal bases and procedural rules across the EU. The creation of Eurojust in 2002, based on the Treaty of Amsterdam, 1999 added another layer of cooperation, providing a structure for judicial cooperation in criminal matters.

The activation of Secure Information Exchange Network Application (SIENA) has been central to cross-border information exchange, acting as Europol's information hub for law enforcement across the EU. Through SIENA, European competent authorities can share 'information in a swift, secure, and user-friendly way, with each other, Europol, and a number of third parties' (European Commission, n.d.1). The databases of SIENA provide cooperation facilitation for cross-border law enforcement whereby EU Member States can identify common investigations, making it possible for strategic and thematic analysis to be conducted. Additionally, Directive (EU) 2023/977 on the exchange of information between the law enforcement authorities of Member States has established harmonised rules for the adequate and rapid exchange of information between the competent law enforcement authorities for the purpose of preventing, detecting, or investigating criminal offences. Another important instrument is the European Criminal Records Information System (ECRIS), which was established in April 2012 to enhance information exchange on criminal records across the EU. This system not only ensures that there is uniform, fast and compatible information exchange on convictions between EU Member States but also it provides judges and prosecutors with easy access to comprehensive information on the criminal history of persons concerned (European Commission, n.d.2). In relation to information exchange on financial matters, Directive (EU) 2019/1153, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation, or prosecution of certain criminal offences, has facilitated access to and the use of financial information and bank account information by relevant competent authorities across the EU.

Furthermore, the ongoing development and implementation of the Schengen Information System II (SIS II) provides a crucial tool for exchanging real-time information on wanted persons, stolen property, and other relevant data. The European Public Prosecutor's Office (EPPO), established in 2017 under Regulation (EU) 2017/1939, represents a significant step towards centralised prosecution of EU-wide crimes, primarily focusing on offences against the EU's financial interests. However, its jurisdiction is currently limited to participating Member States, highlighting the ongoing challenges in achieving complete harmonisation.

The Council of Europe Convention on Cybercrime, 2001 (Budapest Convention) significantly enhances international cooperation in gathering and sharing information crucial for investigating and prosecuting cybercrimes, indirectly impacting the fight against white-collar crime. By establishing harmonised legal frameworks for accessing and transferring electronic evidence across borders, the Convention facilitates investigations into complex financial schemes often concealed online. The Convention's provisions on computer-related offences, data protection, and mutual legal assistance

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

streamline the process of obtaining crucial digital evidence, such as financial records or communications, which are frequently central to white-collar crime cases. This improved information flow allows for more effective cross-border investigations and prosecutions, thereby increasing the likelihood of apprehending perpetrators and recovering illicit assets.

The EU Electronic Evidence Legislative Package, 2023 (European Commission, n.d.3) has built upon the above Europe-wide Convention and contextualised cross-border electronic information exchange in the EU. It seeks to ensure easier and faster electronic evidence exchange between law enforcement and judicial authorities in investigating and prosecuting criminals. The package consists of Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, and Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering e-evidence in criminal proceedings, which has: created a European Production Order (for information exchange between authorities); created a European Preservation Order; included strong safeguards; created a decentralised IT system through which all communication between authorities and service providers can take place in a secure and reliable way, ensuring authentication of all participants; obliged service providers to designate an establishment or appoint a legal representative in the Union; and provided legal certainty for businesses and service providers (European Commission, n.d.3).

Application and admissibility of AI is limitedly covered in these mechanisms. One of the twelve key recommendations of the TRACE Project on electronic evidence is for the EU to 'develop a robust and harmonised legal framework for collection, processing, preserving, production, and admissibility of electronic evidence from both traditional computer systems and emerging technologies such as AI, machine learning, blockchain' (Turksen et al., 2024), internet of things (IoT), virtual reality (VR), and augmented reality (AR). The use of AI in facilitating cross-border exchange of electronic evidence is particularly important.

These instruments are some of the key mechanisms that form the legal backbone of the EU's approach to law enforcement cooperation and information exchange, ensuring that national authorities can share data securely and efficiently; access criminal records and biometric data, coordinate investigations across borders, and respond to terrorism and serious and organised crimes in a harmonised legal framework. Therefore, to counter cross-border crimes and terrorism, the EU has put in place several mechanisms to ensure 'a quicker, safer, and more structured law enforcement cooperation' (European Commission, 2024) across Member States both physically and electronically.

Generally speaking, the EU's instruments for law enforcement cooperation and information support the use of AI (even if implicit), particularly for data analysis,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

predictive policing, and evidence processing, in so far as they comply with the EU AI Act, the General Data Protection Regulation (GDPR) and related protection mechanisms. High-risk AI applications must meet strict obligations. Data protection instruments such as Directive (EU) 2016/680 ensure that AI systems respect privacy of people, thus, balancing security needs with fundamental rights. Ongoing developments on AI and future technologies indicate a dynamic landscape, with a need for continuous monitoring to address implementation challenges and emerging risks.

6.3.1 *General Barriers to Cross-Border Cooperation*

The burgeoning field of AI offers transformative potential for criminal investigations, streamlining processes and enhancing efficiency. However, the increasing transnational nature of crime presents significant cross-border challenges in the deployment and regulation of AI-powered investigative tools.

One primary obstacle is the conflict between data sovereignty laws and the need for seamless data sharing across jurisdictions. AI algorithms, particularly those employing machine learning, rely heavily on vast datasets. The collection, storage, types, and processing of this data are governed by differing national and regional regulations. Sharing data across jurisdictions necessitates navigating complex legal frameworks, raising concerns about compliance, consent, and the potential for misuse. The lack of harmonised legal standards creates fragmentation and hampers the ability of international investigative teams to effectively leverage AI's capabilities.

AI algorithms are trained on data, and biases present in that data can be amplified and perpetuated by the algorithm itself (Barocas and Selbst, 2016). This is particularly problematic in cross-border contexts, where datasets may reflect existing societal biases and/or different methods and standards of data or evidence collection in different jurisdictions. An algorithm trained primarily on data from one country might perform poorly or even exhibit discriminatory outcomes when applied to data from another, raising serious ethical and legal concerns regarding fairness, reliability, and due process. Addressing this necessitates rigorous auditing of algorithms and datasets, coupled with international collaboration to establish common standards for algorithmic fairness, reliability, and transparency.

Different LEAs may utilise diverse AI tools and platforms, leading to interoperability challenges in international investigations. The lack of standardised data formats, communication protocols, and analytical approaches hinders effective data exchange and collaboration. This necessitates the development of common standards and protocols, fostering a more interconnected and efficient global network for AI-assisted policing. International collaboration and the establishment of interoperable systems are paramount for overcoming these barriers.

The use of AI in investigations inevitably involves the processing of sensitive personal data. Ensuring the privacy and security of this data across borders is crucial,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

requiring robust data protection measures and mechanisms for secure data transfer. Concerns surrounding potential surveillance abuses and the risk of data breaches are amplified in cross-border contexts, where oversight and accountability mechanisms may be less robust. International agreements and cooperation are essential for establishing effective safeguards and ensuring responsible data handling practices.

The deployment of AI in LEA investigations raises complex ethical questions regarding accountability and transparency. Determining responsibility when AI-powered tools make errors or contribute to wrongful convictions requires careful consideration of legal frameworks and accountability mechanisms that span national borders. International cooperation is vital in establishing ethical guidelines and ensuring accountability for the actions of AI systems in cross-border investigations.

One other primary obstacle to cross-border law enforcement cooperation is the lack of comprehensive multi-national, bi-national, and national frameworks on information exchange (Birdi et al., 2021) and the absence of a shared Criminal Procedure Code (Basic & Yakhlef, 2022). This lack of legal frameworks for information sharing can lead to information being handled too restrictively or too informally, because of uncertainty among police officers, violate legal procedures and undermine data protection as well as privacy rights of suspects or witnesses (Birdi et al., 2021). Furthermore, different national Criminal Procedure Codes, as well as the distribution of competences (e.g., whether public prosecutors or judges have the authority to determine certain investigative measures) and the fragmentation of LEA compositions (e.g., when different LEAs are assigned to different ministries or different regional authorities) can hinder cooperation (Peters et al., 2016; Salom Lucas & Llambés Sánchez, 2021).

These findings are mirrored in our study in TRACE, where we surveyed LEA and personnel of judicial agencies on the topic of cooperation using an online questionnaire, as well as interviews and focus groups (Kreissl et al., 2023). A detailed description of the methods and data as well as an overview of the sample composition and description, including information on the interview partners referred to in the following paragraphs via the different interview codes are provided in Chapter 4. For example, 62 per cent of the survey respondents considered differences in legal systems to be the main barrier to information exchange (Figure 6.1). Likewise, the interview participants identified differences in national legal systems, especially in criminal law and criminal procedure law, as the most significant barriers to cooperation.

Typically, differences in criminalisation of offences and the different legal requirements for the authorisation of investigative measures (e.g., wiretapping, or comparable surveillance measures) are mentioned as a crucial barrier. For instance, the differences in the regulation of tax offences or money laundering (e.g., different legal provisions and law enforcement practices applied to these types of crimes) hinder joint investigations required in cross-border financial crimes (Turksen et al.,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

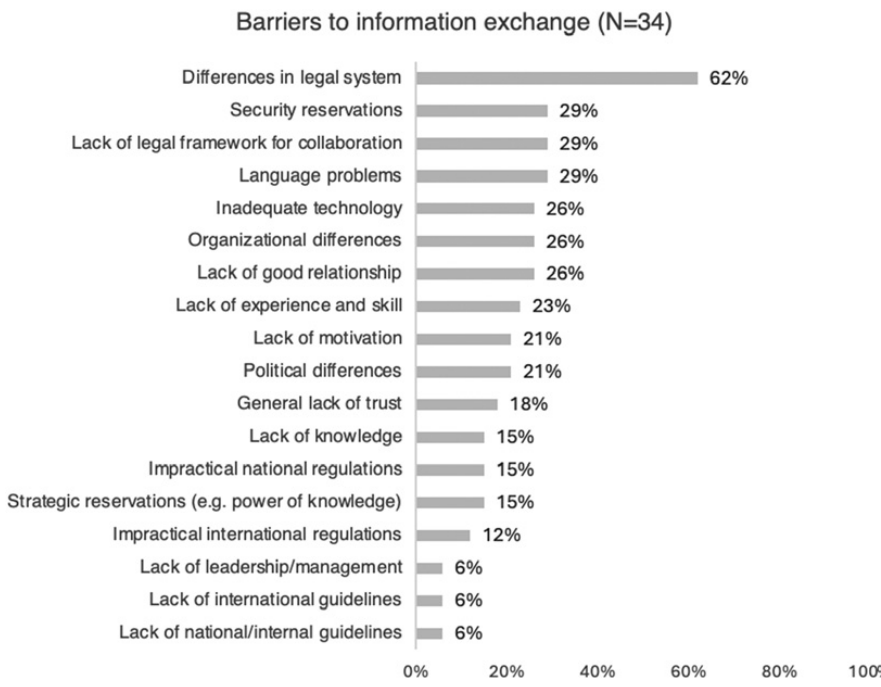

FIGURE 6.1 Perceived barriers for information exchange and cooperation.

2023; Erken & Turksen, 2024). TRACE project research also revealed that the definition and criminalisation of tax offences can vary considerably depending on the member state, or that in some Member States (such as Austria) money laundering is still only punishable in connection with legally regulated predicate offences (Ip2_Po_AT). In practice the mentioned differences in the legal systems can lead to severe imbalances. One of the German police officers (Ip1_PO_DE) described a Joint Investigation Team (JIT) case with Italy where both sides sought intrusive surveillance measures. While common in Italian Mafia investigations, such measures in Germany require strict judicial oversight and approval. Consequently, surveillance requested by German officers was conducted in Italy, providing them with intelligence, but the reverse was not possible, due to the stricter German regulations.

However, not only formal regulations but also the informal policing and prosecution practices can hinder cooperation. Here, national disparities can result in a 'hierarchy of offences' (Ip3_Po_DEI). A law enforcement officer from Estonia (Ip_7_PO_EST) for example explained, that while the seizure of several kilos of marijuana is a rare case in Estonia and thus prompts intensive investigations, in Spain the same quantity is considered minor. Thus, if the Estonian police suspects

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

links to Spain and, therefore, sends a cooperation requests, this may receive little interest from Spanish authorities, as the investigative effort outweighs the potential benefits.

Besides regulatory barriers the most common constraint for cooperation and knowledge exchange is the lack of trust (e.g., Aden 2016; Basic & Yakhlef 2022; Block 2008; Hufnagel & McCartney 2017; Lefebvre 2003; Venema 2020; Yakhlef 2023). In the context of police cooperation, trust is a multi-level construct that not only exist between individual officers, but also at the organisational and state level. Trustworthy relationships have several prerequisites, including good bi-national political relations, a general cultural closeness, good historical relations, and a common language (Venema 2020). This picture is also – at least partially – reflected in our survey data. About one-third of respondents identified language barriers as a challenge to cooperation. For roughly a quarter (26 per cent), the main issue was poor inter-agency relationships. Additionally, around one-fifth cited differing political stances between countries (21 per cent) and a general lack of trust in LEAs from other nations (18 per cent) as significant obstacles (see Figure 6.1).

Further barriers are highlighted in the qualitative interviews, where participants mentioned organisational constraints such as limited resources, the underestimation of information management, or the lack of recognition of international experience. One law enforcement officer from Germany noted that smaller regional police departments struggle with cross-border cooperation due to the high demands on time and workload, personnel, and resources (Ip1_Po_DE). In terms of knowledge management, participants stressed the lack of organisational strategies. Trusted personal contacts, which are key to effective cooperation, are often tied to individual officers. When these officers retire or change roles, their knowledge and networks are frequently lost due to inadequate transfer mechanisms (Ip7_Po_EST). This issue is exacerbated by a prevailing 'silo mentality' where officers limit knowledge-sharing to enhance their own value within the organisation. This silo mentality extends beyond individuals to entire organisations. When and what information is exchanged is thus often determined by different organisational self-interests (e.g., in the case of arrests or the seizure of illegal assets), which can hinder cooperation even between authorities from the same country (Ip2_PO_AT). Another barrier is the lack of intra-organisational recognition of international secondments like Europol postings. In some countries such secondments are still treated as having little organisational value (Ip2_PO_AT) and can lead to a 'career setback' (Ip8_Ep_EU).

Finally, also the attitudes and behaviours of employees have an impact on information exchange and cooperation. As one of the German officers put it, modern criminal policing requires 'globally thinking' (Ip1_Po_DE) officers. Yet, also at the personal level, the most important factor for successful information exchange and effective cooperation remains that officers have trusting international relationships.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

6.3.2 *Facilitators of Cross-Border Cooperation*

In terms of facilitators for effective information sharing, studies highlight the importance of supranational level, multilateral and bilateral agreements (Birdi et al. 2021). Such agreements and strategies should always be developed with the involvement of practitioners since top-down solutions may overlook their needs. Other enablers include the harmonisation of knowledge transfer processes and system among EU Member States (Griffiths et al. 2016). Maybe even more important than having an appropriate legal and policy framework is the need to establish trustworthy cooperation between LEAs. Block describes this trust-based direct contacts between police officers as the backbone of successful operational police cooperation in Europe (Block 2008).

One reason for this is that trust-based personal contacts provide informal connections and communication pathways, which enable a low-threshold flow of information and increases the effectives and speed of exchange even where there are legal, cultural and political obstacles (Machado & Granja 2019). Building trust between officers requires personal contact and exchange via joint investigations or operations, meetings, conferences, or training courses. In contrast, mere formal cooperation is not enough to build trustworthy relationship, as officers have been found to prefer personal information networks over formal channels to share intelligence (Cotter 2017). Moreover, trustworthy relations require shared norms and values (Hufnagel 2017).

In this regard, Basic and Yakhlef (2022) show how the development of shared values involves the formation of a common identity, the perception as an 'in-group' and the establishment of a shared moral order via collaborative work. Therefore, sustainable cooperation in the form of common contact points and joint institutions like Police and Customs Cooperation Centres (PCCCs) or the Liaison Officer system (Block 2010; Mészáros 2016) are paramount, as these provide the setting for regular direct face to face exchange of information (Birdi et al. 2021; Guille 2010).

The importance of trust is also evident from our analysis. In the TRACE survey, as can be seen in Table 6.1, respondents ranked improving good working relationships with other LEAs (38 per cent) as the most important factor for improving information exchange. This is followed by improving the legal framework (33 per cent). Standardisation of technological tools and platforms for information sharing was also endorsed by nearly a third of respondents (29 per cent). When combining agreement ('very true') and agreement ('true'), greater awareness of legal differences is also considered important (67 per cent), in fact, ranking this factor second place. By contrast, improved language skills are considered the least important. The same is true for raising awareness for organisational differences.

The interview and focus group participants offer similar perspectives. Trusting contacts, the harmonisation of legal frameworks and the standardisation of technology for the exchange of information (e.g., in the form of dedicated messenger

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 6.1 *Improvement of cooperation and information exchange*

Ways to improve information exchange (N=42)					
	Very true	True	Not so true	Not true at all	n.a.
Establish good working relations with other LEAs	38%	33%	7%	0%	21%
Improve the existing legal framework governing collaboration between LEAs	33%	33%	0%	7%	26%
Standardise technology systems	29%	29%	14%	5%	24%
Increase awareness of international centres/ organisations	19%	29%	24%	5%	24%
Increase awareness of jurisdictional differences	17%	40%	12%	5%	26%
Increase awareness of organisational differences	9%	31%	26%	5%	29%
Improve language skills	9%	29%	36%	5%	21%

services) are described as a major facilitator for improved cooperation and information exchange. While the first two points require comprehensive political and legal commitment, the bureaucratic and regulatory scope of which can hardly be estimated, strengthening trusting relationships requires comparatively little effort. In this regard, our research suggests three pathways for developing and fostering such relations. First, existing cooperation systems should be strengthened, whether they are designed for long-term and non-case-specific cooperation (e.g., liaison officers) or for case-specific cooperation (in particular JITs).

Second, further training and education programmes, such as those offered by the European Union Agency for Law Enforcement Training (CEPOL), should be further expanded and more closely linked to national police education and training programmes. Third, and connected to this, the EU and its Member States should consider whether, in the future, a dedicated Erasmus-like programme should be developed for the exchange of police officers. This could be an expansion of CEPOL's General Exchange Programme. The centrepiece of such a programme, which initially could be tested in different European border regions, would have to be the integration of seconded officers into (at least parts of) the everyday work of police officers in the host country. This way, both a comprehensive understanding of the work of foreign LEAs and close and lasting personal relationships can be built.

6.4 TECHNOLOGY AS A FACILITATOR AND BARRIER TO CROSS-BORDER COOPERATION

Previous research reports that technology often slows down or hinders cross-border cooperation and information sharing, because systems lack interoperability or due to legal and security restrictions (Birdi et al. 2021; Griffiths et al. 2016; Guille 2010).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Other practical issues are the insufficient technical proficiency of police staff (Griffiths et al. 2016) or the lack of trust in the security of digital information networks (Cotter 2017). Yet, modern policing is hardy imaginable without the use of technology. Thus, the role of (AI-supported) technology for cross-border police cooperation proves to be ambivalent. Although in our study interviewees and the focus group participants in general acknowledged the benefits of modern and AI-supported technologies, they tended to do so at an abstract level and with some reservations.

On the one hand, there are well established European LEA information exchange systems such as the SIENA, the Schengen Information System II (SIS II) or the Europol Information System (EIS) which participants highly valued. All these systems were described having a high degree of usefulness and were seen as an important part of the wider EU LEA information network. What these platforms have in common, however, is that they are not intended to support concrete, case-related, and structured cooperation between specific LEAs. In this regard, as the results of the online survey and the interviews show, there is a lack of appropriate technology. As presented in Figure 6.1, 26 per cent of survey participants believe that inadequate technology is a barrier to cooperation, and as shown in Table 6.1, 58 per cent think that one way to improve cooperation is to standardise technological system.

A major problem however is that different countries use different technological equipment, and this applies to both hardware and software (Guille 2010). While this problem already existed a decade ago, it is now exacerbated by the rapidly growing technology market, coupled with the different national security regulations. Such differences are already often present within a country, and in some countries, such as Germany, differences in technological equipment even exist between the various regional police forces (Ip1_Po_DE, Ip3_Po_DE). Yet, the situation is certainly most problematic in cross-border circumstances. At the same time, in some areas, such as simple communication services, interviewees reported the lack of secure applications LEA officers could use in cross-border cooperation to communicate sensitive information securely. Participants pointed out that they themselves already have made use of the products of private telecommunications providers, some of which are based outside the EU, in the course of sharing information or to organise operational meetings.

Finally, participants described the practical limits of technologically supported investigative cross-border work, using the example of automatically generated translation (natural language processing and translation). Such systems would, in practice, be confronted with the problem of identifying cultural codes. According to several participants, it is therefore not enough to simply have an AI-supported natural language processing system, but what is needed is an interpreter who is familiar with the specific cultural and linguistic codes, intonations, dialects, and so on. In the best-case scenario, the interpreter has many years of experience in working with the police and similar institutions, is familiar with the dialects and local customs of the suspects, and so on.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

6.5 CONCLUSION

The use of AI in cross-border investigations of financial crimes such as money laundering and financing of terrorism characterises a transformative frontier in pursuing crime and justice. As financial crime becomes increasingly sophisticated and transnational, AI technologies do present unique capabilities to LEAs to identify, analyse, track, and prosecute offenders. Chapter 6 has critically analysed the evolving nature of financial crime in a complex cross-border environment of the EU, providing a nuanced perspective on the significant role AI plays in improving cross-border investigations.

AI tools, such as machine learning algorithms and advanced data analytics, have revolutionised how financial crimes are detected and investigated. AI has enabled LEAs to unpack complex financial transactions, predict illicit activities, analyse, and visualise vast datasets for patterns that show existence of financial crime. Using real-world cases backed by TRACE research, we have demonstrated how AI equips LEAs with necessary tools to navigate the complex dynamics of financial crime in ways that secure more efficient and effective investigative processes.

The deployment of AI in cross-border investigations, however, has several challenges – some of which we have highlighted in this chapter. For instance, data sovereignty laws, which vary across the EU, foster fragmentation and undermine seamless sharing of data between LEAs. Further, LEAs from different jurisdictions face interoperability issues drawn from the diverse AI tools and platforms they use. It is, therefore, necessary to develop common standards and protocols to facilitate interoperability between different LEAs. Data protection issues also arise in cross-border investigations. As it is crucial for LEAs to ensure the privacy and security of sensitive personal data across the EU, robust data protection measures and mechanisms for secure data transfer are needed – a challenge, which can frustrate or slow down investigation of financial crimes. Additionally, biases in datasets can be amplified by AI algorithms, which raise ethical and legal concerns in relation to fairness and due process.

This chapter demonstrates that it is crucial to ensure effective cross-border cooperation and information exchange for countering cross-border financial crimes. In this regard, it is necessary to sustain trust-based relationships between LEAs, which are facilitated by personal contact and exchange through joint investigations, meetings, conferences, and training courses. Cross-border cooperation is further enhanced by multilateral, bilateral, and supranational agreements, as well as harmonisation of knowledge transfer processes, and standardised technological tools. The TRACE project has provided useful insights into the barriers and facilitators of cross-border cooperation, providing practical recommendations for improving cross-border collaboration and sharing of information.

The chapter provides a guide for professionals and researchers that seek a nuanced understanding of the synergy between AI and cross-border investigations. The

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

germane challenges, solutions, and opportunities we have provided in the use of AI for cross-border investigations do contribute to EU's efforts towards the development of more effective strategies and tools for countering financial crime. Continued enhancement of elements such as trust-based collaboration, ethical considerations, innovation, and technological capability building, public private partnerships, increased investment in AI for law enforcement, and interoperability are key to harnessing the full potential of AI in combating cross-border financial crime. Future developments are likely to focus on strengthening digital capabilities, improving information sharing, streamlining investigative procedures, addressing the evolving nature of crime, and further reinforcing the legal framework for EU police cooperation, while continually addressing the crucial balance between security needs and the fundamental rights of individuals.

REFERENCES

Aden H. (2016) The role of trust in the exchange of police information in the European multilevel system, in Delpeuch T. and Ross J. (eds.), *Comparing the Democratic Governance of Police Intelligence*. Cheltenham: Edward Elgar Publishing, pp. 322–344.

Barocas S. and Selbst A. D. (2016) Big data's disparate impact. *California Law Review*, 104, pp. 671–732. Available at: https://ssrn.com/abstract=2477899 (Accessed 26 May 2025).

Basic G. and Yakhlef S. (2022) Anomie and collaboration in intelligence and operational police and border guard work in the Baltic Sea area: In-group mentality and construction of the other. *Policing and Society*, 32(9), pp. 1103–1123.

Birdi K., Griffiths K., Turgoose C. and Vonaş G. (2021) Factors influencing cross-border knowledge sharing by police organisations: An integration of ten European case studies. *Police Practice and Research*, 22(1), pp. 3–22.

Block L. (2008) Combating organized crime in Europe: Practicalities of police cooperation. *Policing*, 2(1), pp. 74–81.

Block L. (2010) Bilateral police liaison officers: Practices and European policy. *Journal of Contemporary European Research*, 6(2), pp. 194–210.

Burton J., Janjeva A., Moseley S. and Alice (2025) *AI and Serious Online Crime*. CETaS Research Reports, March. Available at: https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime (Accessed 26 May 2025).

Carlisle D. (2023) *The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond*. Chichester: Wiley.

Charter of Fundamental Rights of the European Union (2000/C 364/01).

Cotter R. S. (2017) Police intelligence: Connecting-the-dots in a network society. *Policing and Society*, 27(2), pp. 173–187.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Treaty) OJ L 210, 6.8. 2008, pp. 1–11.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') OJ L 283, 31.10.2017, pp. 1–71.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA OJ L 88, 31 3.2017, pp. 6–21.

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA PE/64/2019/REV/1 OJ L 186, 11 7..2019, pp. 122–137.

Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA PE/70/2022/REV/2 OJ L 134, 22 5.2023, pp. 1–24.

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings PE/3/2023/REV/1 OJ L 191, 28 7.2023, pp. 181–190.

Erken E. and Turksen U. (2024) *Anti-Money Laundering and the Law: Comparative Approaches to Countering Predicate Crimes*. London: Routledge.

European Commission (n.d.1) Information exchange. Available at: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/information-exchange_en (Accessed 26 May 2025).

European Commission (n.d.2) European Criminal Records Information System (ECRIS). Available at: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en (Accessed 26 May 2025).

European Commission (n.d.3) E-evidence – cross-border access to electronic evidence. Available at: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (Accessed 26 May 2025).

European Commission (2024) Law enforcement cooperation. Available at: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation_en (Accessed 26 May 2025).

European Union (n.d.) Stepping up cross-border cooperation – the Prüm decision. EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:jl0005 (Accessed 26 May 2025).

Europol (2025) *European Union Serious and Organised Crime Threat Assessment: The Changing DNA of Serious and Organised Crime*. Luxembourg: Publications Office of the European Union.

Europol (2024) *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*. Europol Innovation Lab. Available at: www.europol.europa.eu/publication-events/main-reports/ai-and-policing (Accessed 26 May 2025).

Europol (2020) *Malicious Uses and Abuses of Artificial Intelligence*. European Cybercrime Centre (EC3). Available at: www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf (Accessed 26 May 2025).

FBI (2024) Criminal Use of Generative Artificial Intelligence to Facilitate Financial Fraud, *Public Service Announcement*, Alert Number: I-120324-PSA, 3 December.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Federal Department of Foreign Affairs (FDFA) (2025) *Police Cooperation (Prüm Decisions)*. Available at: www.europa.eda.admin.ch/en/police-cooperation-prum-decisions (Accessed 26 May 2025).

Griffiths K., Birdi K., Andrei D. and Mouhanna C. (2016) Knowledge sharing practices and issues in policing contexts: A systematic review of the literature. *European Journal of Policing Studies*, 3(3), pp. 267–291.

Guille L. (2010) Policing in Europe: An ethnographic approach to understanding the nature of the cooperation and the gap between policy and practice. *Journal of Contemporary European Research*, 6(2), pp. 257–272.

Hufnagel S. (2017) Regulation of cross-border law enforcement: 'Locks' and 'dams' to regional and international flows of policing. *Global Crime*, 18(3), pp. 218–236.

Hufnagel S. and McCartney C. (eds.) (2017) *Trust in International Police and Justice Cooperation*. Oxford: Hart Publishing.

King T. C., Aggarwal N., Taddeo M. and Floridi L. (2019) Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 25, pp. 1–29.

Lefebvre S. (2003) The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and Counterintelligence*, 16(4), pp. 527–542.

Liu Y., Tian M. and Shao Y. (2022) *Cybercrimes and Financial Crimes in the Global Era*. Singapore: Springer. Available at: https://link.springer.com/book/10.1007/978-981-19-3189-5 (Accessed 26 May 2025).

Machado H. and Granja R. (2019) Police epistemic culture and boundary work with judicial authorities and forensic scientists: The case of transnational DNA data exchange in the EU. *New Genetics and Society*, 38(3), pp. 289–307.

Mészáros E. L. (2016) The evaluation of police cooperation between Hungary and Romania in the fight against cross-border financial criminal activities. *Eurolimes*, 21, pp. 143–156.

Nerantzi E. and Sartor G. (2024) Hard AI crime: The deterrence turn. *Oxford Journal of Legal Studies*, 44(3), pp. 673–698.

Peters M., Vanderhallen M. and Nelen H. (2016) Cross-border criminal investigation in the Meuse-Rhine Euroregion: International policing and the theory of (inter-)organisational conflict. *European Journal on Criminal Policy and Research*, 22, pp. 41–60.

Rebovich D. J., Kim J. and Layne M. (2021) The changing face of financial crime: New technologies, new offenders, new victims, and new strategies for prevention and control. *Victims & Offenders*, 16(5), pp. 617–636.

Regulation (EU) 2023/1543 of the European Parliament and of the Council 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings PE/4/2023/REV/1 OJ L 191, 28 7.2023, pp. 118–180.

Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 (Prüm II Regulation) PE/75/2023/REV/1 OJ L 2024/982, 5.4.2024.

Salom Lucas A. and Llambés Sánchez M. I. (2021) Mutual legal assistance on criminal matters: When theory meets practice – a real story. *ERA Forum*, 22(2), pp. 337–349.

Sheptycki J. W. E. (2007) Transnational crime and transnational policing. *Sociology Compass*, 1, pp. 485–498.

TRACE (n.d.) *Developing AI solutions to disrupt illicit money flows*. Available at: https://trace-illicit-money-flows.eu/ (Accessed 26 May 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Turksen U. et al. (2023) *Tax Crimes and Enforcement in the European Union: Solutions for Law, Policy and Practice*. Oxford: Oxford University Press.
Turksen U. et al. (2024) D7.6: Recommendations for streamlining evidence collection procedures for transborder crimes (No 101022004 – TRACE, 2024).
Venema A. E. (2020) The sum of all friends: Improving cross-border intelligence sharing in Europe – the case of the Benelux. *The International Journal of Intelligence, Security, and Public Affairs*, 22(1), pp. 5–19.
Yakhlef S. (2023) Humour, trust, and tacit knowledge of police and border officers in international police collaboration. *Journal of Policing, Intelligence and Counter Terrorism*, 18(2), pp. 174–188.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

7

Dual Use of Emerging Technologies and Decentralised Financial Assets

Bogdan Adamyk and Vladlena Benson

7.1 INTRODUCTION

The financial landscape is being transformed as emerging digital technologies increasingly integrate with decentralised financial assets. Technologies such as blockchain, artificial intelligence (AI), and the Internet of Things (IoT) are being incorporated to form new financial products and services that operate without traditional intermediaries (Divyashree and Mishra, 2025). This convergence promises substantial benefits: for example, blockchain provides a tamper-resistant ledger that enables peer-to-peer transactions and self-executing agreements (smart contracts) with transparency and security (Kmet, 2018). In financial contexts, AI largely means machine learning algorithms and data-driven models that perform tasks such as prediction, classification, optimisation, and anomaly detection (Pillai, 2023). AI algorithms can automate complex decision-making in lending, trading, and fraud detection, far beyond human speeds (Clarke, 2023).

The IoT refers to the network of physical objects equipped with sensors, software, and connectivity, enabling them to collect and exchange data (Laghari et al., 2021). Simple environmental sensors comprise one end of the IoT device range, while smartphones, smart appliances, vehicles, and industrial machines form the other end. IoT devices can transfer real-time data into blockchain networks (via oracles), letting smart contracts respond to real-world events – for instance, changing insurance payouts based on sensor data or triggering supply chain payments when goods are delivered (Ashfaq, 2022). Together, these innovations start a new era of financial inclusion, efficiency, and automation in financial services.

At the same time, these technologies provide dual functionality, which allows legitimate uses to co-exist with illegal and unethical activities. Money laundering, fraud, and criminal activities can occur on decentralised and anonymous platforms because these systems hide transaction data from regulatory oversight (Benson, Turksen and Adamyk, 2023). AI tools that enhance services present a risk for malicious activities since they can be used to manipulate markets while automating cyber-attacks (Sumner, 2025). The vulnerability of IoT devices enables attackers to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

inject adversarial data into smart contracts or reveal important financial data to unauthorised parties. Thus, the features that make emerging tech attractive for finance (speed, pseudonymity, automation) can become a 'digital cloak' for illegal activity if proper safeguards are not in place (George, 2024). Financial industry professionals and government regulators currently face the dual challenge of harnessing blockchain-based finance, AI, and IoT while mitigating the risks of misuse and maintaining stability and trust in financial markets.

The European Union's regulatory move demonstrates this balancing act. Recently, the EU established a comprehensive framework, the Markets in Crypto-assets Regulation 2023 (MiCA), to oversee digital asset markets and the Artificial Intelligence Act 2024 to set rules for AI systems, alongside a new Anti-Money Laundering Authority (AMLA) to manage illicit financial risks. These initiatives aim to advance innovation in areas such as decentralised finance (DeFi) and AI, as well as address security, consumer protection, and financial crime concerns. Against this backdrop, this chapter provides a structured analysis of the dual-use phenomenon in emerging financial technologies.

Section 7.2 outlines a conceptual framework for understanding dual-use technologies in the financial domain. Section 7.3 explains the technological underpinnings of blockchain, DeFi, AI, and IoT. The benign applications and benefits of this integration are highlighted in Section 7.4, followed by the adversarial risks and malicious uses in Section 7.5. Section 7.6 discusses ethical considerations and evolving regulatory measures. Section 7.7 explores the state-of-the-art developments and initiatives at the time of writing. Finally, Section 7.8 presents a future outlook and concludes with strategies to handle the dynamic complexities of this ecosystem.

7.2 CONCEPTUAL FRAMEWORK FOR DUAL-USE TECHNOLOGIES IN FINANCE

The term *dual-use technology* describes innovations that can serve both beneficial needs and destructive objectives. Financial dual use describes how modern innovative tools benefit legitimate economic actors and simultaneously provide opportunities for criminals and bad actors (David, 2023). The dual-use concept can be observed through the convergence between DeFi, AI, and IoT technologies. Advanced technologies serve as dual-purpose tools that enable financial democratisation and improved efficiency, yet they also enable control of subversion and illegal operations. A structured approach must be established to handle the dual nature of these systems.

At its core, DeFi is a system that recreates traditional financial instruments – lending, trading, payments, insurance – on distributed blockchain platforms, reducing dependence on central intermediaries (Adamyk et al., 2025). By design, DeFi protocols such as decentralised exchanges or lending platforms let peer-to-peer transactions be governed by code (smart contracts) rather than by banks or brokers.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

The absence of intermediaries and openness of DeFi are profoundly positive innovations: they can lower costs and barriers to access and foster the transparency of transactions (Vasishta et al., 2025). For example, users can interact with DeFi platforms through the internet to loan money or withdraw funds without needing bank authorisation. Nevertheless, the same features which enable open access and eliminate financial intermediaries also create possible misuse opportunities. Users can execute large sums of money transfers via unidentified wallet addresses while concealing their payment sources, hindering anti-money laundering (AML) enforcement efforts (Kmieliauskas, 2025). The conceptual framework of dual use needs to address how user empowerment from direct access coexists with removing traditional risk management processes.

The dual-use problem is exacerbated by AI and IoT technologies. In finance, AI incorporates machine learning models, algorithms and autonomous agents that can analyse data or make decisions (Lakhchini, Wahabi and Kabbouri, 2022). These range from credit scoring systems to high-frequency trading algorithms (Turksen, Benson and Adamyk, 2024). Integrated with DeFi, AI can automate complex financial strategies or detect transaction anomalies. Adversaries can repurpose the same AI tools that help banks detect fraud to evade detection, generate synthetic identities, or identify exploitable market patterns (Sumner, 2025). Likewise, the IoT – networks of sensors and smart devices generating real-time data – can feed invaluable information into DeFi systems (for example, an IoT sensor measuring crop growth might trigger an automatic crop insurance payout) (Ahamad et al., 2022). However, those IoT devices, if subverted, can become entry points for cyber-attacks or sources of compromised data input, undermining integrity of financial contracts (Gummadi, 2023). The IoT ecosystem often lacks effective security and is notorious for vulnerabilities such as weak authentication and unencrypted data streams. The attack capabilities of criminals increase substantially when IoT devices become integrated with financial transactions within a dual-use framework (Vaseashta, 2025).

The dual-use issue becomes easier to understand by examining a spectrum of use cases from purely beneficial to completely malicious rather than two opposing categories. Most new technological applications exist in a 'grey area' between clear beneficial and harmful uses. For instance, an algorithmic stablecoin might promote financial inclusion in emerging markets, yet it could also facilitate capital movement or collapse and harm users if poorly designed (Clements, 2021). Trading bots could bring trading liquidity, but unscrupulous AI algorithms can drive bots to perform market manipulation. The proposed framework needs to combine the functions of different stakeholders: developers (who create protocols and AI models); users (who may be legitimate or criminal); and law enforcement or regulatory agencies (who need oversight capabilities). Each stakeholder has a different incentive – innovators often prioritise openness and functionality, whereas regulators emphasise controls and safeguards. Governance mechanisms become vital in aligning these perspectives. For decentralised projects, governance may be algorithmic or

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

community-driven (via token voting), raising questions about accountability for dual-use outcomes.

The timeline between technological adoption and implementation of regulatory measures is commonly known as the Collingridge dilemma because it becomes challenging to predict and control societal impacts during early development stages, yet the technology becomes highly entrenched when unfavourable consequences appear (Tigard, 2022). The same pattern exists in present-day DeFi and AI systems. They have swiftly overtaken traditional legal frameworks, creating a lag in regulatory response. Therefore, new regulatory framework must incorporate adaptive regulation and ethical design principles. For example, AI developers are encouraged to implement fairness and transparency measures to prevent biased or inscrutable models from causing harm. In the blockchain context, there are proposals for self-regulation through code – for example, smart contracts that enforce compliance (such as only allowing transactions if specific criteria are met or embedding identity verification credentials such as soulbound tokens (Adams, 2024) to user wallets). While such measures are still emerging, they represent efforts to resolve dual use by technical means.

In summary, the conceptual dual-use model in modern financial technologies depends on recognising how blockchain, AI, and IoT components function as both constructive elements and security threats. The framework demands analysis from three distinct viewpoints: technological aspects regarding system operations, legal/regulatory elements describing applicable rules, and ethical considerations of societal values.

7.3 TECHNOLOGICAL UNDERPINNINGS: BLOCKCHAIN, DEFI, AI, AND IOT

A sound understanding of the technologies is essential before exploring their dual uses. Blockchain is the foundational technology underpinning DeFi. The blockchain operates as a distributed ledger system while multiple computers (nodes) validate and record transactions through encrypted blockchains (Adamyk et al., 2025). Bitcoin is the most well-known application of blockchain technology, introducing digital money through a decentralised system, while blockchain itself now underpins a wide range of platforms beyond cryptocurrencies. Smart contracts added onto Ethereum blockchain enable self-executing code to run on blockchain networks, which enforces agreements through automated processes such as payments after goods delivery. The key properties of blockchain networks include decentralisation, immutability, and transparency (Ali, Norman and Azzuhri, 2023).

Decentralisation refers to the distribution of ledger maintenance across a network of independent nodes rather than a single trusted authority; this architecture mitigates single-point-of-failure risks and reduces the potential for unilateral control or censorship (Papadopoulos, Pitropakis and Buchanan, 2022). Immutability denotes the cryptographically enforced impossibility of altering validated records without

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

network consensus, thereby providing a tamper-evident audit trail that underpins data integrity and legal verifiability (Vaigandla et al., 2023). Transparency arises from the public accessibility of ledger entries and validation rules, enabling any participant to verify past transactions and system behaviour, which in turn fosters accountability and trust among otherwise unconnected stakeholders (Sedlmeir et al., 2022).

Blockchain network operates without a single controlling authority because records become nearly impossible to modify after entry, and all transactions remain visible to participants through pseudonymous addresses. Blockchain technology provides ideal features that enable financial services to build their infrastructure. Traditional finance (TradFi) relies on central authorities (banks, clearing houses) to maintain ledgers and enforce contracts. By contrast, a blockchain-based system allows direct peer-to-peer value transfer and confirmable execution of logic without needing to trust a middleman. For instance, in a DeFi lending protocol, borrowers and lenders are matched through code, collateral is held in escrow by a smart contract, and interest rates adjust algorithmically based on supply-demand – all recorded on a public ledger (Harvey and Rabetti, 2024).

DeFi refers to the ecosystem of financial applications built on blockchain networks that operate in a decentralised manner. Key components of DeFi include:

- *Cryptocurrencies and tokens*: The blockchain network operates through digital value transfer tokens and smart contract fuelling assets such as Ether for Ethereum transaction fee payment. Many DeFi platforms issue their own governance tokens, which confer voting rights to holders for protocol changes.
- *Decentralised Exchanges (DEXs)*: Platforms such as Uniswap or SushiSwap that allow users to trade tokens directly from their wallets using liquidity pools and automated market-making algorithms rather than through a central exchange.
- *Lending and Borrowing platforms*: Platforms such as Aave and Compound enable users to earn interest through asset deposits, while others can borrow money by providing collateral under smart contract automation. Through programming code these platforms maintain real-time control over collateral ratios together with interest rates.
- *Stablecoins*: Stablecoins act as cryptocurrencies that maintain their value by linking to stable assets (primarily USD) thus providing the stability required for DeFi applications. Stablecoins exist mainly in two distinct types: asset-backed through reserve holdings and algorithmic foundations.
- *Payment networks and remittances*: Blockchain is used to send payments globally at a low cost and remove intermediaries such as correspondent banks.
- *Derivatives and asset management*: The decentralised environment enables users to generate derivative instruments and asset management tools, including synthetic assets that track real-world commodities and yield aggregation services (Adamyk et al., 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

The combination of these features creates a parallel financial system operating continuously worldwide through computer code. DeFi platforms experienced substantial growth in early 2025 as tens of billions of dollars were locked into DeFi contracts worldwide (Kranjec, 2025). This growth shows the importance of understanding both the innovation and the vulnerabilities inherent in this new financial and technological architecture.

In traditional finance, AI is used for credit scoring, algorithmic trading strategies, fraud monitoring, customer service chatbots, and portfolio management, among other applications.

AI thrives on data, and the financial sector offers plenty of it – transaction histories, market data, customer profiles, and so on (Chang and Benson, 2023). Blockchain-based finance provides beneficial public access to structured transaction records that AI analysis can effectively use as valuable resources. Moreover, the deterministic nature of smart contracts means AI can constantly trigger financial actions by invoking those contracts as needed. The intersection of AI and DeFi thus creates autonomous financial agents and data-driven decision-making in a decentralised environment (Sumner, 2025). An example is the use of AI for real-time fraud analytics on a DeFi platform: the AI system could constantly monitor blockchain transactions and flag suspicious patterns (e.g., rapid large transfers between mixers and exchanges) for immediate intervention (Clarke, 2023). Another example is AI-driven lending: a DeFi lending pool might use an AI model to dynamically adjust collateral requirements or interest rates based on a borrower's behavioural pattern and risk profile, computed from on-chain data and external credit data.

The connection between physical assets and digital ledgers in DeFi and blockchain operations relies on IoT as an interface between these domains. IoT sensors generate reliable data for blockchain smart contracts by using Oracle services, which serve as a data connection between external information and the blockchain (Al Sadawi, Hassan and Ndiaye, 2022). Supply chain finance is an example: IoT trackers on shipping containers can log a shipment's location and condition (temperature, shock, etc.) to a blockchain. The source data feeds into supply chain financing contracts, enabling instant transactions to suppliers once their products reach their destination without damage (Kmet, 2018). The blockchain supply chain platforms Maersk's TradeLens and IBM were among numerous projects that demonstrated how IoT data updates blockchain ledgers while performing automatic trade operations.

When uniting IoT with blockchain, the main technological challenge lies in ensuring data integrity – confirmation that device-generated data remains accurate and without manipulation. Two methods for resolving this issue consist of trusted sensors with cryptographic hardware that authenticate their readings and consensus algorithms which verify multiple source data. The security of IoT remains a recognised vulnerability because resource-limited devices are unable to run complex encryption; they may be left with default passwords or outdated firmware

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

that serve as easy entry points for cyber attackers (Kornaros, 2022). When such devices are connected to financial smart contracts, a compromised device could lead to false triggers – for example, a hacker simulating a sensor reading to illicitly trigger an insurance payout. Thus, for any significant implementation of IoT within DeFi networks, strong security measures for IoT devices and reliable Oracle systems must be the foundational elements.

Therefore, in terms of the way these technologies complement each other, blockchain offers a decentralised, immutable ledger and transaction logic; DeFi establishes the financial functions and instruments built on that ledger; AI contributes intelligence and automation in decision-making; and IoT brings external, real-world data and connectivity. Each technology on its own is powerful, but their combination is what enables truly innovative fintech applications.

7.4 BENEFITS OF INTEGRATING EMERGING TECHNOLOGIES IN DEFI

The fusion of blockchain, AI, and IoT with DeFi brings many potential benefits that could noticeably improve financial services and economic systems. These benefits span operational efficiencies, enhanced security and trust, new financial inclusivity, and innovative products.

Greater Efficiency and Automation: The most urgent advantage that emerges from this technology is the elimination of time-consuming manual procedures. By leveraging automation through smart contracts and AI, financial transactions that once took days or weeks and involved layers of intermediaries can be executed in seconds. For example, traditional trade finance requires documents to be verified by banks alongside customs and insurers, which results in both slow operations and high costs. Multiple verification steps in a blockchain-IoT system use automation to verify delivery through sensors and cheque conditions with smart contracts followed by immediate settlement of payments. The optimised process reduces management expenses and decreases the chances of manual errors. The digital world enables the redesign of standard back-office functions such as reconciliations, settlements, and compliance cheques (Kmet, 2018).

AI algorithms perform automatic real-time account matching and detect errors that legacy systems manage through monthly audits. AI monitoring of straight-through processing enabled by blockchain leads to transaction self-execution, which allows financial processes to execute with minimal human interaction, such as loan approvals, claim payouts, and cross-border payments. Such cost optimisation enables financial services to maintain continuous operations while expanding without needing proportional increases in staff numbers.

Improved Transparency and Trustworthiness: Blockchain-based finance delivers an important feature of increased transparency in financial systems. Any stakeholder can verify blockchain transactions because they are stored in a chronological and immutable manner on public blockchains. Financial transparency created by

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

blockchain technology helps decrease both fraud and financial corruption. The blockchain receives IoT device data, such as machine usage records under leasing conditions, generating a unified, trustworthy database that both parties can rely upon. The analysis of transparent data repositories performed through AI systems enables fast irregularity detection. An AI system tracking DeFi platform activity instantly detects unusual transaction activities and suspicious addresses because it has complete visibility into the ledger database (Kute et al., 2021).

Traditionally, banks find fraud after the fact or require lengthy investigations into separate records. Openness in financial operations establishes stronger consumer trust since users can validate the paths their funds take and their contractual terms. Traditional finance derivative contracts remain difficult for ordinary people to understand, yet DeFi smart contracts provide public access to their open-source code base, which allows users to view their rules even if they must understand expert-level technicalities. The integration of AI can further explain some of these processes to users – for instance, AI chatbots can interpret and present the terms of a smart contract in plain language, improving user comprehension and empowerment (Rane, Choudhary and Rane, 2024).

Financial Inclusion and Accessibility: The emerging DeFi ecosystem offers access to financial services through two key features – direct service provision without intermediaries and using technology to assess risk in novel ways. Billions worldwide do not have banking services because they lack credit history and geographic limitations. Users need only an internet connection combined with a digital wallet instead of traditional bank accounts to use DeFi platforms, which decreases entry requirements. The inclusion process receives AI enhancements through alternative data assessment, which supports creditworthiness evaluation and product customisation. A decentralised platform grants loans to users who lack traditional credit records when AI algorithms detect stable wallet fund flows and timely micro-loan repayments in their blockchain transactions.

Traditional credit scoring processes overlook many people, but this approach allows them to obtain credit. Through IoT technology, farmers from lower-income groups gain access to micro-insurance services that automatically pay out smart contracts activated through sensor data collection without dealing with traditional insurance red tape. Automation-based cost efficiencies enable profitable small-scale operations to provide services, thus making micro-transactions possible even when expenses are minimal. The combination of blockchain technology and smart contracts enables financial services that banks have struggled to support economically in the past. Through technological unification, people gain 'smart finance for everyone', which provides them with easy-to-use mobile features and AI-powered interfaces to manage savings, borrowing, and investments.

Enhanced Security: While security is a double-edged problem, there are ways in which integrated tech can increase security. Blockchains, by design, provide effective protection against data tampering – once the network confirms a transaction, it

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

cannot be retroactively altered or forged. Such security measures minimise the occurrence of double-spending attacks and protect ledgers from single-point failures (because they lack central databases that could be hacked). IoT and AI can augment security by providing continuous monitoring and immediate incident response. For example, AI-based anomaly detection can identify a cyber-intrusion or suspicious trading activity on a DeFi exchange the moment it happens (Mazhar et al., 2023).

Contrast this with a typical bank, where a breach might go unnoticed for days or fraudulent transactions only flagged after clearing. Additionally, emerging techniques such as AI-driven identity verification can strengthen user authentication. Biometric data from IoT devices (such as a phone's fingerprint reader or face recognition) combined with AI analysis can securely authenticate users in a decentralised system without relying on passwords (often weak links). There are also projects where AI assists in smart contract verification, scanning contract code for vulnerabilities or compliance with regulatory requirements before deployment – essentially an automated audit. Widespread implementation of this security measure would stop numerous potential attacks while creating basic protection for DeFi protocols.

New Financial Products and Innovation: The combination of these technology elements resulted in brand-new creative outputs that were beyond human reach. For instance, dynamic insurance is an innovation wherein insurance coverage and premiums can adjust in real time based on IoT data and AI risk assessments. Insurance premium calculation in a smart contract policy depends on mileage usage, while the rate adjustment depends on monitored driving safety through telematic devices installed in the car. Real-time driving safety would decrease rates, while reckless acceleration would increase them through smart contracts and AI automation instead of traditional premium readjustments. Such insurance design establishes both fairness and individualised policies between customers. This creates a more equitable and personalised insurance model.

Similarly, in investment management, there is the rise of robo-advisers, which, when connected to DeFi, can not only advise but directly execute portfolio changes through smart contracts, offering retail investors sophisticated strategies such as automated rebalancing and yield farming that previously required expensive active management. The tokenisation of assets is another product innovation: real-world assets (RWA) such as real estate, commodities, or even art can be tokenised on blockchain and managed or traded by AI algorithms (Gottschalk, 2023). This could unlock liquidity in traditionally illiquid assets, allowing someone to buy a tiny fraction of a rental property as easily as buying a stock, with AI platforms managing the asset's income distribution and maintenance via IoT monitors. Indeed, forecasts suggest RWA tokenisation in DeFi has the potential to grow exponentially, potentially bringing trillions in value on-chain over the next decade as legal frameworks catch up (Dioquino, 2025). The process enables more people to access investment opportunities through decentralised markets that might operate more efficiently.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Compliance and Regtech Solutions: Integrating AI and blockchain can also foster regulatory compliance and anti-fraud efforts (the 'good side' of dual use). AI-driven analytics on transparent blockchain data can let regulators or financial institutions to monitor compliance with AML/CFT (anti-money laundering and counter-terrorist financing) rules in near real-time. Suspicious transaction reports that used to be filed after delays could become immediate algorithmic alerts. Cryptographic identity solutions on blockchain might modernise know-your-customer (KYC) processes – for instance, a user could have a verifiable digital identity token that AI systems accept across platforms, reducing duplication of checks. Some DeFi projects are exploring on-chain KYC attestations so that participants retain privacy but can prove to decentralised applications that they are not sanctioned or of a specific jurisdiction (Malhotra, Saini and Singh, 2022).

AI can verify documents and perform background checks faster and more precisely than humans in many cases, and doing this, in combination with decentralised identity on the blockchain, offers a path to embedded compliance by design. Theoretically, this could lessen the tension between DeFi and regulators by making decentralised platforms at least as capable of enforcing financial regulations as centralised ones, although through code and AI rather than human compliance departments. While these solutions are nascent, they highlight a benefit often overlooked: emerging tech can strengthen the financial system's integrity when applied constructively (Chainalysis, 2020).

Integrating blockchain, AI, and IoT in finance can lead to faster, cheaper, more inclusive, and perhaps more transparent financial services. It aligns well with the goals of increasing efficiency and access in the EU's Digital Finance Strategy, which seeks to adapt regulatory frameworks to digital innovation and promote data-driven finance (Berger, 2021). The benefits, however, do not come without trade-offs. As the next section will discuss, the very features that produce these advantages – openness, automation, immutability – also create new vectors for risk and exploit (Khan et al., 2024). The dual-use dilemma thus becomes apparent: how to harness these benefits while controlling the corresponding risks.

7.5 DUAL-USE RISKS: ILLICIT EXPLOITATION OF DEFI AND EMERGING TECH

Conducting financial operations through innovative technologies creates serious problems with their improper use. Malicious actors can repurpose the same innovations that streamline and democratise finance to bypass controls, perpetrate crime, or destabilise markets. This section outlines the significant dual-use risks, focusing on how blockchain/DeFi, AI, and IoT can be exploited in illicit or harmful ways.

Financial Crime and Money Laundering via DeFi: The decentralised finance platforms often miss out on performing customer identification and transaction monitoring measures that traditional financial institutions use. The combination

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

of user anonymity and missing intermediaries provides ideal conditions for money launderers and terrorists to carry out their illegal activities, including fraud and sanctions avoidance. Europol has warned that cryptocurrencies, DeFi platforms and AI-driven automation 'facilitate greater anonymity' for criminals seeking to obscure illicit transactions (Kmieliauskas, 2025). The real-world use of DeFi allows criminals to execute different types of abuse. One common tactic is using 'chain-hopping' and mixers: criminals move illicit funds through multiple cryptocurrencies and DeFi protocols, swapping from Bitcoin to Ether to privacy coins, using mixers (tumbling services that pool and reallocate crypto) in between, to sever tracing links (Benson, Turksen and Adamyk, 2023). For example, the mixer service ChipMixer managed to launder 152,000 Bitcoins worth approximately $13 billion until its shutdown in 2023 (Kmieliauskas, 2025). Dark web markets, together with ransomware operations and additional serious offences, received most of those funds.

DeFi provides criminals with another option for fund transfer through liquidity pools and complicated token swapping procedures to obscure tracking. These transactions move at the speed of the internet and without borders, so law enforcement agencies (LEAs) find it hard to step in before it is too late. Additionally, DeFi has experienced a surge of fraudulent activities, including rug pulls, when developers drain funds after gaining user investments and hosting Ponzi schemes disguised as profitable farming opportunities. Users lack proper protection because there is no centralised control system. These incidents not only harm victims financially but also undermine trust in the ecosystem at large (Trmlabs.com, 2022).

Cyber-attacks and Exploits: The complex smart contract code and open nature of DeFi platforms present technical risks, which skilled attackers exploit. Many high-profile DeFi protocol hacks have occurred over the past few years, and hackers have stolen hundreds of millions of dollars from users. The Ronin Network suffered a $600 million loss in 2022, while Poly Network faced a $610 million theft attempt in 2021 but recovered part of the funds (Yao et al., 2025). Criminals discover logical bugs in smart contracts through their code analysis, for instance, identifying collateral value calculation or permission setting issues to execute malicious transactions that remove funds from systems.

The decentralised nature of blockchain means no authority is capable of halting suspicious transactions since code runs automatically according to its programming even when it results in total asset transfer to attackers. Attackers exploit DeFi protocols through flash loans, which provide unsecured one-blockchain-transaction financing to manipulate asset prices for profit and empty lending pools (Harvest Finance and other platforms fell victim to this attack method in 2020) (Oosthoek, 2021). The decentralised automated nature of DeFi enables attackers to conduct particular types of attacks, which have no parallel in traditional financial systems.

AI can supercharge cybercrime in this realm by helping find and exploit vulnerabilities at scale. For example, an AI agent could be trained to scan hundreds of

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

smart contracts for known bug patterns far faster than a human, automatically execute multi-step attacks (such as the flash loan manipulation sequence) and even adapt to defences. Ransomware groups use AI capabilities to develop better malware and phishing techniques, which produce higher rates of success when stealing private keys and exchange account data from users. The development of self-operating hacking AI systems presents a concerning future scenario because they may discover unknown vulnerabilities in DeFi code while running attacks independently of human supervision (TRM, 2025) .

Market Manipulation and Stability Risks: AI and algorithmic tools in the wrong hands can distort markets. *AI-powered trading bots*, already prevalent in crypto markets, can be employed to conduct manipulative strategies such as pump-and-dump schemes or flash crashes. Advanced bots exploit the collaboration between multiple DeFi platforms by linking decentralised exchanges and lending protocols to carry out wash trading or spoofing through false order placement, resulting in price manipulation for bots to profit (Sumner, 2025).

The speed and complexity of AI-driven strategies can outpace the ability of human traders or regulators to react, potentially leading to amplified volatility. Any implementation of algorithmic stablecoins that utilises automated algorithmic systems to manage pegs must be appropriately designed to prevent systemic risks from occurring. An algorithmic stablecoin suffered a total collapse in 2022, destroying tens of billions in value and spreading panic throughout the market (Metelski and Sobieraj, 2022). The pursuit of profit by an AI agent could potentially trigger attacks against these systems (as some traders did with Terra by shorting it during a moment of weakness and accelerating the death spiral) (Dearing, 2025).

Privacy Invasions and Surveillance: The advantages of anonymity through these technologies come with the danger of extensive monitoring and improper use of personal data. AI systems that operate with DeFi platforms possess the ability to identify users through on-chain activities and off-chain information such as IP addresses and behavioural data. The technique helps police capture offenders, yet it poses a threat to privacy protection when handled by unauthorised entities.

There is also concern about algorithmic bias and unfairness: if DeFi platforms start using AI for credit decisions or pricing, and those AI models are trained on biased data (perhaps reflecting historical discrimination or inaccuracies), they could reinforce inequities – denying certain groups loans or charging higher fees unjustly. Unlike a regulated bank, a decentralised platform has no equal opportunity laws governing its code. If an AI model exhibits bias, it might go unaddressed, especially if its workings are a 'black box' (opaque neural network) (Hassija et al., 2024). The implementation of biased algorithms leads to both ethical concerns and legal risks because they violate anti-discrimination standards while damaging the reputation of these technologies.

Financial systems that depend on IoT devices also generate privacy and safety problems. The majority of IoT devices acquire valuable personal data and

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

environmental data. If those data are published to a blockchain (even in processed form) or used by AI, questions arise: Who has access to the raw data? Is personal data being adequately anonymised? The system presents an opportunity for unauthorised tracking of people as well as the development of profiles without authorisation. The continuous observation of car insurance policyholders through IoT systems in smart contracts allows insurers and authorised users to track driving behaviour and locations, resulting in privacy concerns. A compromised attack on IoT devices creates threats that result in physical damage along with financial losses.

Automation at Scale and Loss of Human Oversight: The adoption of AI and automation creates a hidden threat to finance because human supervision becomes reduced. Financial systems with 'self-driving' capabilities tend to generate behavioural outcomes that humans do not expect, as well as collective operational malfunctions. The chaotic behaviour of automated trading has been shown through flash crashes in stock market trading. Users in DeFi worry about cascading failures: for instance, an AI agent liquidator might aggressively liquidate collateral on one platform, crashing prices that trigger liquidations on other platforms in a cascade. Traditional trade suspensions for panic control would have been possible through human intervention, but decentralised protocols lack built-in stopping mechanisms unless developers build them in. The May 2022 crypto market crash had elements of this, where automatic liquidations across lending platforms accelerated the price declines in a feedback loop (Avgouleas and Seretakis, 2023). Similarly, highly complex AI-driven derivatives might create hidden interdependencies and tail risks that are not well understood – akin to the CDOs (Collateralised Debt Obligations) and synthetic derivatives that contributed to the 2008 financial crisis, but potentially even more opaque if driven by AI.

In summary, the risk landscape of dual use is broad: from straightforward criminality (money laundering, fraud, hacking) through market integrity issues (manipulation, volatility) to systemic concerns (cascades, loss of control) and ethical pitfalls (bias, privacy breaches). The European Union, in its 2025 Serious and Organised Crime Threat Assessment, explicitly labels crypto-assets, DeFi and AI as offering a 'digital cloak' for money laundering and criminal finances (Kmieliauskas, 2025). This underscores that law enforcement perceives a growing threat posed by rising levels of illicit activity linked to emerging technologies. Criminal networks composed of private and nation-state actors (such as the North Korea-affiliated Lazarus Group) exploit DeFi bridges and exchanges to wash cryptocurrency stolen through hacks before moving the funds, for example, into weapons programmes (Yun and Wood, 2025). This scenario represents the perfect dual-use threat when emerging technology supports worldwide security challenges.

7.6 ETHICAL AND REGULATORY CONSIDERATIONS

The dual-use character of emerging financial technologies raises profound ethical questions and regulatory challenges. Financial technology stakeholders must handle

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

ethical matters such as privacy concerns, fairness issues, accountability requirements, and social technology effects. Regulators, for their part, are tasked with creating frameworks that mitigate harms (financial crime, consumer abuse, systemic risk) without unduly hampering innovation. The European Union has taken a proactive stance by drafting and implementing comprehensive regulations such as MiCA, the General Data Protection Regulation (GDPR), the AI Act, and a new AML regime to address these concerns in a coordinated manner.

Ethical Considerations: The main ethical dilemma exists between maintaining privacy and assuring transparency. The combination of blockchain-based finance transparency with analytics reduces user financial privacy because transactions become detectable. Is it ethical to have every transaction one ever makes be potentially traceable and analysed by AI? The crypto ethos often emphasises pseudonymity to preserve privacy and individual freedom (Zhuk, 2025). The ability of criminals to conceal their identity through pseudonyms creates a dilemma that prompts experts to demand transaction de-anonymisation for security purposes. Striking the right balance is difficult.

The EU's approach to privacy is anchored in the GDPR, which enshrines data protection as a fundamental right. The permanent nature of blockchain records creates difficulties when applying GDPR regulations because the GDPR's right to erase data conflicts with this characteristic. Designers of DeFi systems hold an ethical duty to evaluate data minimisation practices together with assessing the necessity to store sensitive personal data (such as IoT-collected health or location data for insurance or lending) either on-chain or off-chain through proof and aggregated results transmission (El Mestari, Lenzini and Demirci, 2024).

Closely related is the issue of algorithmic fairness and bias in AI. AI applications in finance must strictly avoid discriminatory practices and biased outcomes to fulfil ethical requirements. However, AI models learn from existing data, which may reflect societal biases. A lending AI, for example, could unintentionally eliminate applicants who belong to specific postal areas or backgrounds even though each applicant poses no risk of default because these areas show higher default rates in historical data, which amounts to digital redlining (Tilmes, 2022). The AI might not explicitly use protected characteristics such as race, but proxy variables could introduce bias. The EU's draft AI Act addresses this by classifying credit scoring algorithms as 'high-risk AI' that will be subject to strict requirements on data quality, transparency, and human oversight (Regnier, 2024). When using AI in DeFi deployment, all companies must conduct bias tests and maintain diverse data representations to prevent discriminatory results. The system must include explainability features that enable users to understand and question why AI denies loan requests. New legal requirements point in this direction since the AI Act plans to mandate documentation together with decision explanations for high-risk AI systems, and GDPR provides rights to individuals regarding automated decision-making.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

A significant ethical issue arises from the matters of responsibility and accountability. In decentralised, autonomous systems, who is responsible when things go wrong? If an AI-run smart contract causes a massive loss or behaves unpredictably, the traditional accountability model (holding a company or individual liable) becomes blurred. Code is law, but someone writes code – should developers bear responsibility for unforeseen abuses of their smart contracts? The open-source nature allows others other than authors to deploy the code, while anonymous token holders could potentially govern the DAO (Decentralised Autonomous Organisation). This diffuse responsibility challenges legal and ethical norms. The developers and governors who create protocols are required to provide safety protocols through proper auditing and emergency pause functionality in a manner similar to product liability standards.

The EU's trustworthy AI ethics guidelines require accountability through human involvement or another entity that takes responsibility for AI actions. DeFi protocols require similar safety mechanisms to guarantee human control and backup systems when making essential decisions concerning major updates or active security threats. The implementation of 'ethical by design' principles means establishing code-based protective measures which stop dangerous conduct. For example, the code architecture of lending smart contracts includes defensive programming features that prevent users from leveraging excessively even if they are not explicitly prevented from doing so, thus prioritising safety above efficiency (Vionis and Kotsilieris, 2024).

Globally, regulators are catching up with rapid innovations. The European Union, in particular, has rolled out a slate of regulations that, taken together, create one of the most comprehensive legal regimes for digital assets.

Markets in Crypto-Assets Regulation (MiCA) is the EU's landmark regulation for crypto-assets and associated services. MiCA establishes licensing requirements for crypto-asset service providers (CASPs) such as exchanges, custodians, and wallet providers, imposing obligations around capital, governance, disclosures, and consumer protection. It also regulates issuers of crypto-assets, including stablecoins (termed 'asset-referenced tokens' and 'e-money tokens' in the regulation) (Benson et al., 2024). MiCA's aim is to create a harmonised single market framework for crypto, balancing innovation with financial stability and investor protection. Importantly, MiCA largely avoids direct regulation of DeFi protocols that have no identifiable issuer or intermediary – a conscious choice acknowledging the difficulty of regulating pure decentralisation.

However, MiCA mandates the European Commission to produce, in a few years, a report on the emergence of DeFi and potentially propose adjustments. So, while DeFi currently sits in a 'grey zone', the trend is that if DeFi platforms have some governance body or provide certain services, they may eventually be brought into regulatory scope. Even now, if an entity actively facilitates a supposedly decentralised system (for instance, running a DeFi platform's front-end or controlling its

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

development), regulators might deem it a CASP subject to MiCA. Under MiCA, users gain rights such as clear information on crypto-assets and recourse mechanisms against service providers for fraud or operational failures (InnReg, 2025). This should deter some malicious behaviour by professionalising the industry. From a dual-use perspective, MiCA also integrates with AML laws – CASPs will be 'obliged entities' under AML rules, meaning they must do KYC and report suspicious activities.

Global Coordination versus Jurisdictional Arbitrage: Regulatory efforts face the challenge of DeFi and crypto activities being geographically diffuse. If regulations are too onerous in one region, projects or users may migrate to more permissive jurisdictions (a phenomenon known as regulatory arbitrage). The EU's approach, while comprehensive, will only directly cover activities in the EU or by EU-based entities. Nevertheless, its market size often forces global players to comply (as happened with GDPR). International bodies such as the Financial Action Task Force (FATF) are working to harmonise standards, for example, FATF's guidance includes applying AML rules to 'virtual asset service providers' and calls out DeFi (noting that creators, owners or operators of DeFi protocols may fall under regulation even if the marketing suggests the project is decentralised) (Europol, 2025).

This international pressure helps close gaps – for instance, by 2025, many countries will have implemented travel rule requirements for crypto (originator/beneficiary information with transfers), making it harder to find an AML blind spot (Rayner, 2024). Still, true DeFi with no intermediaries remains a regulatory challenge: you cannot KYC a smart contract or sanction an algorithm easily. Some proposals suggest regulators could target the user interface layer (e.g., websites through which users access DeFi) or rely on voluntary compliance mechanisms such as decentralised identity solutions. There is also discussion of creating whitelisting schemes: for example, liquidity pools that only accept funds from verified addresses, thus splitting the DeFi ecosystem into 'clean' and 'grey' pools (Ocampo, Branzoli and Cusmano, 2023). These are contentious but illustrate creative regulatory thinking.

An ethical evaluation requires attention to the dangers arising from excessive regulatory practices. The prohibition of privacy coins and mixers as a result of AML regulation has the potential to diminish both technical advances in privacy-enhancing technology and legitimate privacy rights. Unwarranted regulatory actions aimed at AI finance operations will strengthen established financial institutions while limiting the potential growth of new fintech startups. Forcing full identification on all crypto transactions would create a problem because it could build a surveillance financial system which diminishes users' cryptocurrency freedoms. To meet their ethical duty, regulators must implement regulations that reach their targets by minimising undesirable consequences. The EU tends to incorporate proportionality and stakeholder input in its laws.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

7.7 STATE-OF-THE-ART DEVELOPMENTS AND CURRENT INITIATIVES

The year 2025 marks a period when technology developers and regulators work together to harness DeFi, AI, and IoT benefits through new approaches that overcome developing challenges (FTSG, 2025). This section highlights some state-of-the-art developments on these fronts, including technical innovations, industry best practices, and nascent regulatory or collaborative initiatives.

Advancements in Blockchain and DeFi Technology: On the technical side, a major focus has been improving the scalability and interoperability of blockchain networks, which enhances performance and security (by reducing congestion-related exploits). The Ethereum network maintains most DeFi activity as it implements Proof of Stake transition and develops Layer-2 scaling solutions through Optimistic and ZK-Rollups that enable thousands of off-chain transactions with proof-based recording on the blockchain. These Layer-2 networks significantly increase throughput and lower transaction fees, making micro-transactions (vital for IoT use cases) economically viable and reducing the risk of blockchain overload during usage spikes (Camargo, 2023). Importantly, improved scalability also prevents specific spam attacks and reduces front-running issues in DeFi by shortening the time transactions spend in mempools (i.e., memory pools).

In parallel, cross-chain interoperability protocols (e.g., Polkadot, Cosmos, or bridge networks) are advancing to allow assets and data to flow between different blockchains. The future demands different specialised ledgers to perform unique tasks while interacting, such as an IoT-optimised ledger connected to a finance-optimised ledger. Still, bridges themselves have been targets of major hacks, so the state-of-the-art response is developing more secure bridging tech, such as 'trust-minimised bridges' using cryptographic proofs or decentralised validation (for example, Chainlink's forthcoming Cross-Chain Interoperability Protocol (CCIP) aims to securely relay data and tokens across chains using its decentralised Oracle network) (Camargo, 2023). These efforts, while technical, directly influence dual-use outcomes: a robust, interconnected infrastructure leaves less room for criminals to exploit isolated weak links or cause systemic outages.

Integration of Privacy-Enhancing Technologies (PETs): A noteworthy trend is the integration of PETs in blockchain and AI systems to merge transparency with privacy. Zero-knowledge proofs (ZKPs) have matured substantially and are now used to build privacy-preserving DeFi and identity solutions. For instance, protocols such as zkSync and Aztec enable transactions where the amounts and parties can be shielded but still cryptographically verified for correctness on Ethereum (Ismayilov and Özturan, 2025). There are prototypes of AML-compliant confidential transactions using ZKPs: a user could prove that their transaction does not involve blacklisted addresses or that they have undergone KYC without revealing their entire identity or transaction history on the public ledger. This is state-of-the-art because it potentially offers the 'best of both worlds' – anonymity for legitimate users and

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

traceability for bad actors (since a bad actor would be unable to produce proof of clean funds).

On the AI side, explainable AI (XAI) techniques are being actively researched for financial algorithms. Complex machine learning models (such as deep neural networks) are often 'black boxes', which is problematic in finance when a decision needs justification. New AI tools produce explanations together with indicators pointing out which variables affected model decisions – for example, through LIME (Local Interpretable Model-agnostic Explanations) or SHAP (SHapley Additive exPlanations) values. Financial institutions use these explainable AI systems to fulfil regulatory requirements and establish positive user relationships. An explainable AI loan approval system would notify applicants why they were rejected (for example, because of low income and high existing debt). This transparent approach replaces confusing denial with clear justification.

In trading, XAI helps risk managers understand AI-driven strategies so they can veto ones that might, say, concentrate too much risk. Many financial institutions have created their own AI ethics committees and model risk management procedures for AI in compliance with European Banking Authority standards (European Banking Authority, 2024). This is state-of-the-art in organisational practice, ensuring a human check on AI which, if widely implemented in DeFi teams and crypto projects, could prevent some dual-use outcomes (for instance, an AI feature that was found to be easily weaponisable might be modified or scrapped).

Case Study – RWA Tokenisation Boom: Tokenisation of real-world assets became a leading DeFi development during the latter part of 2024 and 2025. Projects enable blockchain integration of Treasury bills, trade receivables, real estate, and traditional assets that become blockchain-based tokens. Various startups alongside Goldman Sachs and Santander created public blockchain-based tokenised bond offerings while also launching DeFi-based short-term government bond versions that deliver interest. TradFi and DeFi systems blend together to form CeDeFi (centralised-decentralised finance).

The current advanced platforms within this domain establish multi-signature and escrow systems and create legal token wrappers for token rights registration, along with specific compliance tools that create blockchain-based regulated platforms (Zimperium.com, 2025). The dual-use perspective views this trend favourably because it adds legitimacy through oversight to DeFi but introduces potential risks when tokenised asset system breaches harm real-world financial markets. The continuous rise of RWAs entering DeFi platforms to exceed $10 billion within early 2025 (Tangem, 2025) represents the advancing state-of-the-art, which shows the decreasing distinction between DeFi and conventional finance systems.

Law Enforcement and Regtech Tools: On the regulatory side, we see governments and compliance firms deploying advanced blockchain analytics and AI tools as a state-of-the-art answer to financial crime. Companies such as Chainalysis, Elliptic, and TRM Labs have developed sophisticated software that uses machine

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

learning to cluster blockchain addresses, identifying likely exchange wallets, mixers, darknet markets, and mapping funds flows. These tools proved highly successful by monitoring ransomware payments through numerous transactions to detect exchange hits and reveal smart contract scam authors through linked patterns.

Law enforcement agencies in the EU and US now routinely use such analytics; in one case, the FBI and Europol traced and seized billions in crypto from the Silk Road case years after the crimes, showing that 'crime does not pay' if the blockchain trail remains. To keep up with criminals' use of AI, agencies are also experimenting with their own AI, for instance, Interpol's collaboration on an AI system to comb social media and the dark web for early warning of crypto scam campaigns. 'Follow the Money 2.0' represents the state-of-the-art method that employs AI to track digital funds through an automatic process spanning multiple blockchain networks and reaching data outside blockchains (Choi and Kim, 2025).

Regulators also launch innovation hubs and regulatory sandboxes focusing on fintech/DeFi and AI. The European Commission, through its Digital Finance Strategy, supports pan-European regulatory sandboxes for Distributed Ledger Technology (DLT), where companies can test innovative solutions under supervision (PwC, 2025). One such pilot allows selected firms to trial use cases such as trading tokenised bonds or using AI for AML on a blockchain, with regulators observing and providing feedback without immediate threat of enforcement. These sandboxes are state-of-the-art regulatory tools to learn and refine approaches in collaboration with industry. The knowledge gained feeds into guidelines and future regulation, ensuring laws keep pace with tech. The European Blockchain Sandbox (2023–2026) results will help shape regulatory changes to MiCA or the creation of separate rules for DeFi.

Cybersecurity and Resilience Efforts: The increasing number of hacks has led to enhanced efforts for better security measures in smart contract creation. Auditing firms (including CertiK and ConsenSys Diligence and Trail of Bits) employ manual expert assessment and automated analysis systems (some of which utilise AI technology) to examine code. Secure coding standards emerge as various auditing organisations distribute their best practices through a continuous consolidation process. There is movement towards 'formally verified' smart contracts – writing contracts in languages such as Coq or using verification tools (e.g., Certora, Ethereum's Vyper with formal specs) that mathematically prove specific properties (e.g., 'this contract will never allow an unauthorised withdrawal'). The application of formal verification remains rare because of its complexity, although advanced security specialists have used it to check critical contracts, especially portions of Ethereum 2.0 consensus code. High-value DeFi protocols are expected to implement routine extensive checks in the future to create better protection against hacking attempts (Xiang et al., 2024).

In terms of collaboration and knowledge-sharing, communities of practice have emerged. The DAO community works together to investigate security exploits

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

because researchers worldwide use Twitter and forums to analyse hacks and identify solutions within short periods following attacks. Such crowdsourced financial response marks a new approach in the field of finance. Ethical hackers now participate in bug bounty programmes operated by DeFi protocols since they receive compensation for detecting vulnerabilities before they become exploitable weaknesses. The payment of bounties totalling millions of dollars has proven to be more affordable than allowing actual security breaches to occur. The approach turns the global talent base that could participate in criminal activities into defenders of security through financial incentives, thus reducing dual-use risk (Arshad et al., 2024).

Finally, it is notable that academic research is active at this intersection of disciplines. Conferences and journals now regularly feature papers on topics such as AI for blockchain consensus optimisation, machine learning to predict DeFi liquidations, game-theoretic modelling of miner behaviour, and secure multi-party computation for privacy in finance. The state-of-the-art knowledge is thus rapidly evolving, and many cutting-edge ideas (such as using homomorphic encryption to compute on encrypted financial data or multi-agent AI simulations to test economic scenarios in crypto markets) are on the horizon of practical deployment.

7.8 FUTURE OUTLOOK AND CONCLUSION

The rapid convergence of blockchain, AI, and IoT in finance stands at an inflexion point. The coming years will likely define whether the optimistic vision of decentralised, intelligent financial systems empowering individuals can be realised or whether the pessimistic scenario of widespread abuse and regulatory restrictions will dominate. In reality, both paths will co-exist in a dynamic tension, and the outcome will be shaped by technological evolution, regulatory adaptation, and the collective actions of stakeholders.

Technological Trajectory: We can expect significant technical maturation in this space. Blockchain technology is likely to become more scalable (with Ethereum 2.0 upgrades and alternative high-throughput networks), more interoperable (through standardised protocols or even eventual consolidation of chains), and more user-friendly (abstracting away complex cryptographic processes behind intuitive interfaces). This will make the benefits of DeFi and associated tech accessible to a broader population – possibly integrating with mainstream banking apps or using corporations and governments for routine processes. Central Bank Digital Currencies (CBDCs) might also come into play: if major jurisdictions issue CBDCs, these could interface with DeFi protocols, blurring the line between traditional and decentralised finance even more.

AI is poised to become more potent with advances in deep learning and the availability of ever-larger datasets (including rich financial and IoT data). We may see autonomous economic agents become a reality – AI bots transacting,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

contracting, and collaborating with other bots and humans in financial markets. It raises the prospect of wholly machine-driven finance in some niches (for example, IoT devices negotiating for energy prices with each other, settling in cryptocurrency, and AI optimising their trading strategies).

Such a hyper-connected, AI-automated financial ecosystem would be efficient but highly complex and potentially fragile. It will demand new forms of risk management. Real-time oversight might shift towards AI as well – regulators might deploy their own AI 'agents' that roam the blockchain finance ecosystem, flagging rule violations or systemic risks instantaneously. Indeed, 'embedded supervision' is a concept the Bank for International Settlements has floated: using the transparent data from DLT to let compliance be automated (PwC, 2025). We might see regulatory nodes directly plugged into major blockchains, running analytics continuously. Regulation technology (RegTech) and SupTech (supervisory tech) will lean on AI to cope with the scale.

Regulatory Adaptation: Regulators are likely to refine and expand frameworks iteratively. The EU's MiCA and AI Act are first-generation rules – they will be reviewed and updated as the market and technologies evolves. By around 2026–2027, we expect discussions on 'MiCA 2.0' or dedicated DeFi regulations. Suppose DeFi platforms remain significantly non-compliant with AML norms – in that case, regulators may attempt more assertive measures: for example, a regime of licensed DeFi where major liquidity pools or protocols could voluntarily become certified under specific standards (much as exchanges are licensed) – offering users a safer option and marginalising rogue protocols. Alternatively, regulators might leverage chokepoints, requiring internet service providers or app stores to block known illicit decentralised applications, and so on. However, such measures raise censorship concerns and are easily bypassed by savvy users.

Global Cooperation: Given the global nature of the tech, international coordination should intensify. The G20 and bodies such as the International Organization of Securities Commissions (IOSCO) and FATF should push for baseline standards. FATF will likely update its guidance on virtual assets to clarify DeFi further – perhaps recommending that countries require DeFi project teams to register if they have control or to mandate that DeFi front-ends implement customer verification above specific volumes. We might also see bilateral agreements for sharing data on crypto transactions among law enforcement (somewhat akin to how SWIFT data is shared for bank transfers in anti-terrorism efforts).

On the other hand, divergence in approaches is also possible: some jurisdictions may intentionally position themselves as crypto-friendly with lighter rules to attract innovation (or illicit activity). There is a scenario where a kind of regulatory arbitrage arms race happens, with havens for unregulated DeFi persisting. However, the magnitude of risks (money laundering, investor harm) may pressurise even laissez-faire jurisdictions to come on board with basic norms, especially if lack of

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

compliance starts to exclude from the international financial system (e.g., greylisting by FATF).

Ethical and Social Outlook: Ethically, the dialogue around AI and autonomy in finance will sharpen. There will be a public reaction if AI causes a financial crash or deliberately biased outcomes. This could spur stricter ethical codes and possibly the involvement of external auditors or certifiers for algorithms (an idea floated in policy circles is creating something such as a 'Financial Algorithm Auditor' role). The concept of algorithmic accountability will become not just a guideline but an enforceable requirement. At the same time, society will likely grow more adapted to AI and digital finance – new generations may trust an AI adviser more than a human banker, for example.

Privacy will remain a contested domain. By 2030, perhaps, privacy-enhancing tech will mature so that users can routinely enjoy confidential transactions on public networks (Auer et al., 2025). Suppose law enforcement were also to develop methods for selectively piercing anonymity (through legal processes and advanced analytics), we might reach an equilibrium where everyday privacy is protected, but criminals still find it hard to hide – this is almost a *holy grail* outcome, reconciling dual use. Achieving it will require continuous innovation and dialogue between the cryptography community and regulators to embed 'lawful access' mechanisms without compromising overall security.

Conclusion: The dual use of emerging technologies in DeFi is not a temporary phase but a fundamental characteristic of our modern digital financial system. Just as the internet brought tremendous good while enabling new crimes, so will we manage the dual-use challenges of blockchain, AI, and IoT. The trajectory so far shows a pattern: groundbreaking innovation, exploitation by bad actors, and a cycle of adaptation with improved practices and regulatory oversight. Each cycle brings the technology to a more mature and stable state. We can be cautiously optimistic that the positive applications – financial inclusion, efficiency, resilience – will significantly outweigh the negatives with responsible innovation.

From a legal scholarship perspective, this domain will remain rich for analysis. The EU's legal frameworks will serve as a living laboratory: MiCA and the AI Act might need amendments as new types of assets or algorithms emerge (for instance, how to regulate AI-driven DAOs or value that only exists in the metaverse). Courts may also have to interpret how existing laws apply (e.g., liability in fully automated transactions, GDPR rights apply on a blockchain, etc.). New case law and perhaps new principles (such as treating code as persons for certain liabilities or recognising DAOs as legal entities) could develop.

Finally, one might recall the proverb, 'Technology is neither good nor evil; it is the use that makes it so'. DeFi, AI, and IoT convergence demonstrate this truth in the modern financial context. These tools can decentralise and democratise finance, create wealth, and improve risk management – but if unchecked, they can equally concentrate power in algorithms or facilitate large-scale crime. The challenge and

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

responsibility for the current generation of technologists, regulators, and scholars is to handle this dual-use potential towards broadly beneficial outcomes. That means building effective systems with ethics and compliance in mind from the design phase, encouraging collaboration between innovators and authorities, and educating users about opportunities and dangers.

REFERENCES

Adams J. and Young D. (2024) *Are fraudsters (soul)bound to fail? An overview of soulbound tokens and their use in fighting fraud*. Available at: www.penningtonslaw.com/insights/are-fraudsters-soulbound-to-fail-an-overview-of-soulbound-tokens-and-their-use-in-fighting-fraud/ (Accessed 9 September 2025).

Adamyk B., Benson V., Adamyk O. and Liashenko O. (2025) Risk management in DeFi: Analyses of the innovative tools and platforms for tracking DeFi transactions. *Journal of Risk and Financial Management*, 18(1), p. 38.

Ahamad S., Gupta P., Acharjee P. B., Kiran K. P., Khan Z. and Hasan M. F. (2022) The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market. *Materials Today: Proceedings*, 56, pp. 2070–2074.

Al Sadawi A., Hassan M. S. and Ndiaye M. (2022) On the integration of blockchain with IoT and the role of oracle in the combined system: The full picture. *IEEE Access*, 10, pp. 92532–92558.

Ali V., Norman A. A. and Azzuhri S. R. B. (2023) Characteristics of blockchain and its relationship with trust. *IEEE Access*, 11, pp. 15364–15374.

Arshad J., Talha M., Saleem B., Shah Z., Zaman H. and Muhammad Z. (2024) A survey of bug bounty programs in strengthening cybersecurity and privacy in the blockchain industry. *Blockchains*, 2(3), pp. 195–216.

Ashfaq A. (2022) *Application of Blockchain Technology & IoT Based Smart Sensors in Supply Chain Management via Business Development Approach*. Available at: https://webthesis.biblio.polito.it/22542/ (8 July 2025).

Auer R., Böhme R., Clark J. and Demirag D. (2025) *Privacy-enhancing Technologies for Digital Payments: Mapping the Landscape*. Available at: www.bis.org/publ/work1242.pdf (Accessed 8 July 2025).

Avgouleas E. and Seretakis A. (2023) How should crypto lending be regulated under EU law? *European Business Organization Law Review*, 24(3), pp. 421–438.

Benson V., Adamyk B., Chinnaswamy A. and Adamyk O. (2024) Harmonising cryptocurrency regulation in Europe: Opportunities for preventing illicit transactions. *European Journal of Law and Economics*, 57(1), pp. 37–61.

Benson V., Turksen U. and Adamyk B. (2023) Dark side of decentralised 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.

Berger P. (2021) *The EU Digital Finance Package. DLA Piper*. Available at: www.dlapiper.com/es-pr/insights/publications/2021/01/the-eu-digital-finance-package (Accessed 8 July 2025).

Camargo A. M. (2023). Integrating blockchain into global finance: A case study of SWIFT's strategic collaboration with Chainlink. *Revista de Gestão e Secretariado*, 14(12), pp. 21723–21738.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Chainalysis (2020) *DeFi Regulation and Compliance Requirements Remain Unclear. Chainalysis*. Available at: www.chainalysis.com/blog/defi-regulation-compliance/ (Accessed 11 April 2025).

Chang W. L. and Benson V. (2023) Migration and financial transactions: Factors influencing mobile remittance service usage in the pandemic. *Information Technology & People*, 36(5), pp. 2112–2136.

Choi, N. and Kim, H. (2025) Technological convergence of blockchain and artificial intelligence: A review and challenges. *Electronics*, 14(1), 84. https://doi.org/10.3390/electronics14010084 (Accessed 13 October 2025).

Clarke A. (2023) *Unleashing the Power of AI in Decentralized Finance: Opportunities and Challenges*. Available at: www.nasdaq.com/articles/unleashing-the-power-of-ai-in-decentralized-finance-opportunities-and-challenges (Accessed 9 September 2025).

Clements R. (2021) Built to fail: The inherent fragility of algorithmic stablecoins. *Wake Forest L. Rev. Online*, 11, p. 131.

David M. (2023) *Networked Crime: Does the Digital Make the Difference?* (1st ed.). Bristol: Bristol University Press. https://doi.org/10.2307/jj.4953556 (Accessed 9 September 2025).

Dearing T. (2025) *How AI Is Helping Hackers Hunt for Weaknesses*. Securityinfowatch.com. Available at: www.securityinfowatch.com/ai/article/55291093/how-ai-is-helping-hackers-hunt-for-weaknesses (Accessed 23 April 2026).

Dioquino V. (2025) *Real World Asset Tokenization to Hit $50B in 2025: Ozean. Decrypt*. Available at: https://decrypt.co/301222/real-world-asset-tokenization-to-hit-50b-in-2025-ozean (Accessed 13 October 2025).

Divyashree K. S. and Mishra A. (2025) Blockchain and IoT integration for financial sector revolution. In: Chowdhary C. L., Tripathy A. K., Wu Y. (eds.) *Smart Computing Techniques in Industrial IoT. Studies in Computational Intelligence*, vol. 1172. Springer, Singapore. https://doi.org/10.1007/978-981-97-7494-4_9 (Accessed 13 October 2025).

El Mestari S. Z., Lenzini G. and Demirci H. (2024) Preserving data privacy in machine learning systems. *Computers & Security* 137, p. 103605. https://doi.org/10.1016/j.cose.2023.103605 (Accessed 9 September 2025).

European Banking Authority (2024) *Special topic – Artificial intelligence. European Banking Authority*. Available at: www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence (Accessed 23 April 2026).

Europol (2025) *European Union Serious and Organised Crime Threat Assessment: The Changing DNA of Serious and Organised Crime*. Available at: www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf#:~:text=Europol%20www,automation%20has%20transformed%20illicit%20finance (Accessed 13 October 2025).

FTSG (2025) *2025 Tech Trends Report*. Available at: https://ftsg.com/wp-content/uploads/2025/03/FTSG_2025_TR_FINAL_LINKED.pdf (Accessed 23 April 2026).

George S. (2024) Finance 4.0: The transformation of financial services in the digital age. *Partners Universal Innovative Research Publication*, 2(3), pp. 104–125. https://doi.org/10.5281/zenodo.11666694 (Accessed 13 October 2025).

Gottschalk S. (2023) International financial regulation of cryptoassets and asset-backed tokens. In Kim, S.-J. (ed.) *Fintech, Pandemic, and the Financial System: Challenges and Opportunities* (pp. 145–181). Bingley: Emerald Publishing Limited.

Gummadi J. C. S. (2023) IoT security in the banking sector: Mitigating the vulnerabilities of connected devices and smart ATMs. *Asian Business Review*, 13(3), pp. 95–102.

Harvey C. R. and Rabetti D. (2024) International business and decentralized finance. *Journal of International Business Studies*, 55(7), pp. 840–863.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Hassija V., Chamola V., Mahapatra A., Singal A., Goel D., Huang K., Scardapane S., Spinelli I., Mahmud M. and Hussain A. (2024) Interpreting black-box models: A review on explainable artificial intelligence. *Cognitive Computation*, 16(1), pp. 45–74.

InnReg (2025) *Markets in Crypto-Assets Regulation (MiCA) Updated Guide*, InnReg. Available at: www.innreg.com/blog/mica-regulation-guide (Accessed 1 June 2025).

Ismayilov G. and Özturan C. (2025) PTTS: Zero-knowledge proof-based private token transfer system on Ethereum blockchain and its network flow based balance range privacy attack analysis. *Journal of Network and Computer Applications*, 233, p. 104045.

Khan B., Goh K., Khan A., Zuhairi M. and Chaimanee M. (2024) Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. *Processes*, 12(9), 1825. https://doi.org/10.3390/pr12091825 (Accessed 13 October 2025).

Kmieliauskas L. (2025) Europol labels crypto and AI as a 'money laundering cloak'. Available at: https://cybernews.com/crypto/europol-crypto-money-laundering-ai (Accessed 9 September 2025).

Kornaros G. (2022) Hardware-assisted machine learning in resource-constrained IoT environments for security: Review and future prospective. *IEEE Access*, 10, pp. 58603–58622.

Kranjec J. (2025) *Total value locked in DeFi soars 137% YoY to a staggering $129 billion*. FOCUS ON Business. Available at: https://focusonbusiness.eu/en/news/total-value-locked-in-defi-soars-137-yoy-to-a-staggering-129-billion/6554 (Accessed 13 October 2025).

Kute D. V., Pradhan B., Shukla N. and Alamri A. (2021) Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review. *IEEE Access*, 9, pp. 82300–82317.

Laghari A. A., Wu K., Laghari R. A., Ali M. and Khan A. A. (2021) A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, pp. 1–19.

Lakhchini W., Wahabi R. and Kabbouri M. E. (2022) Artificial intelligence & machine learning in finance: A literature review. *International Journal of Accounting, Finance, Auditing, Management and Economics*, 3(6-1), pp. 437–455.

Malhotra D., Saini P. and Singh A. K. (2022) How blockchain can automate KYC: Systematic review. *Wireless Personal Communications*, 122(2), pp. 1987–2021.

Mazhar T., Irfan H. M., Khan S., Haq I., Ullah I., Iqbal M. and Hamam H. (2023) Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet*, 15(2), p. 83.

Metelski D. and Sobieraj J. (2022) Decentralized finance (DeFi) projects: A study of key performance indicators in terms of DeFi protocols' valuations. *International Journal of Financial Studies*, 10(4), p. 108.

Ocampo D., Branzoli N. and Cusmano L. (2023) *Crypto, Tokens and DeFi: Navigating the Regulatory Landscape*. Bank for International Settlements. Available at: www.bis.org/fsi/publ/insights49.pdf (Accessed 23 April 2026).

Oosthoek K. (2021) Flash crash for cash: Cyber threats in decentralized finance. *arXiv preprint*. Available at: https://arxiv.org/abs/2106.10740 (Accessed 23 April 2026).

Papadopoulos P., Pitropakis N. and Buchanan W. J. (2022) Decentralized privacy: A distributed ledger approach. *In Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0* (pp. 1805–1830). Cham: Springer International Publishing.

Pillai V. (2023) Integrating AI-driven techniques in big data analytics: Enhancing decision-making in financial markets. *International Journal of Engineering and Computer Science*, 12(07), pp. 25774–25788.

PwC (2025) *PwC Global Crypto Regulation Report 2025*. (*Legal.pwc.de*, 2025). Available at: https://legal.pwc.de/content/services/global-crypto-regulation-report/ (Accessed 9 September 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Rane N., Choudhary S. and Rane J. (2024) Artificial Intelligence (AI), Internet of Things (IoT), and blockchain-powered chatbots for improved customer satisfaction, experience, and loyalty. Available at : https://ssrn.com/abstract=4847274 (Accessed 9 September 2025).

Rayner B. (2024) *2025 Trends in AML and Financial Crime Compliance: A Data-Centric Perspective and Deep Dive into Transaction Monitoring*. Available at: www.silenteight.com/blog/2025-trends-in-aml-and-financial-crime-compliance-a-data-centric-perspective-and-deep-dive-into-transaction-monitoring (Accessed 23 April 2026).

Regnier T. (2024) *Artificial Intelligence – Questions and Answers*. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_168 (Accessed 23 April 2026).

Sedlmeir J., Lautenschlager J., Fridgen G. and Urbach N. (2022) The transparency challenge of blockchain in organizations. *Electronic Markets*, 32(3), pp. 1779–1794.

Sumner J. (2025) *The AI-Crypto Nexus: Navigating the Risks and Rewards of a Transformative Convergence*. GRC World Forums. Available at: www.grcworldforums.com/risk-digital-north-america/the-ai-crypto-nexus-navigating-the-risks-and-rewards-of-a-transformative-convergence/10023.article (Accessed 23 April 2026).

Kmet C. T. (2018) *How Blockchain, AI, and IoT Are Reshaping Finance*. Available at: www.icpas.org/information/copy-desk/insight/article/winter-2018/how-blockchain-ai-and-iot-are-reshaping-finance (Accessed 23 April 2026).

Tangem (2025) *Top 10 Real World Assets (RWA) Crypto in April 2025. Tangem Blog*. Available at: https://tangem.com/en/blog/post/real-world-assets-rwa/ (Accessed 23 April 2026).

Tigard D. (2022) Embedded ethics as preparatory regulation of technology: A new solution to the Collingridge Dilemma? In Lawrence, D. R. and Morley, S. (eds.) *Novel Beings: Regulatory Approaches for a Future of New Intelligent Life* (pp. 12–28). Cheltenham: Edward Elgar Publishing.

Tilmes N. (2022) Disability, fairness, and algorithmic bias in AI recruitment. *Ethics and Information Technology*, 24(2), p. 21.

TRM (2025) *The Rise of AI-Enabled Crime: Exploring the evolution, risks, and responses to AI-powered criminal enterprises*. TRM Insights. Trmlabs.com. Available at: www.trmlabs.com/resources/blog/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises (Accessed 23 April 2026).

Trmlabs.com (2022) *Illicit Crypto Ecosystem Report*. Available at: www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022 (Accessed 23 April 2026).

Turksen U., Benson V. and Adamyk B. (2024) Legal implications of automated suspicious transaction monitoring: eEnhancing integrity of AI. *Journal of Banking Regulation*, 25(4), pp. 359–377.

Vaigandla K. K., Karne R., Siluveru M. and Kesoju M. (2023) Review on blockchain technology: Architecture, characteristics, benefits, algorithms, challenges and applications. *Mesopotamian Journal of CyberSecurity*, 2023, pp. 73–84.

Vaseashta A. (2025) Intrinsic and existential risks associated with emerging security threats from dual-use technologies. In Rocha, Á. and Vaseashta, A. (eds.) *Multidisciplinary International Conference of Research Applied to Defense and Security* (pp. 125–137). Singapore: Springer Nature Singapore.

Vasishta P., Dhiman A., Smith S. and Singla A. (2025) How can DeFi improve the quality, affordability, access and usage of financial services? A systematic literature review. *Journal of Economic and Administrative Sciences*. Available at: https://doi.org/10.1108/JEAS-07-2024-0243Yes (Accessed 23 April 2026).

Vionis P. and Kotsilieris T. (2024) The potential of blockchain technology and smart contracts in the energy sector: A review. *Applied Sciences*, 14(1), p. 253.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Xiang D., Lin Y., Nie L., Zheng Y., Xu Z., Ding Z. and Liu Y. (2024) An empirical study of attack-related events in DeFi projects development. *Empirical Software Engineering*, 29(2), p. 49.

Yao S., Ni H., Ma S., Schiff N., Myers A. C. and Cecchetti E. (2025) A language for smart contracts with secure control flow (technical report). *arXiv.org*. Available at: https://arxiv.org/abs/2407.01204 (Accessed 26 October 2025).

Yun Y. and Wood A. (2025) *Timeline*: *How Bybit's lost Ethereum went through North Korea's washing machine*. Cointelegraph. Available at: https://cointelegraph.com/news/timeline-bybit-lost-ethereum-north-korea-money-launder (Accessed 13 October 2025).

Zhuk A. (2025) Beyond the blockchain hype: Addressing legal and regulatory challenges. *SN Social Sciences*, 5(2), pp. 1–37.

Zimperium.com (2025) *Multisig Wallets*. Available at: https://zimperium.com/glossary/multisig-wallets (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

8

The Use of AI by Banks in Financial Crime Risk Management

Adam Abukari, Julia Werberich, and Ololade Durodola

8.1 INTRODUCTION

The digital age has ushered in an era where criminals use advanced technologies to flood the financial system with financial crime risks (FCRs), showing a level of sophistication that traditional crime prevention measures struggle to counteract effectively. Article 3(2) of the EU AI Act 2024 defines risk as 'the combination of the probability of an occurrence of harm and the severity of that harm'. According to the UK's Financial Conduct Authority (FCA's) 2025 Firm's Guide to Countering Financial Crime Risks FCRs (FCA, 2025), FCRs include but are not limited to risk of money laundering and terrorist financing; fraud; bribery and corruption; sanctions, asset freezes, and proliferation financing; and insider dealing and market manipulation. Banks such as HSBC see FCR as the risk that their products and services will be exploited for criminal activities such as 'fraud, bribery and corruption, tax evasion, sanctions and export control violations and evasion, money laundering, terrorist financing and proliferation financing' (HSBC, n.d.). In an increasingly interconnected economic landscape, financial institutions face a persistent and growing threat from resourceful and adaptable financial criminals, who engage in these criminal offences. These crimes pose unprecedented threat to the integrity and stability of financial systems worldwide.

8.1.1 *Traditional and AI Approaches to Countering FCRs*

Classical approaches to preventing and addressing financial crime, which historically relied heavily on manual oversight, intuitive analysis, and reactive measures, have, therefore, undergone considerable revision. The limitations of these traditional systems have become increasingly clear in the face of evolving criminal tactics. As an inevitable counterforce, the field of financial crime prevention and countering has had to integrate advanced Artificial Intelligence (AI)-driven algorithms into the traditional preventive strategies.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Pursuant to Article 3(1) of the EU AI Act, AI is defined as a machine-based platform or computer system designed with differing levels of operational autonomy, which could show 'adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'. AI mimics human intelligence to act in diverse settings, with capability to perform tasks that typically require human intelligence to excel (Chowdhary and Chowdhary, 2020). For instance, AI performs tasks such as understanding of natural language, recognition of patterns, decision-making, and learning from experience with minimal human intervention (Balcıoğlu, 2024; Rashid and Kausik, 2024).

While the traditional systems are often rule-based and are limited in their real-time risk detection and capabilities, AI can swiftly analyse vast transactional data, identifying anomalies and potentially fraudulent or other illicit activities in real time. For instance, deep learning (e.g., neural networks) is one of the tools, which can be trained on historical fraud data to precisely discern intricate patterns and predict fraudulent transactions (Aziz and Andriansyah, 2023). Banks are uniquely positioned to leverage AI technologies to transform the traditional risk management paradigms, substituting manual analyses with advanced algorithms that process extensive datasets in real time. AI's machine learning algorithms are trained and exposed to vast data overtime, the algorithms refine their accuracy in making decisions or predictions, and mimicking human learning process, but done at a scale and speed that humans are not able to effectively emulate. This characteristic offers significant opportunities for managing FCRs in banks' activities (Hilal, Gadsden, and Yawney, 2022).

8.1.2 *Determining the Use of AI in Financial Crime Risk Management (FCRM)*

Amidst the evolving threat landscape, AI has emerged as a critical strategic asset, which fundamentally alters the approach to FCRM. FCRM encapsulates a broad range of practices designed to identify, assess, and mitigate risks faced by financial institutions. It serves as the cornerstone of financial integrity, health, and stability within the sector, ensuring the longevity and resilience of financial entities against market volatilities, credit failures, operational breakdowns, and fraudulent activities.

AI has the power to enhance the effectiveness and efficiency of detection and mitigation processes of these illicit activities. It also has the power to ensure comprehensive compliance with the ever evolving and increasingly stringent regulatory frameworks. The capability of AI to ingest vast quantities of structured and unstructured data, detect subtle patterns and anomalies, and continuously learn

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

from new information is transforming how banks identify, assess, and mitigate illicit behaviour.

FCRM remains a paramount concern for senior executives in the financial services industry, with AI increasingly leveraged to enhance detection, mitigation, and regulatory compliance (Durodola, 2021). Financial institutions leverage AI to conduct analysis on patterns in large transaction datasets for identification of anomalies that could elicit criminal activities (Hilal, Gadsden, and Yawney, 2022). This helps financial institutions such as banks to take proactive steps to prevent financial loss and maintain trust and integrity (Balcıoğlu, 2024). AI use in risk management in banks is crucial because the need for further development of this area constantly grows (Milojević, 2021). AI in FCRM provides a promising mechanism for not only optimising risk assessment but also enhancing operational resilience and improving decision-making processes for banks, thereby ushering in an era of sustainable and responsible innovation that aligns with Fairness, Education, Accountability, and Transparency (FEAT) that undergird AI adoption (Garud, 2025; Kishore, 2025).

The utility of AI in FCRM, however, comes with challenges such as in relation to data quality, data security, regulatory compliance, algorithmic bias, regulatory uncertainties, system integration and algorithm optimisation, model explainability, and ethical dilemmas (Mittelstadt, 2016; Durodola, 2024). Sustainable FCRM is, therefore, contingent on navigating the challenges and taking advantage of opportunities to operationalising an AI ecosystem that prioritises FEAT decision-making and implementation methodologies. This is an innovative way to the sustainable and responsible use of AI in FCRM.

This chapter examines the sustainable and responsible deployment of AI in FCRM from two dimensions. It involves how to leverage AI to improve efficiency, effectiveness, and predictive accuracy. It also includes building a resilient AI governance architecture that bolsters elements such as proactive regulatory framework, ethical oversight, establishment of standards, and best decision-making practices within financial institutions such as banks to ensure that the use of AI aligns with societal wellbeing and the FEAT (Dafoe, 2024).

The chapter uniquely synthesises rich insights from theoretical and empirical studies to demonstrate the direction in which financial institutions should navigate to ensure sustainable and efficacious use of AI in FCRM to fighting financial crime including fraud detection, anti-money laundering (AML) compliance, and enhanced Know Your Customer (KYC) verification, while also exposing critical vulnerabilities exploited by financial criminals. The rest of this chapter is, therefore, organised as follows: Section 8.2 explores AI application and use cases. This is followed by Section 8.3, which presents voices of bank employees while challenges and opportunities are presented in Section 8.4. Section 8.5 presents AI and FEAT in FCRM. The conclusion of this chapter is then presented in Section 8.6.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

8.2 APPLICATIONS OF AI IN FINANCIAL CRIME

8.2.1 *AI in Financial Crime Prevention and Detection*

The establishment of digital banking and the proliferation of online financial services have increased the potential for criminal activities in financial institutions, which makes the prevention of and protection against criminal activities in banks both a matter of mitigating financial loss and maintaining consumer trust as well as market stability (Al-Badran, 2021). AI has rapidly matured into a practical and indispensable tool for financial institutions seeking to safeguard their operations and protect their customers, crossing both prevention and detection applications. The synergy between these two dimensions is critical: while prevention enables financial institutions to proactively neutralise emerging threats with remarkable speed, precision, and effectiveness, thereby significantly reducing their exposure to a wide spectrum of financial risks, detection ensures the processing of massive and intricate data streams to allow for the identification of subtle and previously undetectable patterns indicative of fraudulent behaviour. Therefore, this dual approach offers a robust framework for financial institutions to operate securely in an increasingly complex threat landscape.

On the one hand, prevention strategies primarily leverage AI's predictive capabilities, enabling financial institutions to anticipate potential threats before they materialise. This foresight allows for the deployment of proactive countermeasures, including advanced identity verification processes, sophisticated behavioural analytics, and robust predictive modelling techniques. These AI-powered tools analyse historical data and identify emerging trends to dynamically assess and recalibrate customer risk profiles, enabling a more targeted and effective allocation of preventive resources.

Conversely, detection methodologies emphasise real-time AI-powered surveillance, meticulous and continuous transaction monitoring, and intricate network analysis. These tools are specifically designed to swiftly identify and respond to illicit activities that have successfully circumvented initial preventive defences. Real-time transaction monitoring systems powered by AI can instantaneously assess the risk associated with financial transfers, effectively halting questionable transactions before completion and preventing potential losses. Furthermore, AI's analytical capabilities extend to dissecting and interpreting complex transactional networks, uncovering clandestine financial relationships, shell companies, and ultimately dismantling fraudulent schemes.

8.2.1.1 AI-Driven Tools for Preventing Financial Crime

8.2.1.1.1 REVOLUTIONISING KYC AND DUE DILIGENCE WITH AI. Traditional KYC processes have historically been characterised as cumbersome, labour-intensive, and

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

prone to human error and inefficiency. These processes, often requiring extensive manual review of documentation and significant personnel resources, have undergone revolutionary transformations due to the integration of AI-driven tools such as the adoption of AI-driven biometric verification systems, advanced document authentication procedures, and optical character recognition (OCR) technologies. This integration has led to substantial improvements in accuracy, speed, efficiency, and reliability. For instance, AI-powered systems can achieve verification accuracy as high as 99 per cent and reduce the time taken for customer screening and onboarding from hours to just seconds (Kothinti, 2025).

Furthermore, natural language processing (NLP) techniques have enabled institutions to maintain a real-time and comprehensive understanding of potential risks. By constantly scanning and analysing global media outlets, regulatory databases, and adverse news reports, NLP significantly enhances proactive risk identification and mitigation strategies. AI agents utilising NLP can efficiently screen vast quantities of unstructured data, such as thousands of negative news articles daily, to identify relevant risk information concerning individuals or entities (Mahadevkar et al., 2024).

Moreover, behavioural analytics, powered by sophisticated machine learning algorithms, dynamically recalibrate customer risk profiles based on continuously evolving transaction behaviours, digital activity, and social network associations. AI facilitates a continuous risk assessment process, adjusting risk scores in real-time as new data becomes available, ensuring that risk profiles remain current and reflective of the latest customer activities and market conditions. This proactive monitoring allows for the early detection of potential security risks and anomalous behaviours that may indicate fraudulent activity (Wang, 2024).

Additionally, graph analytics leverage AI's computational capabilities to dissect, interpret, and illuminate complex transactional networks. By linking various entities such as individuals, addresses, companies, and bank accounts, graph analytics effectively uncover clandestine financial relationships, shell companies, and ultimately dismantle fraudulent schemes before they can fully materialise or inflict substantial financial damage. Techniques like entity resolution and network filtering, often enhanced by deep learning methodologies such as graph representation learning, enable financial institutions to gain a comprehensive understanding of intricate cash flow relationships and identify high-risk entities within these networks (Cheng, et al., 2025).

8.2.1.1.2 FRAUD PREVENTION WITH ADAPTIVE TOOLS. As will be shown in detail, financial institutions highlight the importance of using advanced AI-driven tools, such as anomaly detection algorithms, to address sophisticated and adaptive fraud attempts. These AI tools meticulously identify unusual transactional behaviours that deviate from established norms, which can be indicative of potential fraud, thereby substantially enhancing institutions' preventive capabilities. AI dramatically

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

improves anomaly detection by processing vast amounts of data in real-time and adapting to new forms of fraud, providing instant alerts when suspicious activity is detected.

Supervised and unsupervised machine learning methodologies significantly refine the predictive accuracy of AI systems. Supervised learning models, trained on labelled historical fraud data, excel at identifying known fraud patterns, while unsupervised learning algorithms are particularly valuable in detecting emerging fraud typologies and proactively identifying previously unseen threats without relying on pre-existing labels (Sarker, 2021; Chaudhary, Khurana and Ayalasomayajula, 2024). This combination allows institutions to address both established and novel forms of financial crime with greater efficacy.

Furthermore, deep learning models exhibit unparalleled precision in detecting payment-related fraud. These models, capable of processing large and complex datasets, can identify subtle patterns indicative of fraudulent transactions. This capability is further complemented by AI-powered device fingerprinting techniques, which create unique identifiers for devices based on their hardware and software configurations, helping to distinguish between legitimate users and potential fraudsters.

Additionally, AI plays a crucial role in synthetic identity fraud detection by analysing vast datasets to identify inconsistencies and anomalies that often signal the presence of fabricated identities (Zhang, Gill, Liu and Anwar, 2025). These advanced AI methodologies collectively provide comprehensive protection against advanced, innovative, and continuously evolving financial threats.

8.2.1.2 AI-Driven Tools for Detecting Financial Crime

8.2.1.2.1 TRANSACTION MONITORING: SPEED, SCALE, AND PRECISION. Traditional rule-based transaction monitoring systems, often relying on predefined scenarios and thresholds, can miss novel or complex threats and frequently generate a high volume of false positive alerts. As stated below, bank employees in the UK have reported substantial improvements through AI-driven predictive analytics, which proactively and accurately flag suspicious transactions while significantly reducing the incidence of false positives, thereby streamlining investigative processes. AI can present self-learning anomaly detection systems or models that can dynamically adapt to evolving fraud patterns, which could significantly reduce false positives compared to traditional rule-based systems (Fritz-Morgenthal, Hein and Papenbrock, 2022). Thus, AI can help mitigate risks associated with fraud by employing advanced algorithms to detect suspicious activities or transactions in real-time, thereby enhancing the security of financial transactions (Mohan, 2024).

Real-time AI-driven transaction screening systems instantaneously assess transaction risks, effectively halting questionable transfers before completion, thus

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

preventing potential losses. These systems provide immediate transaction oversight and can be integrated seamlessly into existing infrastructure. Moreover, AI's nuanced, risk-based scoring models enable investigators to efficiently prioritise cases. AI-based systems can assign risk scores to customers based on their past activity and KYC information, allowing for a more focused allocation of investigative resources. Automated case management systems further enhance detection accuracy and responsiveness by clustering related suspicious activities and providing comprehensive analyses.

These AI-powered platforms consolidate all relevant compliance data into a unified investigative environment, offering real-time access to customer risk profiles, transaction histories, and regulatory reports, ultimately leading to faster and more informed decision-making.

8.2.1.2.2 AI'S EXPANDING ROLE IN AML OPERATIONS. Historically, traditional AML methods have consistently struggled to match the increasingly sophisticated tactics employed by criminal organisations. Rule-based systems often find it difficult to adapt to evolving money laundering techniques such as smurfing, layering, and the use of high-risk jurisdictions. However, AI-driven graph analytics have exceptional efficacy, capable of reconstructing complex transaction flows and uncovering advanced money laundering techniques, such as layering and structuring, with unprecedented clarity and precision (Pavlidis, 2023). Graph analytics enables the identification, analysis, and visualisation of relationships between entities based on various data points, offering innovative ways to combat money laundering and improve the effectiveness of traditional AML programmes (Pavlidis, 2023).

Additionally, AI-driven transaction linking reveals intricately disguised patterns that would typically evade detection by rule-based systems, significantly enhancing investigative accuracy (Goldbarsht, 2023). AI algorithms analyse multiple data points to identify suspicious patterns of activity, complementing traditional review processes and spotting patterns hidden within large volumes of data. Automated adverse media screening further fortifies institutions' AML capabilities by proactively identifying high-risk entities. By continuously monitoring various media sources for negative news concerning individuals or entities, these AI-powered tools provide a crucial additional layer of risk assessment that was previously unattainable through manual or traditional processes alone.

8.2.1.2.3 CYBER THREAT AND AI DEFENCE. The proliferation of cyber threats has considerably intensified the risks faced by financial institutions, therefore requiring the deployment of sophisticated AI-enhanced intrusion detection systems (IDS) (Arreche, Guntur and Abdallah, 2024). These AI-powered systems autonomously monitor network activity, swiftly detecting anomalies indicative of security breaches, malware incursions, or unauthorised access attempts (Devarajulu, 2022).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

AI-driven NLP tools effectively identify phishing attempts and malware threats, further enhancing institutions' defensive capabilities. NLP enables AI to analyse the content and context of communications, recognising malicious intent and flagging suspicious language or patterns commonly associated with phishing attacks (Pavlidis, 2023). Advanced AI methodologies are also instrumental in combating emerging and complex threats, such as deepfake identity fraud and increasingly sophisticated algorithmic phishing attacks, which are explicitly highlighted as growing concerns by banking professionals. AI-powered systems can detect subtle inconsistencies in audio, video, and images that are imperceptible to the human eye and ear, providing a critical defence against these advanced forms of impersonation and fraud (Salem et al., 2024).

8.3 VOICES OF BANK EMPLOYEES ON THE USE OF AI

While our critical analyses above have thrown more light on the existing literature, the empirical dimension of these elements in the context of benefits and utility has been limitedly approached. This sub-section, thus, explores UK banking employees' perspectives on AI adoption in relation to advantages and best practices for responsible deployment and utilisation in AI-driven FCRM systems. In this regard, we anecdotally surveyed thirty-seven employee respondents (including frontline client-facing teams, compliance officers, risk analysts, and AI specialists) from top three UK high street banks (i.e., Barclays Bank, HSBC Bank, and Lloyds Banking Group), selected based on their description as a major UK bank by the Bank of England in its 2024 resolvability assessment of major UK banks published on the 6th of August 2024 (Bank of England, 2024). We have then analysed the findings from this anecdotal survey on the perspectives of bank employees on AI's application in FCRM in the three UK banks, along with authoritative statements of senior bank managers we extracted from the websites of the banks and third parties. These have been complemented with findings from a 2024 AI qualitative survey by the Bank of England and FCA based on 118 survey responses (Bank of England and FCA, 2024). The following thematically represent the results therefrom.

The first theme considered was strategic advantages. One of the strategic advantages of AI in FCRM identified by all the thirty-seven respondents is that AI enhances fraud detection and transaction monitoring. Respondents posit that AI-driven fraud detection algorithms identify anomalous financial behaviours in real time, strengthening response mechanisms. They also opine that machine learning models reduce false positive rates, improving efficiency in fraud mitigation (El Hajj and Hammoud, 2023; Jofre, Bosisio and Riccardi, 2024).

Another strategic advantage is that AI deployment in FCRM ensures operational efficiency and cost optimisation. To this end, respondents have averred that responsible deployment of AI can automate compliance tasks, streamline labour-intensive processes and reduce operational costs (Doddipatla, 2024). Respondents also observe

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

that AI-enhanced KYC frameworks expedite customer due diligence while ensuring regulatory adherence. This is in line with authoritative statements from NatWest, HSBC, and Barclays extracted from the internet. For instance, the Head of Payment Fraud of NatWest, Nick Elliot, observes that a new Mastercard's AI tool helps the bank to 'identify payments to fraudsters and stop them before money is lost' (Mastercard, 2024).

Similarly, HSBC's Group Head of Financial Crime, Jennifer Calvery, notes that 'AI has helped us to improve the precision of our financial crime detection and reduce alert volumes, meaning less investigation time is spent chasing false leads . . . contributing to more effective outcomes in the fight against financial crime' (Calvery, 2024). Barclays Group Chief Information Officer, Craig Bright, has also said that 'while analytical AI has long helped us manage fraud and money laundering risks, generative AI creates opportunities to help us reduce these even more – something that is absolutely essential for us as a bank' (Barclays, 2024).

In fact, as part of the above advantage, the adoption of AI in UK financial services has grown significantly, with banks leveraging machine learning and generative AI to address FCRs. The 2024 Bank of England and FCA AI survey shows that of 118 survey responses, 75 per cent of financial firms currently use AI, with an additional 10 per cent planning to adopt it in the next three years. The survey highlights that 33 per cent of respondents are using AI for fraud detection, and an additional 31 per cent plan to do so over the next three years. AML and combating the financing of terrorism (CFT) are also among the top use cases, with 64 per cent of firms either currently using or planning to use AI in these areas (Bank of England and FCA, 2024).

Ensuring regulatory compliance and institutional reputation is yet another advantage espoused by the respondents under the strategic advantages' theme. In this regard, AI-driven risk assessment tools bolster compliance with regulatory bodies such as the FCA and the Competition and Markets Authority (CMA). In the same vein, AI strengthens compliance mechanisms in FCRM to reinforce institutional credibility and clients' trust.

Apart from the strategic advantages, gendered disparities in AI perceptions were thematised. The responses on this theme exhibit notable gender-based variations in attitudes toward AI for FCRM in banking. While female respondents are more likely to affirm the ethical viability of AI in FCRM, male respondents display a broader range of opinions, including higher levels of uncertainty. These findings resonate with prior research indicating that gender influences ethical decision-making and risk aversion in financial contexts (Marcus and Hargrave, 2021). Studies such as Huang and Kisgen (2013) suggest that women in financial sectors tend to exhibit heightened ethical awareness and greater caution in risk assessment (Huang and Kisgen, 2013).

The other theme considered is generational divide in AI acceptance. Here, the data reveals that younger banking professionals exhibit a stronger propensity to

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

endorse AI as an effective tool for financial crime mitigation, whereas older respondents present a more ambivalent or critical stance. This divergence is aligned with existing scholarship on technology acceptance, which posits that younger demographics may demonstrate a higher level of adaptability to AI-driven solutions in financial services (Dwivedi et al., 2021). Resistance among older professionals may stem from entrenched scepticism regarding AI's capacity for unbiased decision-making and regulatory compliance.

The last theme considered is institutional trust and risk perception. The dataset on the thirty-seven respondents suggests that professional trust in AI governance frameworks significantly influence attitudes toward AI ethics. Respondents who have expressed neutrality or disagreement with AI deployment in FCRM harbour concerns regarding algorithmic bias, data privacy risks, and regulatory oversight (De Silva, 2025). Conversely, respondents in strong agreement view AI as an indispensable instrument in combating financial crime through automation and predictive analytics. These survey results resonate with findings from statements of Lloyds Banking Group and NatWest Group executives on their websites. For instance, talking about Lloyds Banking Group's AI Centre of Excellence, Dr Rohit Dhawan, Director of AI and Advanced Analytics at the Group, has observed that as they push the boundaries of GenAI, it is 'vital that we have the appropriate safeguards in place to ensure the technology is implemented ethically and safely' (Lloyds Banking Group, 2025). In the same vein, NatWest Group Chief Information Officer, Scott Marcar, notes that AI 'is already playing a vital role in our digital transformation' and that bank commits to deploying it 'in the safest and most responsible way' under a strict ethics code (NatWest Group, 2025).

8.4 CHALLENGES AND OPPORTUNITIES OF AI IN FCRM

The increasing integration of AI into FCRM has been associated with several challenges and opportunities, which change the ecosystem of regulatory compliance in relation to financial services. We have explored a few of these challenges and opportunities that contribute to robust FCRM systems.

One of the primary challenges of FCRM is that financial institutions need to upgrade their underlying data to ensure high-quality data and analytics capabilities, which comes with significant costs. The voices of the thirty-seven UK bank employees also point out that effective integration of AI depends on building and sustaining robust data quality infrastructures. This is in line with participants in numerous studies that stress that the accuracy and reliability of AI outputs are fundamentally connected to the quality of input data, and that insufficient or poor data quality can lead to misinterpretation of financial risks. For instance, the 2024 Mosaic study of six million fixed income, currencies, and commodities (FICC) transactions from global and regional investment banks in Australia, Canada, European Union (EU), Japan, South Africa, South America, UK, and US finds that 66 per cent of banks are

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

challenged with 'data quality, gaps in important data points and some transaction flows not being captured at all' (Mosaic, 2024).

Similarly, in support of the above, the 2022 Bank of England's Study indicates that 43 per cent of firms identify data quality and structure issues as significant risks associated with machine learning (Bank of England, 2022). This finding is further supported by studies such as by the Central Banking Staff (2022) and Ramaliba and Jacobs (2024). Therefore, data quality emerges as a cornerstone in the responsible and effective implementation of AI-based FCRM. It is imperative to fully establish rigorous data governance practices, continuous data cleansing, and verification mechanisms to capitalise on AI capabilities.

The requirement for high-quality datasets implies that banks need to invest more in infrastructure, technology, and AI-skilled personnel, alongside dealing with the nuances of data privacy and management to ensure effective compliance with relevant regulatory frameworks such as the Data Protection Act (DPA) 2018 (Rouhollahi, 2021; Sari and Indrabudiman, 2024). Our survey of the thirty-seven respondents from the three major banks shows that respondents are concerned about the lack of AI regulation in the UK together with AI's reliance on large-scale data aggregation and the impact of these on clients' privacy and data protection (Kanamori, et al., 2022). While AI regulations are being formulated, financial institutions in the UK should maintain strict adherence to DPA, General Data Protection Regulation (GDPR) and other international data governance frameworks (European Commission, 2025).

Another challenge is that the risk of algorithmic bias remains high. For instance, if the datasets used to train AI systems have biased elements in favour of high-income earners, such systems are likely to inadvertently perpetuate these biases. This could lead to erroneous FCR assessments and compliance failures. These could result in poor decisions on FCRs, exacerbate systemic inequalities, and erode public trust (Kurshan and Shen, 2020). We also find from our thirty-seven survey respondents that AI systems may reinforce discriminatory biases, disproportionately affecting marginalised demographics (Barocas, Hardt and Narayanan, 2023). Ensuring algorithmic fairness and transparency therefore remains a pressing ethical imperative (Durodola, 2024).

An additional challenge is that, although AI systems can identify complex patterns and anomalies, they are also inclined to produce false positives, which can overwhelm compliance teams, undermining confidence in the overall results (Kan, 2024). This can be attributed to the fast-evolving nature of financial crimes, which requires AI systems to continuously adapt and learn. This adaptive learning requires banks to constantly update their algorithms to keep pace with new fraud tactics that criminals deploy (Odeyemi et al., 2024). The risk of banks to unduly rely on AI to address FCRs is also high. This could lead to complacency among human analysts who may neglect their critical judgement in favour of AI-generated insights (Kanupriya, 2024). Banks' reliance on AI systems in FCRM also raises concerns

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

such as opacity of decision-making processes, which challenges fairness, accountability, and transparency of these systems (Owolabi, 2024).

Furthermore, there is inadequate AI-related skills in banks, which makes effective FCRM challenging. The continued evolvement of AI systems along with limited qualified professionals that are adept in AI-related skills such as machine learning, NLP, data science and financial regulations does hinder the implementation and advancement of AI applications in FCRM (Liu, 2023). This issue is particularly pronounced in small-scale financial institutions that may not have enough resources to attract top talent to develop and maintain sophisticated AI systems related to FCRM. For instance, the sophistication of deepfakes using deep learning does challenge data integrity, requiring highly skilled bank professionals to unravel. Deepfakes refer to the outcome of cloning real-life situations, which are often difficult to be detected even by experts.

As a case in point, criminals used deepfakes to impersonate 'chief financial officer of a multinational firm through a video conference' (Vecchietti, Liyanaarachchi and Viglia, 2025, p. 1) to deceive a finance professional into paying them US$25 million. Unique challenges of deepfakes such as the manipulation of video calls to impersonate clients, production of fake financial documents, and creation of synthetic identity fraud have particularly been critical to the banking sector. Deepfakes compromise data by threatening the accuracy, reliability, authenticity, and consistency of data, which makes it challenging for banks to trust the information they use for FCRM decision-making, even with the help of AI (Vecchietti, Liyanaarachchi and Viglia, 2025).

In the same light, we have gathered from our thirty-seven survey respondents that there is high rate of sophisticated AI-driven financial crime in the UK. Respondents note that malicious actors exploit AI's capabilities for advanced cyber fraud, including deepfake identity fraud, and algorithmic phishing attacks (King et al., 2021). Respondents propose that AI-driven adversarial attacks necessitate continuous system refinement to counter emerging threats. The Bank of England and FCA AI Survey 2024 supports this finding, further highlighting that AI-based disinformation tools such as deepfakes could be used to increase economic uncertainty. Notwithstanding this, AI has the potential to be used to enhance ability of financial institutions to counter threat or malicious actors, such as in the detection 'of cyberthreats by improving the automated identification of malware or illicit finance activity' (Bank of England, 2025).

Additionally, as AI technology continues to evolve and there is no comprehensive AI regulation covering all present and future risks, the evolving regulatory landscape for AI in financial institutions complicates compliance efforts (Buckley, Arner and Zetzsche, 2024). For instance, we find that the absence of comprehensive standardised AI governance protocols in the UK poses challenges for bank employees and their financial institutions seeking regulatory clarity. Overall, in our survey of the

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

thirty-seven bank employees, they agreed strongly that the deployment of AI in banks is challenging.

Despite these challenges, AI provides several opportunities in FCRM (Dwivedi et al., 2021), which can be aligned to sustainable and responsible use of AI. One of the notable opportunities is that AI systems can predict potential vulnerabilities and anticipate fraudulent activities before they occur (Rouhollahi, 2021; Milon, 2024). This enables banks to allocate resources more judiciously and mitigate risks before they materialise. Additionally, AI tools such as machine learning algorithms and deep learning can enable real-time tracking of financial transactions and instantaneously flagging of suspicious activities (Kan, 2024; Kuzmenko et al., 2023). This measure supports banks to better understand risks and approaches that can be used to address such risks. For instance, biometric authentication and advanced encryption using machine learning algorithms bolster security and decrease the likelihood of fraud.

The deployment of AI to automate and streamline compliance operations can enhance the ability of banks to monitor and comply with stringent AML regulations such as in relation to reporting suspicious activities and transactions (Milon, 2024). This is particularly significant because there is increasing scrutiny from regulators on compliance and penalties for violations, which can have huge financial ramifications for the institutions. For instance, in October 2024, TD Bank was fined about US$3.09 billion for AML failures in its USA's operations (KYC360, 2025).

The opportunity to use AI systems in enhancing collaborative approaches to tackling financial and economic crime is also notable. Improving data-sharing mechanisms through AI offers banks the opportunity to foster better cooperation among themselves and regulatory bodies (e.g., LEAs). This enables a more coordinated approach to uncovering cross-border illicit activities (Jamil et al., 2021; Fauzi et al., 2018). Such collaboration could provide financial institutions with a more comprehensive view of potential risks and crime syndicates, which enhances their FCRM and deterrent capabilities.

AI tools can empower banks to respond to several risk factors and economic uncertainties more deftly and adaptively. For instance, advanced (AI-embedded) robotic process automation (RPA) can automate routine banking processes such as compliance checks and transaction monitoring, which can significantly reduce operational costs and potential human error (Nama, Reddy and Pattanayak, 2024; Temelkov, 2023).

AI can be integrated into business intelligence to identify vulnerabilities in banking operations and to prioritise remediation efforts, thereby strengthening risk protection mechanisms in banks such as cybersecurity measures amid increasing threats associated with economic and financial uncertainties. AI integration in FCRM leads to agile organisational structures that could better respond to risks and even sudden economic shifts. Stakeholders will better benefit from a more adaptive approach to FCRM provided by AI systems or tools (Oyeniyi et al., 2024).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

8.5 AI AND FEAT IN FCRM

The integration of AI with FCRM must be approached with a commitment to sustainable and responsible principles such as those encapsulated in the FEAT framework. The thirty-seven survey respondents opine that financial institutions should integrate FEAT principles into AI governance frameworks to ensure equitable, accountable, and transparent AI applications (Bogina et al., 2021). Fairness (F) is a principle that must be upheld in the deployment of AI systems in FCRM. As AI systems that are trained on historical data could inadvertently perpetuate existing inequalities (Owolabi, 2024; Adeyelu, 2024; Kurshan, 2021), banks must implement rigorous testing and validation processes to ensure that AI models do not discriminate against any group or individual.

This includes applying fairness-aware algorithms to regularly audit AI systems to identify and rectify unintended biases in areas such as approving credit or loan pricing, ensuring that there are equitable outcomes in the risk management ecosystem. It also includes engaging with diverse stakeholder teams to incorporate fair AI algorithms in the development and deployment of AI (Ostmann and Dorobantu, 2021; Rizinski et al., 2022; Owolabi, 2024). For instance, fairness-aware algorithm used in IBM's AI Fairness 360 (AIF360) can check for unwanted biases in datasets and machine learning models, and present state-of-the-art algorithms to mitigate such biases (IBM, 2018; Fritz-Morgenthal, Hein and Papenbrock, 2022).

Education (E) also plays a pivotal role in fostering FCRM. Banks must continuously equip their staff with the knowledge and skills to understand the dynamic nuances of AI technologies such as interpretation AI outputs as well as ethical considerations, implications, and limitations of AI in banking and finance (Hasan et al., 2023; Oyewole, 2024). Bank professionals and other stakeholders should remain abreast of emerging trends and best practices in AI and risk management. AI and FCRM education in banks can promote a culture of informed decision-making, thereby enhancing their capacity to leverage AI responsibly and ethically as well as the overall landscape of FCRM (Hasan et al., 2023; Oyewole, 2024). Industry-wide knowledge sharing enhances the collective resilience of financial institutions against AI-enabled financial crime.

Accountability (A) mechanisms are equally essential to ensure that AI systems are used responsibly in FCRM. Banks must establish clear lines of accountability for AI-driven decisions, ensuring that specific individuals or teams are assigned the responsibility of overseeing the implementation of AI (Owolabi, 2024; Adeyelu, 2024). To harness accountability of AI in FCRM, it is crucial to foster a regulatory framework that emphasises the human oversight. While AI can enhance efficiency, it is also fallible and should, thus, be used as a tool to support judgement of bank professionals in FCRM rather than replace it (Adeyelu, 2024; Akinrinola, 2024).

Thus, there should be a human-in-the-loop process established, as exemplified in the Quilt Framework with a robust Senior Managers and Certification Regime

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

(SM&CR). This measure enhances accountability and mitigates risks associated with automated decision-making (Owolabi, 2024; Adeyelu, 2024; Durodola, 2024). In addition, AI models must undergo continuous refinement to address the evolving accountability issues and tactics of financial criminals. Similarly, there should be more investments in explainable AI (XAI) as this will enhance regulatory confidence and institutional accountability.

Such an accountability framework must have protocols for addressing any adverse outcomes from AI decisions (Owolabi, 2024; Adeyelu, 2024). Therefore, it is imperative for banks to implement frameworks that ensure their AI systems are interpretable and that their decision-making processes can be effectively audited regularly (Maree et al., 2020). Regular AI audits and bias assessments should be mainstreamed as they enhance the reliability and fairness of decision-making algorithms. Further, banks should advance practices that facilitate the explainability of AI models. This should be done in such a way that stakeholders can comprehend the rationale behind automated decisions (Maree et al., 2020).

Transparency (T) is also vital in FCRM. Banks should enhance predictive analytics to refine, for instance, credit risk assessment, making it more transparent and reliable for stakeholders involved in decision-making processes (Brown, 2024). With the use of AI-driven analytics, banks can better assess creditworthiness of clients and tailor financial products to underserved populations, thus, promoting financial inclusion (Sari and Indrabudiman, 2024; Kanupriya, 2024).

In the same vein, stakeholders such as clients and regulatory bodies should be able to access clear information regarding how AI systems operate, their performance, impact, and the criteria used in decision-making processes (Maree et al., 2020; Akinrinola, 2024). Banks should, thus, engage in transparent reporting practices to foster a culture of accountability, trust, continuous improvement, and empowerment of users to make informed decisions based on insights generated from AI (Maree et al., 2020; Akinrinola, 2024).

Furthermore, the integration of AI in FCRM necessitates a proactive regulatory approach to ensure that as many risk factors as possible are covered. This requires close collaboration between policymakers, banks, and technology providers to develop and update regulations that foster innovation while safeguarding against potential risks of AI deployment in FCRM (Truby et al., 2020; Ekundayo, 2024). This includes bolstering measures such as standards for AI governance, risk assessment, and data management that promote sustainable and responsible financial practices (Ekundayo, 2024; Zhou, 2023).

Additionally, the ethical deployment of AI in FCRM necessitates a commitment to sustainability. Banks should consider the environmental, social, and governance (ESG) implications of their AI deployment in FCRM, ensuring that the use of AI contributes positively to sustainable development goals (SDGs) (Oyewole, 2024; Lim, 2023). By aligning AI applications with ESG principles, banks can enhance

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

their reputation and build trust with stakeholders, which will lead to a more resilient and sustainable financial ecosystem (Oyewole, 2024; Lim, 2023).

In the nutshell, UK bank employees have increasingly recognised that AI integration is a pivotal change agent in the ecosystem of FCRM, which does provide significant enhancements to operational processes and compliance functions. Employees covered in the selected studies observe that AI can streamline the detection of sophisticated financial crimes such as money laundering and fraud while reducing manual error and reliance on outdated rule-based systems (Balcıoğlu, 2024; Kapate et al., 2025). UK bank employees are actively shaping responsible AI by establishing dedicated governance bodies, embedding ethics into development lifecycles, and upskilling workforces. Across the UK banking sector, staff-driven working groups, Centres of Excellence, and ethics boards are being established as key mechanisms for balancing innovation with the regulatory, operational, and reputational risks of AI. The senior managers of these banks are upbeat about ensuring robust security and safety mechanisms to address FCRs.

These findings underscore the necessity for targeted AI adoption strategies that accommodate varying levels of trust and acceptance among banking employees. Financial institutions should implement AI responsibility and ethics training programmes to bridge the gap in AI literacy and foster confidence in AI's regulatory compliance. Furthermore, inclusive policy development is imperative to ensure gender-equitable discourse on AI ethics and integrate diverse professional perspectives in AI governance (Gebru, 2020). These views do reflect an underlying optimism about the role of AI in not only managing FCRs but also ensuring financial integrity and stability.

8.6 CONCLUSION

AI uses advanced analytics to identify, assess, and mitigate potential threats. Banks are using AI-powered systems to conduct analysis of patterns and behaviours in transaction data, which could be overlooked by humans. With unprecedented capabilities, the AI systems are used in the detection of subtle anomalies, in real time, which could exhibit fraudulent activities. This reduces the incidence of financial loss and enhances consumer trust (Balcıoğlu, 2024; Nguyen et al., 2023). Although there is increasing recognition of the potential for AI to mitigate FCRs by improving 'the accuracy, speed, and cost-effectiveness of AML processes' (Goldbarsht, 2023, p. 61), significant challenges of using AI in FCRM such as data quality, bias, privacy, interpretation, collaboration, big data, liability, and costs persist. These undermine innovations in AML compliance.

Essentially, the sustainable and responsible use of AI in FCRM hinges on a commitment to the ethical and legal principles of FEAT. By harnessing these principles, banks can enhance the transformative potential of AI while mitigating the associated risks and ethical concerns. This approach enhances operational

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

efficiency and decision-making as well as fosters trust among stakeholders and promotes a more equitable and sustainable financial landscape. The integration of AI in FCRM must be guided by a robust ethical framework that prioritises fairness, education, transparency, accountability, and human oversight. By effectively addressing the challenges and harnessing the opportunities of FCRM and AI, banks and related financial institutions can create a more resilient financial ecosystem. As this chapter is the first academic piece that explores AI and FCRM along with the FEAT, future research could explore these elements in a comparative study to enrich the discourse in this area for enhanced financial crime countering and integrity. The future of FCRM hinges on striking a fine balance between leveraging technological advancements and maintaining ethical standards and regulatory compliance.

REFERENCES

Adeyelu O. O., Ugochukwu C. E. and Shonibare M. A. (2024) Ethical implications of ai in financial decision-making: A review with real world applications. *International Journal of Applied Research in Social Sciences*, 6(4), pp.608–630. Available at: https://doi.org/10.51594/ijarss.v6i4.1033 (Accessed: 11 April 2025).

Akinrinola O., et al. (2024) Navigating and reviewing ethical dilemmas in ai development: Strategies for transparency, fairness, and accountability. *GSC Advanced Research and Reviews*, 18(3), pp. 050–058. Available at: https://doi.org/10.30574/gscarr.2024.18.3.0088 (Accessed: 11 April 2025).

Al-Badran O. R. A. (2021) The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal*, 27(6), pp. 1–10.

Arner D. W., Barberis J. N. and Buckley R. P. (2025) The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), pp. 1271–1292.

Arreche O., Guntur T. and Abdallah M. (2024) XAI-IDS: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems. *Applied Sciences*, 14(10), p. 4170.

Aziz L. A. R. and Andriansyah Y. (2023) The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), pp. 110–132. Available at: https://core.ac.uk/download/pdf/578755756.pdf (Accessed: 11 April 2025).

Balcıoğlu Y. S. (2024) Revolutionizing risk management AI and ML innovations in financial stability and fraud detection. In Pandow, B. A., Masoodi, F. S., Iqbal, J. and Hussain, G. (Eds.) *Navigating the Future of Finance in the Age of AI*. Hershey, PA: IGI Global, pp. 109–138.

Bank of England (2022) Machine learning in UK financial services. 11 October. Available at: www.bankofengland.co.uk/Report/2022/machine-learning-in-uk-financial-services?utm_source=chatgpt.coms (Accessed: 11 April 2025).

Bank of England (2024) Resolvability Assessment of Major UK Banks: 2024 (Bank of England, 6 August 2024). Available at: www.bankofengland.co.uk/financial-stability/resolution/resolvability-assessment-framework/resovability-assessment-of-major-uk-banks-2024 (Accessed: 11 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Bank of England (2025) Financial Stability in Focus: Artificial intelligence in the financial system. Available at: www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025 (Accessed: 11 April 2025).

Bank of England and FCA (2024) Artificial intelligence in UK financial services – 2024. Available at: www.bankofengland.co.uk/financial-stability/resolution/resolvability-assessment-framework/resovability-assessment-of-major-uk-banks-2024 (Accessed: 11 April 2025).

Barclays (2024) From intelligence to ability: how Barclays is harnessing AI. Available at: https://home.barclays/news/2024/01/how-Barclays-is-harnessing-AI/ (Accessed: 11 April 2025).

Barocas S., Hardt M. and Narayanan A. (2023) *Fairness and Machine Learning: Limitations and Opportunities*, vol. 1, 1st ed., Cambridge, MA: MIT Press.

Bogina V. et al. (2021) Educating software and AI stakeholders about algorithmic fairness, accountability, transparency and ethics. *International Journal of Artificial Intelligence in Education*, 32. Available at: https://doi.org/10.1007/s40593-021-00248-0 (Accessed: 11 April 2025).

Brown M. (2024) Influence of artificial intelligence on credit risk assessment in banking sector. *International Journal of Modern Risk Management*, 2(1), pp. 24–33. Available at: https://doi.org/10.47604/ijmrm.2641 (Accessed 11 April 2025).

Buckley P. R., Arner W. D. and Zetzsche A. D. (2024) *FinTech: Finance, Technology and Regulation – Introduction*, vol. 1, 1st ed. Cambridge: Cambridge University Press. Available at: https://doi.org/10.2139/ssrn.448605 (Accessed: 23 March 2025).

Calvery J. (2024) Harnessing the power of AI to fight financial crime. Available at: www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime#:~:text=AI%20has%20helped%20us%20to,weeks%20to%20a%20few%20days (Accessed: 11 April 2025).

Central Banking Staff (2022) Data quality and staff skills are greatest AI challenges – benchmark respondents. Benchmarking, 24 February. Available at: www.centralbanking.com/benchmarking/fintech/7932271/data-quality-and-staff-skills-are-greatest-ai-challenges-benchmark-respondents?utm_source=chatgpt.com (Accessed: 11 April 2025).

Chaudhary P. S., Khurana M. R. and Ayalasomayajula M. (2024) Real-world applications of data analytics, big data, and machine learning. In: Singh P. Mishra, A.R. and Garg, P. (eds). *Data Analytics and Machine Learning: Navigating the Big Data Landscape*. Studies in Big Data, vol. 145. Singapore: Springer, pp. 237–263. Available at: https://link.springer.com/chapter/10.1007/978-981-97-0448-4_12 (Accessed: 11 April 2025).

Cheng D., et al. (2025) Graph neural networks for financial fraud detection: A review. *Frontiers of Computer Science*, 19, Article 199609.

Chowdhary K. R. (2020) . *Fundamentals of Artificial Intelligence*. New Delhi: Springer pp. 1–23. Available at: https://doi.org/10.1007/978-81-322-3972-7_1 (Accessed: 11 April 2025).

Dafoe A. (2024) AI governance: Overview and theoretical lenses. In: Bullock J. B. et al., eds. *The Oxford Handbook of AI Governance*. (online) Oxford Academic. Available at: https://doi.org/10.1093/oxfordhb/9780197579329.013.2 (Accessed: 23 March 2025).

De Silva C. (2025) Advancing Financial Risk Management: AI-Powered Credit Risk Assessment through Financial Feature Analysis and Human-Centric Decision-Making. *MDPI AG*. Available at: https://doi.org/10.20944/preprints202502.2059.v1 (Accessed: 23 March 2025).

Devarajulu V. S. (2022) Expert take on AI-augmented cybersecurity measures in financial institutions. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 1(3), pp. 1220–1222.

Doddipatla L. (2024) Ethical and regulatory challenges of using generative AI in banking: Balancing innovation and compliance. *Educational Administration: Theory and Practice*, 30, p. 2848.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Durodola L. O. (2021) Towards a responsible use of artificial intelligence. In Lui A. and Ryder N., eds. *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention* 1st ed. London: Routledge. Available at: https://doi.org/10.4324/9781003020998 (Accessed: 12 March 2025).

Durodola O. (2024) Artificial Intelligence in Global Financial Institutions Based in the United Kingdom: Ethico-Legal, Corporate Governance and Social Responsibility Perspectives. PhD Thesis.

Dwivedi K. Y. et al. (2021) Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy. *International Journal of Information Management*, 57, 101994. Available at: https://doi.org/10.1016/j.ijinfomgt.2019.08.002 (Accessed: 11 April 2025).

Ekundayo F. (2024) Economic implications of ai-driven financial markets: Challenges and opportunities in big data integration. *International Journal of Science and Research Archive*, 13(02), pp. 1500–1515. Available at: https://doi.org/10.30574/ijsra.2024.13.2.2311 (Accessed: 11 April 2025).

El Hajj M. and Hammoud J. (2023) Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. *Journal of Risk and Financial Management*, 16, p.434.

European Commission (2025) Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act. (*Shaping Europe's digital future*, 4 February 2025). Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (Accessed: 23 March 2025).

Fauzi F., Szulczyk K. and Basyith A. (2018) Moving in the right direction to fight financial crime: Prevention and detection. *Journal of Financial Crime*, 25(2), pp. 362–368. Available at: https://doi.org/10.1108/JFC-06-2017-0060 (Accessed: 11 April 2025).

FCA (2022) PS22/9: A new Consumer Duty. Available at: www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty (Accessed: 11 April 2025).

FCA (2025) Financial Crime Guide: A firm's guide to countering financial crime risks (FCG), April 2025. Available at: www.handbook.fca.org.uk/handbook/FCG.pdf (Accessed:25 April 2025).

Fritz-Morgenthal S., Hein B. and Papenbrock J. (2022) Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in Artificial Intelligence*, 5. Available at: https://doi.org/10.3389/frai.2022.779799 (Accessed: 11 April 2025).

Garud S. (2025) AI-driven risk management in financial services from theory to practice in smart education. In Sorayyaei Azar, A., Gupta, S.K., Al Bataineh, K.B., Maurya, N. and Somani, P. (eds.) *Smart Education and Sustainable Learning Environments in Smart Cities*. Hershey, PA: IGI Global Scientific Publishing, pp. 77–92.

Gebru T. (2020) Race and gender. In Dubber M. D., Pasquale F. and Das S., eds. *The Oxford Handbook of Ethics of AI* (online ed.) Oxford Academic, 9 July. Available at: https://doi.org/10.1093/oxfordhb/9780190067397.013.16 (Accessed: 23 March 2025).

Goldbarsht D. (2023) Leveraging AI to mitigate money laundering risks in the banking system. In Bednarz Z. and Zalnieriute M., eds. *Money, Power, and AI: Automated Banks and Automated States*. Cambridge: Cambridge University Press, pp. 51–69.

Hasan Z. et al. (2023) Can artificial intelligence (AI) manage behavioural biases among financial planners? *Journal of Global Information Management*, 31(2), pp. 1–18. Available at: https://doi.org/10.4018/jgim.321728 (Accessed 11 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Hilal W., Gadsden S. A. and Yawney J. (2022) Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, p. 116429.

HSBC (n.d.) Fighting financial crime. Available at: www.hsbc.com/who-we-are/esg-and-responsible-business/fighting-financial-crime (Accessed: 25 April 2025).

Hua S. S. and Belfield H. (2023) Effective Enforceability of EU Competition Law Under AI Development Scenarios. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*. *ACM*. Available at: https://doi.org/10.1145/3600211.3604694 (Accessed: 23 March 2025).

Huang J. and Kisgen J. D. (2013) Gender and corporate finance: Are male executives overconfident relative to female executives? *Journal of Financial Economics*, 108(3), p. 822.

IBM (2018) Introducing AI Fairness 360. Available at: https://research.ibm.com/blog/ai-fairness-360 (Accessed: 11 April 2025).

Jamil A. H. et al. (2021) The covid-19 impact on financial crime and regulatory compliance in Malaysia. *Journal of Financial Crime*, 29(2), pp. 491–505. Available at: https://doi.org/10.1108/jfc-05-2021-0107 (Accessed: 11 April 2025).

Jofre M., Bosisio A. and Riccardi M. (2024) Financial crime risk assessment: Machine learning insights into ownership structures in secrecy firms. *Global Crime*, 25(3-4), p. 242.

Kan Y. (2024) The impact of AI on the development of manufacturing, logistics, and financial company from capital market perspectives. *Advances in Economics, Management and Political Sciences*, 115, pp. 120–125. Available at: www.ewadirect.com/proceedings/aemps/article/view/16973 (Accessed: 11 April 2025).

Kanamori S. et al. (2022) Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks. *Journal of Information Processing*, 30, p. 789.

Kanupriya (2024) Opportunities and challenges of AI in financial risk management: A brief labour-centric analysis. *Forum for Economic and Financial Studies*, 2(2), 1758. Available at: https://ojs.acad-pub.com/index.php/FEFS/article/view/1758 (Accessed: 11 April 2025).

King C. T. et al. (2021) Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. In Floridi L., ed. *Ethics, Governance and Policies in Artificial Intelligence. Philosophical Studies Series*, vol 144. pp. 251–282. Cham: Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-81907-1_13 (Accessed: 23 March 2025).

Kishore S. S. (2025) AI in risk management in finance. In Derbali, A.M.S. (eds) *Artificial Intelligence for Financial Risk Management and Analysis*. Hershey, PA:IGI Global Scientific Publishing, pp. 471–498.

Kothinti K. G. (2025) AI-powered identity verification & risk analysis: The future of fraud prevention in financial services. *European Journal of Computer Science and Information Technology*, 13(9), pp. 23–55.

Kurshan E. and Shen H. (2020) Graph computing for financial crime and fraud detection: Trends, challenges and outlook. *International Journal of Semantic Computing*, 14(04), pp. 565–589. Available at: www.worldscientific.com/doi/abs/10.1142/S1793351X20300022 (Accessed: 11 April 2025).

Kurshan E. et al. (2021) On the current and emerging challenges of developing fair and ethical AI solutions in financial services. *Proceedings of the Second ACM International Conference on AI in Finance*. *ACM*. Available at: https://doi.org/10.1145/3490354.3494408 (Accessed: 23 March 2025).

Kuzmenko O., Yarovenko H. and Perkhun L. (2023) Assessing the maturity of the current global system for combating financial and cyber fraud. *Statistics in Transition New Series*, 24(1), pp. 229–258. Available at: https://doi.org/10.59170/stattrans-2023-013 (Accessed: 11 April 2025).

KYC360 (2025) TD Bank AML Failures What Went Wrong?. *KYC360*. Available at: https://bit.ly/3QK7R7O (Accessed: 11 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Lim T. (2023) Environmental, social, and governance (ESG) and artificial intelligence in finance: State-of-the-art and research takeaways. *Research Square*, pp. 1–45. Available at: https://doi.org/10.21203/rs.3.rs-2849051/v1 (Accessed: 11 April 2025).

Liu X. (2023) New characteristics of AI analysis of financial risks and their transmission traceability paths. *International Journal of Big Data Intelligent Technology*, 4(1). Available at: https://doi.org/10.38007/ijbdit.2023.040105 (Accessed: 11 April 2025).

Lloyds Banking Group (2025) Lloyds Banking Group bolsters AI capabilities by appointing Head of Responsible AI. Available at: www.lloydsbankinggroup.com/media/press-releases/2025/lloyds-banking-group-2025/lloyds-banking-group-bolsters-ai-capabilities-by-appointing-head.html?utm_source=chatgpt.com (Accessed: 11 April 2025).

Mahadevkar S. V. et al. (2024) Exploring AI-driven approaches for unstructured document analysis and future horizons. *Journal of Big Data*, 11, p. 92.

Marcus A. and Hargrave T. (2021) The role of stakeholders in ethical decision-making. In: *Managing Business Ethics: Making Ethical Decisions*. Thousand Oaks, CA: SAGE Publications, Inc. pp. 242–275. Available at: https://doi.org/10.4135/9781506388625.n8 (Accessed: 23 March 2025).

Maree C., Modal E. J. and Omlin W. C. (2020) Towards responsible ai for financial transactions. *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 16–21. Available at: https://doi.org/10.1109/ssci47803.2020.9308456 (Accessed: 11 April 2025).

Mastercard (2024) Mastercard transforms the fight against scams with latest AI tech. Available at: www.mastercard.com/news/press/2024/april/mastercard-transforms-the-fight-against-scams-with-latest-ai-tech/#:~:text=They%20just%20need%20to%20trick,them%20before%20money%20is%20lost. (Accessed: 11 April 2025).

Milojević N. and Redzepagic S. (2021) Prospects of artificial intelligence and machine learning application in banking risk management. *Journal of Central Banking Theory and Practice*, 10(3), pp. 41–57.

Milon M. N. U. (2024) Gravitating towards artificial intelligence on anti-money laundering a PRISMA based systematic review. *International Journal of Religion*, 5(7), pp. 303–315. Available at: https://doi.org/10.61707/py0fe669 (Accessed: 11 April 2025).

Mittelstadt B. D. et al. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). Available at: https://doi.org/10.1177/2053951716679679 (Accessed: 11 April 2025).

Mohan M. B. R. (2024) AI in fraud detection: Evaluating the efficacy of artificial intelligence in preventing financial misconduct. *Journal of Electrical Systems*, 20(3s), pp. 1332–1338. Available at: https://doi.org/10.52783/jes.1508 (Accessed: 11 April 2025).

Mosaic (2024) *Research reveals two thirds of banks struggle with data quality and integrity*. London, 29 January 2024. Available at: https://mosaicsmartdata.com/research-reveals-two-thirds-of-banks-struggle-with-data-quality-and-integrity/?utm_source=chatgpt.com (Accessed: 11 April 2025).

Nagaraj C. T., Anand M. C. J., Priyadharshini S. S. and Aparna P. (2024) 'GCNXG: Detecting Fraudulent Activities in Financial Networks: A Graph Analytics and Machine Learning Fusion', in Gundebommu, S.L., Sadasivuni, L. and Malladi, L.S. (eds.) *Renewable Energy, Green Computing, and Sustainable Development. REGS 2023. Communications in Computer and Information Science*, vol. 2081. Cham: Springer. pp. 17–32. Available at: https://doi.org/10.1007/978-3-031-58607-1_2 (Accessed: 11 April 2025).

Nama P., Reddy P. and Pattanayak K. S. (2024) Artificial intelligence for self-healing automation testing frameworks: Real-Time Fault Prediction and Recovery. *Cineforum*, 64(3S), p.111.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Narajala V. S. and Narayan O. (2025) Securing agentic AI: A comprehensive threat model and mitigation framework for generative AI agents. *arXiv preprint arXiv:2504.19956*. Available at: https://doi.org/10.48550/arXiv.2504.19956 (Accessed: 11 April 2025).

NatWest Group (2025) Innovation and digitalisation. Available at: www.natwestgroup.com/sustainability/society/innovation-and-digitisation.html (Accessed: 11 April 2025).

Nguyen D. K., Sermpinis G. and Stasinakis C. (2023) Big data, artificial intelligence and machine learning: A transformative symbiosis in favour of financial technology. *European Financial Management*, 29(2), pp. 517–548.

Odeyemi O. et al. (2024) Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, 11(01), pp. 2101–2110. Available at: https://ijsra.net/content/reviewing-role-ai-fraud-detection-and-prevention-financial-services (Accessed: 11 April 2025).

Olowu O. et al. (2024) AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *GSC Advanced Research and Reviews*, 21(02), pp. 227–237.

Ostmann F. and Dorobantu C. (2021) AI in financial services. *Alan Turing Institute*. Available at: www.turing.ac.uk/sites/default/files/2021-06/ati_ai_in_financial_services_lores.pdf (Accessed: 11 April 2025).

Owolabi O. S. et al. (2024) Ethical implication of artificial intelligence (AI) adoption in financial decision making. *Computer and Information Science*, 17(1), p. 49. Available at: https://doi.org/10.5539/cis.v17n1p49 (Accessed: 11 April 2025).

Oyeniyi L. D., Ugochukwu C. E. and Mhlongo N. Z. (2024) Implementing AI in banking customer service: a review of current trends and future applications. *International Journal of Science and Research Archive*, 11(2), pp. 1492–1509. Available at: https://doi.org/10.30574/ijsra.2024.11.2.0639 (Accessed: 11 April 2025).

Oyewole A. T. et al. (2024) Promoting sustainability in finance with AI: A review of current practices and future potential. *World Journal of Advanced Research and Reviews*, 21(3), pp. 590–607. Available at: https://doi.org/10.30574/wjarr.2024.21.3.0691 (Accessed: 11 April 2025).

Pavlidis G. (2023) Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), pp. 155–166.

Ramaliba T. and Jacobs L. (2024) Artificial intelligence technology to enhance data quality management practices in the banking industry in South Africa. *SA Jnl Libs & Info Sci*, 90(2). Available at: https://journals.co.za/doi/10.7553/90-2-2392?utm_source=chatgpt.com (Accessed: 11 April 2025).

Rashid A. B. and Kausik A. K. (2024) AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, 7, p. 100277.

Rizinski M. et al. (2022) Ethically responsible machine learning in fintech. *IEEE Access*, 10, pp. 97531–97554. Available at: https://doi.org/10.1109/access.2022.3202889 (Accessed: 11 April 2025).

Rouhollahi Z. (2021) Towards Artificial Intelligence Enabled Financial Crime Detection. Available at: https://arxiv.org/abs/2105.10866v1 (Accessed: 11 April 2025).

Salem A. H. et al. (2024) Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 11, article number 105.

Sari Y. and Indrabudiman A. (2024) The role of artificial intelligence (AI) in financial risk management. *Formosa Journal of Sustainable Research*, 3(9), pp. 2073–2082. Available at: https://doi.org/10.55927/fjsr.v3i9.11436 (Accessed: 11 April 2025).

Sarker I. H. (2021) Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2, p. 160.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Temelkov Z. (2023) Overview of artificial intelligence (AI) application in the banking industry. *International Journal of Economics, Management and Tourism*, 3(2), pp. 43–51. Available at: https://doi.org/10.46763/ijemt23320043t (Accessed:11 April 2025).

Truby J., Brown R. D. and Dahdal A. (2020) Banking on AI: Mandating a proactive approach to ai regulation in the financial sector. *Law and Financial Markets Review*, 14(2), pp. 110–120. Available at: https://doi.org/10.1080/17521440.2020.1760454 (Accessed:11 April 2025).

Tsapa J. A. (2023) Artificial intelligence use cases for banking anti-money laundering. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 1, p. 259.

Vecchietti G., Liyanaarachchi G. and Viglia G. (2025) Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research*, 186, 115010. Available at: https://doi.org/10.1016/j.jbusres.2024.115010 (Accessed: 11 April 2025).

Wang S. X. (2024) The application of artificial intelligence-based risk management models in financial markets. *Open Journal of Social Sciences*, 12, pp. 274–284.

Wang Y. et al. (2024) Quantum computing in community detection for anti-fraud applications. *Entropy*, 26(12), p. 1026.

West J. and Bhattacharya M. (2016) Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, pp. 47–66.

Zhang C. J. et al. (2025) AI-based identity fraud detection: A systematic review. Available at: https://doi.org/10.48550/arXiv.2501.09239 (Accessed: 17 April 2026).

Zhou X. (2023) Challenges and countermeasures of artificial intelligence technology in the application of financial industry. *Advances in Economics, Management and Political Sciences*, 63(1), pp. 77–82. Available at: https://doi.org/10.54254/2754-1169/63/20231382 (Accessed: 11 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

9

Leveraging Artificial Intelligence in Citizenship by Investment Programmes: A Framework for Minimum Due Diligence Standards to Counter Financial Crime

Jeiel Joseph, Lucas Millan-Narotzky, and Umut Turksen

9.1 INTRODUCTION

Investment migration (IM) programmes are broadly classified into two main categories: Citizenship by Investment (CBI), which this chapter covers, and Residence by Investment (RBI). These programmes allow foreign nationals to acquire legal status in a country in exchange for financial contributions (European Commission, 2023). However, they differ fundamentally in terms of legal rights, eligibility requirements, and pathways to full citizenship. CBI programmes grant direct citizenship to investors and their families without requiring long-term residence. Typically, applicants must make substantial economic contributions, such as donations to national development funds, investment in government-approved real estate, or contributions to business ventures. These programmes are sometimes referred to as 'economic citizenship' or 'golden passport' schemes. For example, St Kitts and Nevis established the first CBI programme in 1984 and today requires a minimum investment of USD 250,000 in their Sustainable Growth Fund (Government of St Kitts and Nevis, 2023).

In the European Union (EU) Malta established the Individual Investor Programme (IIP) (Government of Malta, 2023), which attracted scrutiny over potential abuses, including money laundering and granting citizenship to individuals with minimal ties to Malta. Investigative reports, such as the 'Passport Papers', highlighted these concerns (The Guardian, 2025). On 29 April 2025, the European Court of Justice (ECJ) ruled that Malta's IIP contravenes EU law as it commodified EU citizenship, undermining principles of sincere cooperation and mutual trust among Member States. The ruling mandates Malta to terminate the scheme, aligning its citizenship laws with EU principles (Starcevic, 2025).

One of the main criticisms of CBI programmes is that they bypass the core requirements traditionally associated with acquiring citizenship (Surak, 2021). Unlike conventional pathways based on birthright (*jus soli*) or descent (*jus sanguinis*), which typically demand physical residence, language proficiency, cultural integration, and lengthy waiting periods, CBI schemes offer citizenship within

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

months without these obligations. This has raised concerns that CBI undermines the integrity and value of citizenship by reducing it to a transactional process rather than a reflection of genuine national belonging, an assessment supported by the EU (European Commission, 2019) and evidenced by the recommended termination of Malta's IIP.

The demand for CBI programmes has nevertheless surged, particularly among individuals from politically unstable regions or those seeking greater global mobility (CS Global Partners, 2025). For instance, following significant political events, there has been a notable increase in inquiries from United States of America citizens about such programmes (Ahmad, 2024). However, this growing popularity has led to concerns about the integrity of these programmes and the potential or perceived financial crime risks they may pose.

As commented on in Chapter 8: The Use of AI by Banks in Financial Crime Risk Management, banks and financial institutions have increasingly turned to AI technologies, such as Machine Learning to enhance risk detection, improve due diligence (DD), and ensure compliance with international regulatory standards. These advancements provide a valuable blueprint for integrating AI-driven compliance mechanisms within the CBI industry to detect fraudulent applications, assess Illicit Financial Flows (IFFs), and enhance transparency, efficiency, and accountability.

This chapter builds upon the insights from Chapter 8 by applying AI-driven risk management frameworks to the CBI context. It first critically examines the current regulation of CBI, then, DD in CBI including its administration, focusing on money laundering and tax compliance. Accordingly, with the introduction of AI tools, legal and ethical issues in the use of AI in CBI must be evaluated, and its operationalisation can be considered thereafter. Ultimately, this chapter provides an analysis of how AI can be leveraged to ensure minimum DD standards so as to mitigate money laundering and tax compliance risks while upholding ethical principles in CBI programmes.

9.2 REGULATION OF CBI

The regulation of CBI programmes operates at the intersection of national sovereignty driven immigration laws, economic targets, and global financial governance. These are also shaped by the general minimum standards established by international organisations such as the Organisation for Economic Co-operation and Development (OECD) (OECD, 2018b) and the Financial Action Task Force (FATF) (FATF, 2022). While states retain the authority to grant citizenship, international pressure has necessitated stricter DD, transparency, and compliance measures to prevent the misuse of CBI schemes for money laundering and tax evasion. The OECD's Common Reporting Standard (CRS) seeks to close loopholes in tax residency declarations by requiring automatic exchange of financial information,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

compelling financial institutions to conduct enhanced DD (EDD) on CBI applicants (OECD, 2023b).

Simultaneously, the FATF's anti-money laundering (AML) framework mandates that jurisdictions implement risk-based vetting procedures, including source-of-funds verification, applicant background screening, and alignment with international sanctions lists (FATF, 2022). Non-compliance with these standards can result in grey listing or blacklisting, restricting a country's access to the global financial system (OECD, 2018b). As a result, many CBI jurisdictions have introduced stricter vetting protocols, enhanced transparency measures, and legal provisions for revoking fraudulently acquired citizenships (Joseph and Turksen, 2022). However, tensions persist between economic incentives for IM and regulatory obligations, reflecting broader debates on the limits of national discretion in citizenship law within an increasingly interconnected financial and security landscape. Aligning CBI programmes with OECD and FATF standards, arguably leads to stronger due diligence, higher transparency, and global legitimacy.

It is suggested by the authors that the regulation of CBI programmes by international organisations such as the OECD and the FATF can be examined through theoretical frameworks in global governance, financial regulation, and transnational law. These organisations play a pivotal role in shaping DD standards. The FATF and OECD recommend that countries implement multi-layered and risk-based DD processes, enhance the transparency of programme operations, and establish clear accountability mechanisms (OECD, 2018b). They also stress the importance of international cooperation to prevent the exploitation of CBI programmes by illicit actors (OECD, 2018b).

The OECD sets out recommendations, influencing states to adopt tax transparency measures through norm diffusion and policy harmonisation (Abbott and Snidal, 2000), while the FATF functions as a transnational regulatory network, coordinating state policies on AML and counter-terrorist financing (CTF). Within the context of CBI, the OECD's governance mechanisms align with theories of international regulatory cooperation, wherein global institutions impose regulatory expectations on states without legally binding enforcement (Abbott and Snidal, 2000). Whereas the FATF exerts influence through its mutual evaluation, blacklisting and grey listing mechanisms, pressuring jurisdictions with weak AML enforcement to reform their financial and legal structures (FATF, 2022).

The OECD recommends that CBI jurisdictions implement stricter DD measures, including requiring physical presence for tax residency certification, enforcing automatic exchange of information (AEOI), and conducting rigorous background checks to ensure a genuine connection between applicants and the host country (OECD, 2018b). Similarly, the FATF has raised concerns about the role of CBI schemes as potential conduits for IFFs, particularly in jurisdictions with weak regulatory frameworks (FATF, 2022). FATF urges Member States to conduct comprehensive background checks, verify the source of funds, and implement 'Know Your Customer'

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

(KYC) standards to enhance transparency and security. Further, applicants should be screened against international watchlists, such as Interpol and UN sanctions databases, to prevent individuals with criminal ties from exploiting IM programmes.

9.3 DD IN CBI

DD plays a crucial role in the CBI application process by identifying and mitigating risks related to IFFs, including money laundering and tax compliance. In the context of AML and CFT, DD aligns with the regulatory requirements imposed on obliged entities, such as banks and financial institutions. The development of DD in CBI programmes is shaped by the balance between state control and international regulations. Initially, countries had full freedom to grant citizenship to investors as a way to boost their economies (Keohane, 1984). However, as concerns over money laundering and security risks grew, international organisations such as the EU, OECD and FATF pushed for stricter regulations (Shachar, 2017). However, the increasing entanglement of financial mobility with global security risks has necessitated a shift towards regulatory convergence (Drezner, 2001).

The OECD's tax governance framework and FATF's AML measures exemplify this shift, embedding CBI DD within a broader risk-based regulatory paradigm. Current CBI DD mechanisms reflect a networked model of compliance, where states implement enhanced vetting procedures, financial transparency standards, and post-citizenship monitoring under the implicit supervision of international financial institutions (OECD, 2018b). This reflects principal-agent dynamics, wherein CBI states, as agents, comply with regulatory expectations set by global financial authorities (principals) to avoid reputational and economic penalties (Jensen and Meckling, 1976).

Nevertheless, tensions persist between market-driven citizenship policies and external regulatory demands, raising questions about the future trajectory of investment migration governance within an increasingly securitised global order (Strange, 1996). The misuse of CBI programmes for IFFs often involves complex and sophisticated mechanisms that obscure the origins and movement of illicit funds. Moreover, the FATF has emphasised that these programmes may facilitate increased global mobility for criminals and allow them to conceal their identities and illicit activities (FATF, 2022). In response, CBI programmes have established robust, multi-tiered DD frameworks to ensure the integrity and security of their offerings. These processes are designed to meticulously screen applicants, thereby safeguarding national interests and maintaining the credibility of the programmes.

9.3.1 *Administration of DD in CBI*

The administration of due diligence in CBIs is conducted by various entities including licensed agents, state-controlled Citizenship by Investment Units (CIUs),

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Financial Intelligence Units (FIUs), and third-party due diligence service providers. Licensed agents play a pivotal role in the preliminary evaluation of applicants at the onboarding stage. They liaise with the applicant, conduct comprehensive initial screenings, verifying personal documents such as identity papers, proof of income, and financial statements. This approach aims to ensure that only candidates who meet the stringent criteria proceed to the next stage.

CIUs implement a hierarchical risk-based framework and conduct customer due diligence (CDD) on applicants. They are supported with financial intelligence provided by FIUs. FIUs are mainly responsible for gathering, analysing, and disseminating financial intelligence, which aids CIUs in identifying and screening high-risk applicants. FIUs and CIUs play a crucial role in mitigating AML/CFT and tax reporting compliance risks. According to the FATF, these collaborative efforts are essential in ensuring compliance with international standards to prevent the misuse of CBI programmes (FATF, 2012). It can be argued that the effective sharing of information between FIUs and CIUs, facilitated by AI tools for the administration of CDD, can ensure that individuals seeking citizenship are thoroughly vetted and that any illicit activities are detected early in the process.

Enhanced DD (EDD) is administered when CIUs engage independent third-party firms to perform in-depth background checks on applicants who are deemed high risk after CDD is performed. Outsourcing EDD obligations encourages CIUs to delegate certain EDD AML functions to third-party service providers while maintaining ultimate responsibility for compliance. EDD encompasses a more thorough and in-depth background check of biometrics, family background, financial history, source of funds, political exposure, and criminal records, ensuring a comprehensive assessment and verification of information provided from applicants. This multi-layered approach underscores the programme's commitment to thoroughness and integrity (Joseph and Turksen, 2022).

A key component of CBI DD is the identification of ultimate beneficial ownership (BO) assets owned by applicants. Obliged entities are required to establish and maintain written procedures to identify and verify these individuals and their assets. This practice prevents malfeasant applicants from misusing companies to disguise their illicit activities and launder their criminal assets via CBI programmes (Complete Professional Services, 2016). Accessing public repositories of BO data, such as the UK Companies House (Companies House, 2023), bank account information and the EU's Beneficial Ownership Registers (Court of Justice of the European Union, 2022), enables CIUs and third-party service providers to verify applicant legitimacy. Additionally, paid services like Orbis (Bureau van Dijk) (Moody's, 2025), Dun & Bradstreet (Dun & Bradstreet, 2011), Sayari (Sayari, 2025), and LexisNexis (LexisNexis, n.d.) offer comprehensive company structure data, aiding in the identification of complex corporate networks and hidden ownership structures.

Compliance with these standards involves reporting suspicious activities and maintaining records to demonstrate adherence to legal requirements (Kenton,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

2024). Non-compliance with international standards can result in significant penalties and reputational damage for a CBI practicing country and its citizens (OECD, 2023b). For instance, banks may refuse services to CBI passport holders due to perceived risks of money laundering even when no wrongdoing has occurred, leading to further banking and regulatory challenges for their *jus soli* and *jus sanguinis* citizens. By implementing rigorous DD protocols, agents, CIUs, and governments can ensure that only individuals of reputable standing are granted citizenship.

In summary, the structured and thorough DD processes in CBI programmes reflect a strong commitment to security, integrity, and international compliance, thereby offering a secure pathway for qualified investors to obtain citizenship. The analysis of the CBIs reveals how current DD processes are typically multi-tiered and facilitated by the CIU using a hierarchical framework (Joseph, 2021). The DD *modus operandi* operates as shown in Table 9.1, but is not standardised across programmes.

The eventual standardisation of DD processes across various CBI programmes provides a solid foundation for establishing AI-facilitated minimum standards for all involved stakeholders. The European Parliament has highlighted the need for comprehensive security checks and DD in CBI schemes, noting that Member States must have adequate vetting processes and should not solely rely on intermediaries (third-party service providers) (Sophia, 2022). There are no publications illustrating that this is currently being maintained across all CBI practicing countries considered in this chapter.

Nevertheless, the OECD's *DD Guidance for Responsible Business Conduct* offers practical support for implementing responsible business practices, providing clear explanations of DD recommendations and associated provisions (OECD, 2023c). Geographic risk is a critical factor in assessing exposure to financial crime. Financial institutions must carefully evaluate jurisdictions, not limited to CBI, with weak AML/CFT frameworks, particularly those flagged by the FATF as high-risk or under increased monitoring. Moreover, countries viewed as having high levels of corruption, as indicated by Transparency International's Corruption Perceptions Index, pose additional financial crime risks (Transparency International, 2023).

9.3.2 *Anti-money Laundering Compliance*

As financial crimes increasingly transcend national borders, international organisations such as the EU, FATF, and OECD have established international standards designed to combat money laundering and terrorist financing. These standards require states to harmonise AML/CFT practices (FATF, 2012; OECD, 2023b).

The FATF 40 Recommendations emphasise transparency and BO disclosure, particularly in contexts like investment migration schemes where anonymity and asset mobility can be exploited for illicit purposes (FATF, 2022; OECD, 2018b).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

TABLE 9.1 *CBI DD process*

Stages	Process	Actor	Actions
Stage 1	KYC processes and initial screening	Agent	• Confirm applicants' identity • Search databases for instances of sanctions or presence on international criminal watchlists • Initial assessment of the applicants' source of funds
Application submitted to government			
Stage 2	International and National Intelligence and law enforcement	Government CIU	Searching domestic intelligence, foreign partners' intelligence, local law enforcement. • National databases • Outstanding warrants • Suspicion of international criminal activity • Check for criminal record • Check for failed visa applications and reasons for rejection. • Checking with Interpol and other agencies for information on the applicant.
	DD from third-party provider	Third-party DD providers	Searching international intelligence, personal interviews, online databases and physical archive access: • Searches of litigation records; PEP/political exposure; regulatory issues • Checks on trustworthiness and reputation • Adverse media assessment • Validation of primary documents • Checks on disclosed and non-disclosed businesses.
Applicant risk profile created			
Stage 3	Creation of risk assessment		Government CIU

Nonetheless, the practical implementation of these standards is often complicated by the reliance on private intermediaries. Many CBI and RBI programmes outsource due diligence processes to third-party agents or firms, which introduces substantial regulatory ambiguity. These agents may operate under varying levels of scrutiny and with differing standards of compliance, thereby generating inconsistencies in risk assessment and exposure to reputational and financial harm (Joseph and Turksen, 2022).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

In light of these minimum international standards, the EU enacted the Sixth Anti-Money Laundering Directive (AMLD6) (Directive (EU) 2018/1673), which outlines stringent due diligence requirements for obliged entities, particularly in contexts involving high-risk third-country nationals seeking citizenship or residency via financial contributions. Articles 18a to 24 of the Directive establish the necessity for EDD, obligating financial institutions to implement robust KYC mechanisms and report suspicious transactions that may indicate IFFs, especially in sectors vulnerable to abuse such as luxury real estate, shell companies, and cross-border capital movements (European Commission, 2023; FATF, 2022).

The EU AMLD6 attempts to mitigate inconsistent approaches to risk assessment by expanding the scope of due diligence obligations to include non-EU-based entities engaging with EU markets. Notably, Articles 3(3)(l) and 18 of the AMLR6 impose compliance duties on foreign legal professionals, real estate agents, and service providers involved in high-risk transactions or schemes with an EU nexus (European Commission, 2021). However, the enforcement of these provisions remains fragmented. Diverging jurisdictional mandates, coupled with limited cross-border supervisory cooperation, have led to regulatory arbitrage where high-risk individuals strategically exploit legal loopholes and weak oversight in certain jurisdictions to secure residency or citizenship under opaque conditions (Shachar, 2017; OECD, 2023b). This problem is exacerbated by disparities in national enforcement capacities and the voluntary nature of FATF compliance, which renders some states more vulnerable to becoming safe havens for illicit financial actors (Strange, 1996; Keohane, 1984). As such, there is an urgent need for a more centralised and uniform enforcement architecture, accompanied by international data-sharing frameworks and real-time risk profiling technologies, to prevent the circumvention of global AML/CFT efforts.

Complementing this effort, the newly established EU Anti-Money Laundering Authority (AMLA) strengthens transparency requirements, particularly in relation to BO disclosures and high-risk third-country transactions (European Commission, 2024b). The AMLA is expected to have a significant impact on CBI, subjecting them to more uniform and stringent EU-wide AML/CFT standards. In line with broader regulatory trends, both the European Commission and the Court of Justice of the EU have increased their scrutiny of CBI schemes that confer nationality without a demonstrable connection between the applicant and the Member State. The AMLA framework therefore represents a shift toward centralised enforcement, compelling Member States to either reform or discontinue CBI schemes that do not align with EU legal principles and AML expectations (European Commission, 2024b), as illustrated in Malta.

To mitigate the vulnerabilities associated with inconsistent regulatory oversight, there is a compelling need for the establishment of binding minimum standards within global CBI AML/CFT frameworks, particularly concerning the registration and supervision of third-party onboarding agents involved in high-risk financial

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

transactions. A harmonised multilateral approach would require these agents, whether legal professionals, real estate intermediaries, or investment consultants to register with national AML supervisory bodies, thereby ensuring uniformity in compliance expectations and facilitating cross-border regulatory cooperation (FATF, 2022; OECD, 2023a). Such registration would not only promote transparency but also help in closing the enforcement gaps that currently allow regulatory arbitrage and the exploitation of weak jurisdictions by high-risk individuals (Joseph and Turksen, 2022; Shachar, 2017).

The establishment of a unified CBI DD infrastructure aligns with the normative expectations embedded in major international legal instruments. For instance, the United Nations Convention Against Corruption (UNCAC, 2003) explicitly encourages states to enhance cooperation, share financial intelligence, and implement robust preventive measures, including effective oversight of financial intermediaries (UNODC, 2005). Similarly, the 1999 International Convention for the Suppression of the Financing of Terrorism mandates state parties to criminalise the financing of terrorism and to establish mechanisms that ensure the accurate identification of parties involved in financial transfers (United Nations, 1999). These conventions reflect a growing international consensus that AML/CFT regimes must transcend national boundaries and include institutionalised provisions for international coordination and mutual legal assistance.

Moreover, the FATF's 40 Recommendations emphasise the need for a risk-based approach to supervision, including the regulation of Designated Non-Financial Businesses and Professions (DNFBPs), such as those acting as intermediaries in investment migration schemes (FATF, 2012). However, enforcement remains uneven, particularly in jurisdictions where regulatory capture or institutional weakness undermines compliance. As argued by Strange (1996), the diffusion of power to non-state actors complicates the capacity of individual states to assert effective regulatory control. Therefore, embedding multilateral DD frameworks and minimum DD standards is not merely desirable, it is essential for ensuring integrity and safeguarding against the misuse of CBI routes for illicit purposes.

9.3.3 *Tax Compliance*

At first, we must highlight that the obtention of residency and citizenship rights through CBI regimes can be perfectly legitimate insofar as it does not undercut the ability of other countries to levy tax on activities and individuals that are in substance based in those other countries. In that sense, even if a jurisdiction decides not to levy tax on income generated in its territory, it is illegitimate for a jurisdiction to hinder the enforcement of legitimate taxing rights arising in other jurisdictions. Furthermore, it is important to note that fair taxation of individuals with complex economic activities spanning multiple jurisdictions and types of businesses can only be attained through good-faith administrative cooperation and taxpayer disclosure.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

In this section, we review domestic and international tax features that interact with CBI regimes creating risks of tax abuse, to derive a set of minimum standards that jurisdictions offering CBI regimes can follow to minimise such risks.

CBI regimes interact with domestic an international tax regulation in different ways. The most immediate interaction is with the host jurisdiction tax system, where loopholes in personal income tax may allow newly admitted residents to escape their tax obligations in the places of actual physical residence. The tax compliance risk is two-sided in this regard.

On the one hand, CBI regimes that enable tax residency for individuals who do not physically reside at least half of the year in the jurisdiction (United Nations, 2025; OECD, 2025), effectively undermine the tax systems of other countries where CBI applicants may have more substantial economic and social presence. It is important to note that although CBI or RBI regimes provide concrete avenues to obtain the right to reside and work in a jurisdiction, the determination of tax residency is in principle a separate matter which depends on the facts and circumstances regarding the presence and activities within the jurisdiction, beyond the mere right to reside. Of course, the obtention of a physical address and the development of different types of investments in the host jurisdiction are factual circumstances that can lead to the tax residency determination. However, jurisdictions that offer CBI regimes may also have lax domestic tax residency regulations or facilitate the obtention of tax residency through poor enforcement of appropriate rules.

On the other hand, when a CBI applicant obtains tax residency from the host jurisdiction, the key question is: What would be the taxes levied on the individual? Absence of personal income tax (PIT), availability of lump-sum payment systems, or broad exemption of certain revenue streams are tax system characteristics with strong negative spillovers. These characteristics can play a determinant role in the decision of an individual to apply for a CBI regime to legally transfer its tax residence to the host jurisdiction and escape tax obligations in the places where the applicant has stronger social and economic ties. This is particularly the case for high-net worth individuals (HNWI) whose income predominantly derives from capital gains and passive investment income (Advani et al., 2023; Scheuer and Slemrod, 2019).

Indeed, because the taxing rights for these types of income are commonly assigned to the country of residence of the individual receiving such income, or 'realising' capital gains, securing tax residency in a jurisdiction that does not impose tax on these types of income, and that does not enforce customary physical presence requirements – is a particularly straightforward way to escape PIT obligations arising in other countries. Beyond jurisdictions that simply do not have PIT (and therefore may not even require the declaration of income sources and amounts), jurisdictions that allow lump-sum payments provide functional equivalent to full exemptions, insofar as the effective tax rate can be arbitrarily close to 0 per cent where income levels are sufficiently high. Territorial tax systems can also have very similar effects,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

by exempting all income from foreign sources, which is likely to be the principal (or only) source of income for individuals admitted through CBI regimes.

In addition to tax abuse risks derived from the host jurisdiction's domestic regulations, the nature of international tax regulations applicable to the country delivering CBI rights may also result in substantial tax compliance risks. Although international tax features interact with domestic regulations, they are different in the sense that the former can directly affect other countries' ability to enforce legitimate taxing rights and regulatory safeguards, while the latter may only affect other countries to the extent that such other countries sovereignly choose to forego taxation or enforcement. Specifically, we review interactions that CBI regimes can have with AEOI under the OECD CRS, and with tax treaties.

Under the CRS, financial institutions must establish an account holder's tax residency to share relevant financial information with the appropriate jurisdiction. If an individual obtains citizenship or residency documents without a genuine intention to relocate but instead to mislead their bank regarding their residency status, their financial details may either be reported incorrectly or not collected at all (OECD, 2017). For instance, a Brazilian citizen and longtime tax resident in Brazil that obtains CBI rights and a tax residency certificate from Seychelles can open bank accounts in that jurisdiction, or in any other third country, claiming to be a Seychelles tax resident.

The financial institutions where the newly admitted Seychelles resident has accounts will have an obligation to report financial data to the Seychelles, but the information will not be reported to Brazilian authorities. Even if Brazilian tax authorities consider that their citizen continues to be a tax resident or otherwise has tax obligations in the country, they will cease to receive CRS data, and may not even know the jurisdiction to which request tax cooperation, insofar as there is no legal obligation for a country operating a CBI regime to communicate the admission of an individual to his or her previous country of residence. International tax risks are further increased for jurisdictions having chosen 'voluntary secrecy' under Annex A of the Multilateral Competent Authority Agreement (MCAA), such as the United Arab Emirates (UAE) (OECD, 2025).

In this case, for instance, if Brazilian citizen obtains CBI rights in the UAE and thereafter opens bank accounts in various countries as a UAE tax resident, then financial institutions subject to MCAA obligations will not even have to report financial account data, because the UAE refuses to receive CRS information regarding its tax residents. Therefore, in this case, even if Brazilian authorities request relevant data to the UAE through administrative cooperation, the UAE will have no financial account data to share. According to the Tax Justice Network, at least twenty-eight jurisdictions have chosen voluntary secrecy under MCAA Annex A, eighteen of which offer CBI regimes (Tax Justice Network, 2022).

Another aspect of CBI regimes interacts with CRS exchange of information. Indeed, research indicates that although CRS decreases offshore tax evasion at the

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

bilateral level, a large number of tax evaders do not repatriate their funds. They rather find other ways to hide their money (Johannesen and Zucman, 2014). For instance, a 2022 study shows that the introduction of CRS is associated with a significant increase of UK real estate investment from companies incorporated in highly exposed tax havens, suggesting a dynamic of asset substitution to ensure secrecy is maintained (Bomare and Le Guern Herry, 2022). It is also evident that CRS has triggered a significant reaction in terms of taxpayer behaviour, particularly in countries with e-filing systems and stronger CRS enforcement (Alstadsæter et al., 2023). Tax evasion in CBIs can be achieved either through the offshoring of cash deposits into a CBI economy, and the investment of cash in other investments such as real estate.

Otherwise, bilateral tax treaties may also heighten tax compliance risks associated with CBI regimes. Individuals can use CBI regimes to obtain tax residency in a jurisdiction that has tax treaties facilitating tax avoidance and/or treaties that do not provide for assistance in tax collection. Indeed, CBI regimes hosted by low or no tax jurisdictions may in addition have treaties in force that prevent source taxation of important revenue streams. For instance, a jurisdiction that imposes no PIT at all, or that exempts foreign source interests, royalties, or services payments from income tax, may at the same time prevent the country where that income is generated from imposing tax. Way beyond the prevention of double taxation, these aggressive tax planning strategies ensure double non-taxation and undermine domestic resource mobilisation in source countries – where real economic activity takes place.

Another example of tax abuse risks would be tax treaties that restrict source taxation of capital gains resulting from indirect disposal of shares, under Article 13 of UN and OECD model tax conventions (OECD, 2019; United Nations, 2021). For instance, an individual may obtain tax residency in a CBI economy such as Mauritius to prevent source taxation of capital gains derived from shareholdings in India, Ghana or Namibia (Hearson, 2022). Furthermore, anticipating disputes between tax authorities, nefarious actors may strategically choose CBI jurisdictions whose treaties do not provide for assistance in tax collection, such as those that Mauritius has with Bangladesh, Madagascar, or Eswatini (Hearson, 2022).

In terms of minimum standards, we derive a set of regulatory practices that can be implemented by FIUs, CIUs, and service providers, ideally through top-down harmonisation mechanisms complemented with bottom-up calibration of processes and compliance costs. We must underline that available technology can reduce ongoing compliance costs significantly, even if this may require punctual investments in data architecture and process setup.

First, CBI applicants should declare any jurisdiction in which tax residency status has been claimed or obtained in the last five years. False declaration should trigger asset freezing and economic/criminal sanctions. This could take the form of a declaration to the relevant CIU which is shared with the tax authority. Alternatively, tax residency information could also be submitted to the CIU service

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

provider, insofar as it presents clear disclaimers of the relevance of this data and liabilities that the applicant may incur in case of false declaration and shares this information with the CIU in due course. Along the CBI application process, it is important to consider the moment in which tax residency declared data is shared with supervisory authorities beyond the CIU. It is suggested that such information is shared with tax authorities whenever declared assets or residency indicate potentially competing tax residency claims before the application is accepted or rejected. This may allow proactive administrative cooperation with relevant foreign authorities, as well as valuable opinion from domestic tax authorities on flagged applications (which may or may not be binding but should in any case be documented). FIUs should have access to the entirety of the CBI application file upon acceptance of an individual.

Second, upon acceptance of the CBI applicant, the host country should issue an automated notification to all relevant jurisdictions (e.g. all those where the newly admitted citizen/resident has investments). The host country should allow for exceptional non-reporting to any jurisdiction for which the individual can demonstrate unfair prosecution (political, racial, religious) or other risks to its personal or family integrity. While this exceptional treatment should ensure legitimate protection of unfairly prosecuted individuals, it should be meticulously documented and the (confidential) decision recorded indefinitely on public authority records.

Third, minimum standards must ensure clear distinction between CBI rights and tax residency determination, together with strict enforcement of the 183-day tax residency rule. Ongoing monitoring of passenger, vehicle and telecommunications data can distinguish individuals which appear to fulfil physical residency requirements from more complex or illicit practices. The determination of tax residency and tax obligations for highly mobile individuals who do not spend 183 days in any jurisdiction should be determined through good-faith administrative cooperation with other relevant jurisdictions – following the principles of economic substance and source taxation of domestic activities.

Fourth, host countries should participate in the MCAA to implement automatic information of bank account information, without choosing to be listed under MCAA Annex A. The Convention on Mutual Administrative Assistance in Tax Matters (MAA, amended 2010) is also an important instrument for effective cooperation upon request. Host countries should sign and ratify both treaties and seek third country technical assistance and capacity building if considered necessary.

Finally, host countries should conduct a comprehensive review of tax treaties in force, to identify provisions that unfairly restrict source tax rights for income that is not subject to tax in the CBI economy. In addition, the review should flag any treaties which do not ensure mutual assistance for tax collection, and for which such assistance is not ensured through multilateral treaties (e.g. MAA). The United Nations Fast-track instrument allows for streamlined amendment of tax treaties, to modify all necessary provisions (United Nations, 2024). If bilateral relations

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

constrain tax treaty amendment, it is possible to terminate bilateral treaties while ensuring administrative cooperation (via multilateral treaties such as the MCAA and the MAA) and avoiding double taxation (e.g. foreign tax credit system). Under domestic law, it is possible to provide a comprehensive definition of permanent establishment, and also to designate preferential tax treatments or regimes for foreign-based companies that are conditional upon the reciprocal implementation of such regimes by foreign counterparts.

9.4 LEGALITY AND ETHICAL ISSUES IN THE USE OF AI

Before any AI tool is deployed in administering CBI programmes and processing CBI applications, societal, ethical, and legal impact assessment must be conducted. The potential ethical and legal risks associated with the deployment of AI in policing functions have been critically explored in Chapter 5 of this book. In the context of CBI programmes, similar concerns arise. Algorithmic decision-making may inadvertently reinforce societal biases, especially where training data reflects historical discrimination, potentially leading to unjust denials based on race, nationality, or socio-economic status. Additionally, the use of AI in this domain often requires processing large volumes of sensitive personal data, raising serious concerns about privacy, transparency, and accountability. The opacity of certain AI models, especially black-box algorithms, may further undermine applicants' rights to explanation and recourse, posing challenges for both procedural fairness and compliance with data protection frameworks such as the General Data Protection Regulation (GDPR) (European Commission, 2021; EU AI Act, 2024).

While well-designed AI systems and trustable datasets have the potential to mitigate human biases, evidence suggests that many algorithms may also inadvertently perpetuate and even amplify the biases of their designers (Klein, 2019). This occurs because AI systems often identify correlations between characteristics and outcomes, using these patterns to predict future events (Klein, 2019). The critical issue here is that correlation does not imply causation, and relying on such associations can lead to discrimination against specific groups, including women and ethnic minorities (Klein, 2019) or global majorities. In the context of CBI due diligence, risk assessments are particularly vulnerable to profiling, which could be exacerbated by the introduction of novel AI systems.

A pertinent example illustrating the potential repercussions of such biased profiling is the Dutch AI scandal, where over 26,000 families were wrongfully accused of fraud due to an AI system designed to detect large-scale benefit fraud (Arts and Marguerite, 2025). Notably, more than half of the families targeted were from ethnic minorities or had low income. This case underscores the risks associated with AI-driven profiling, highlighting the need for careful consideration in CBI applications to prevent false positives that could unjustly target particular individuals.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Recognising these challenges, proper regulatory standard for AI in CBI DD is needed. For example, the EU has taken proactive steps to regulate the development and use of AI, the same should be emulated in CBI countries operationalising AI. Building upon its GDPR framework (GDPR, 2018), the European Union Artificial Intelligence Act (EU AI Act) (European Commission, 2024a) is the first comprehensive legal framework to regulate AI systems across the EU. The EU AI Act stipulates a risk-based regulatory approach to ensure AI development and deployment are ethical, transparent, and aligned with fundamental human rights.

The EU AI Act also outlines requirements for high-risk AI systems, encompassing data governance, documentation, transparency, human oversight, robustness, accuracy, and security (European Parliament, 2023). High-risk AI systems, which include those handling personal information to determine citizenship, are subject to stricter safeguards. For example, Article 5 of the AI Act deems certain types of social scoring and biometric surveillance as posing an unacceptable risk to privacy and non-discrimination, leading to a complete ban on such AI systems (EU AI Act, 2024). Public authorities are prohibited from scoring individuals' trustworthiness in one context to justify detrimental treatment in another, unrelated context (EU AI Act, 2024, Article 5).

Further, under Article 6 of the EU AI Act (Regulation (EU) 2024/1689), an AI system is classified as high-risk if it is intended to be used in areas where its deployment can significantly impact fundamental rights, safety, or health. This includes AI applications in critical domains such as biometric identification, law enforcement, migration, and the administration of justice. The high-risk designation reflects the potential for such systems to cause harm or infringe on individuals' rights if not properly designed, monitored, and controlled (EU AI Act, 2024, Article 6).

In applying these principles to CBI programmes, it is crucial to ensure that AI systems do not infringe upon applicants' fundamental human rights, including privacy and non-discrimination. Under the EU AI Act, CBI due diligence processes that employ AI-based risk assessment tools would be classified as high-risk AI systems. This is because these systems would process sensitive and personal data to assess applicants while relying on biometric information. Incorporating best practices and risk assessment exercises from initiatives such as the TRACE project (TRACE, 2025), can provide valuable insights and guidance.

The legal requirements for a high-risk CBI AI system, transparency, efficiency, and accountability must be clear. Furthermore, the EU AI Act mandates that human rights impact assessments be performed throughout the lifecycle of the AI system. During the conceptualisation and implementation phases of the CBI AI system, these impact assessments could help to expose any potential human rights risks that may otherwise elude existing CBI programme risk management processes.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

9.5 OPERATIONALISING AI IN CBI DD

AI technologies, particularly Machine Learning (ML), offer substantial potential to strengthen DD procedures in CBI programmes. ML is a subset of AI that enables systems to learn from data patterns and make predictions or decisions without being explicitly programmed (Samuel, 1959; Mitchell, 1997). In the context of CBI, ML algorithms can automate critical stages of the applicant vetting process, including identity verification, source of wealth analysis, and risk profiling. For instance, ML tools can rapidly cross-check applicant data against global sanctions, politically exposed persons (PEP) lists, and adverse media databases, which are commonly used in AML and CFT frameworks (FATF, 2022). Furthermore, ML systems can analyse transactional data to detect anomalies indicative of IFFs, such as layering techniques or unexplained wealth accumulation.

Importantly, ML models can also triage applications by flagging high-risk individuals for enhanced due diligence (EDD), thereby ensuring that additional scrutiny is applied where necessary. This reduces reliance on manual checks, which are often time-consuming and vulnerable to oversight, and enhances consistency in compliance with international AML/CFT obligations (OECD, 2023a). By introducing speed, precision, and scalability into the DD process, AI not only improves operational efficiency but also strengthens the integrity and transparency of CBI schemes. Nevertheless, its deployment must be accompanied by ethical safeguards and robust regulatory oversight to prevent algorithmic bias and ensure accountability (European Commission, 2021).

9.5.1 *Identity Verification*

AI can streamline identity verification by integrating biometric analysis, facial recognition, and document authentication technologies. ML algorithms can detect forgery, tampering, or inconsistencies in passports, national IDs, and supporting documents. By cross-referencing applicant biometrics with government and international databases, AI enhances the detection of identity fraud and impersonation. This ensures that CBI applicants undergo stringent authentication before proceeding with the investment process, reducing the risk of fraudulent applications slipping through weak due diligence checks. AI-driven identity verification solutions can leverage deep learning-based computer vision to authenticate passports, government-issued IDs, and residency documents.

Using OCR (Optical Character Recognition) and facial biometrics, AI can detect forgery, digital manipulation, or deepfake identity fraud. These tools integrate with government databases, PEP lists, and international watchlists to validate applicant authenticity in real time. Finally, AI-powered Natural Language Processing (NLP) can scan news sources, court filings, leaked financial reports, and regulatory databases for negative news, financial crimes, or corruption links associated with

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

applicants. Advanced sentiment analysis and named entity recognition (NER) can help classify high-risk individuals.

9.5.2 *Source of Funds Analysis*

AI can also improve source of funds and BO verification by analysing financial transactions, banking records, and investment histories for suspicious patterns. Anomaly detection models can flag inconsistencies, rapid asset movements, or offshore structuring indicative of money laundering or tax evasion. AI-powered KYC and AML compliance systems can cross-check applicant financial data with sanctions lists, PEP databases, and global financial intelligence networks. This automation not only reduces human error but also accelerates decision-making, ensuring CBI applicants comply with international financial regulations.

These tools use ML to detect deviations from normal financial behaviour, flagging transactions linked to high-risk jurisdictions or sanctioned entities. Distributed ledger technology (DLT), combined with AI, can enhance transparency in CBI applications by securely recording due diligence findings, financial transactions, and approval decisions on an immutable ledger. AI can automate smart contract execution, ensuring compliance with minimum due diligence requirements before citizenship applications are approved. This approach reduces document fraud, ensures auditability, and strengthens trust between governments, financial institutions, and international regulators.

From a tax compliance perspective, the analysis of the source of funds is closely related to the applicant's activities across different jurisdictions. Automated processes can allow for the identification of key countries where the applicant conducts business and requests additional information from relevant authorities, using appropriate document templates. In addition to streamlining international cooperation processes, information resulting from them can be used to undertake enhanced verification of third country activities and assess the nature of funds.

9.5.3 *Compliance Monitoring*

AI can automate compliance with key international standards such as FATF's 40 Recommendations, EU's AMLD6, and OECD's CRS to counter financial crimes. By integrating AI-driven risk assessment dashboards, CBI authorities can align investment migration policies with evolving international obligations and avoid grey/blacklisting risks. Sanctions Scanner's AI-driven compliance system (Sanctions Scanner, 2026) continuously updates sanctions lists, terrorist financing risks, and PEPs, ensuring CBI applicants are screened against real-time global intelligence sources.

Given the fact that most CBI programmes grant citizenship relatively quickly, DD should not stop once citizenship is granted. AI-powered continuous monitoring

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

systems can track post-naturalisation activities to identify red flags such as financial crimes, sudden wealth transfers, or suspicious travel patterns. AI can integrate with international policing organisations (e.g., Interpol and Europol), FIUs, and border security databases to ensure that CBI recipients remain compliant with host country laws. If post-citizenship risks arise, AI can trigger alerts to initiate further investigation by competent authorities.

More specifically in relation to tax compliance, the effective residence of an individual in the host jurisdiction can be assessed with automated tools, for example by monitoring passenger arrival/departure data and/or telecom signal. AI processes can allow to red-flag individuals whose presence in the host jurisdiction appears to be below 183 days, in order to perform additional verifications to determine tax residence.

9.5.4 *Predictive Analysis*

AI can develop predictive risk models by aggregating data from past applicants, compliance failures, and global enforcement actions to generate applicant risk scores. These models consider factors such as economic background, geopolitical risk, past financial activity, and business affiliations to determine the likelihood of an applicant being involved in illicit financial activities. It is important to distinguish the various ways in which AI technologies can contribute to risk assessment models.

First, it is possible to train an AI model with as much data as is available and allow it to determine by way of probabilistic and statistical process which are the risk parameters that are indicative of illicit activities. These techniques are not only prone to bias because they may exploit variables that should not be used such as religious affiliation, but also because they are limited by the type of data used for training, which may be biased in favour of certain activities due to difficulties in monitoring or prosecution of specific types of financial crimes (thus rendering available data insufficient to identify suspicious patterns). Practitioners at national AML supervisory authorities warn against the usage of unsupervised AI models, noting that it is not possible to understand all the reasons why the algorithm has flagged a specific entity or transaction (García Fresno, 2022).

Second, supervised learning models can allow for the calibration of risk assessment techniques that use multiple indicators which are considered relevant to the illicit activity in question. In this case, a variety of algorithmic and probabilistic techniques are available to evaluate how relevant each risk indicator is for the prediction of certain activities. Beyond the choice of the mathematic calibration technique, the most important aspect is to define and obtain relevant data on the outcome variable that should maximised. This can be the choice of an obliged entity to issue a suspicious transaction report (STR), the decision to open an investigation by the FIU, the obtention of a conviction by prosecutorial authorities, or even the amount of funds recovered.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Third and perhaps most important, AI can help making the most out of predictive analysis and facilitating the interpretation of complex risk assessments with the automated production of written summaries and figures that highlight the importance of specific risk indicators. These outputs could assist compliance officers in drafting STRs or supervisory authorities to motivate judicial requests. Ideally, risk assessment technologies would combine risk features related to particular entities, activities, and transactions – with risk features related to the regulatory environment in which activities take place (geographic risk). With increasingly complex risk assessment methods, the capacity of AI technology to make the output of those methods understandable is essential both for human use and method improvement, and for its consideration in legal proceedings (e.g., audits and trials) (Sachoulidou, 2023). AI-generated risk scores allow CBI regulators to allocate resources more effectively, ensuring that higher-risk cases undergo deeper scrutiny while low-risk applicants experience faster processing.

Supervised learning models trained on historical compliance data can generate applicant risk scores based on:

- Geopolitical risk (home country of applicant);
- Past business activities and corporate affiliations;
- Tax compliance and financial disclosure; and
- Cross-border financial behaviour.

For example, AI models trained with information on jurisdiction's tax systems and the level of secrecy in financial services sectors may be able to identify substantial differences between the applicant jurisdiction(s) of origin and the host jurisdiction. These differences can help identifying individuals that seek to obtain CBI for tax evasion or avoidance.

9.5.5 *Automation of Reporting*

AI-driven due diligence solutions can revolutionise CBI programmes by ensuring higher compliance standards, fraud detection, and risk mitigation. By integrating ML, NLP, and blockchain technologies, CBI jurisdictions can establish minimum due diligence standards that meet international AML/CFT standards. However, for AI to be fully effective, CBI regulators must develop standardised governance frameworks, ensuring ethical AI deployment, robust data collection and protection, and human oversight in IM screening processes. In this context, it is very important that FIUs implement strict format requirements to ensure that a minimum set of information fields are systematically made available in a predefined structured data format.

Furthermore, in the case of spontaneous or upon request communications between public authorities, automated processes should allow the minimisation or elimination of cumbersome paperwork, making inter-institutional and international cooperation as efficient as possible. Leveraging existing data on international

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

cooperation treaties (Tax Justice Network, 2022), authorities of a given jurisdiction can automatically generate a document addressed to another jurisdiction which identifies available legal bases for information sharing, judicial cooperation, or assistance in tax collection.

9.6 AI FACILITATING MINIMUM DD STANDARDS

AI can play a crucial role in maintaining minimum DD standards in CBI programmes by ensuring consistent, automated, and data-driven risk assessment across all applications. AI-powered identity verification tools, such as TRACE, Jumio, and Onfido (TRACE, 2025; Jumio, 2024; Onfido, 2024), use deep learning and biometric authentication to detect fraudulent documents and synthetic identities, reducing the risk of applicant misrepresentation. Additionally, AI-driven adverse media screening and sanctions checks, powered by NLP models like IBM Watson and Refinitiv World-Check (IBM, 2024; Refinitiv, 2024), provide real-time monitoring of financial crime risks, ensuring applicants are continuously screened against evolving global watchlists. In verifying the source of funds, AI-based graph analytics tools, such as Quantexa and Feedzai (Quantexa, 2024; Feedzai, 2024), analyse financial transactions to detect hidden connections to high-risk entities, preventing IFFs from entering CBI schemes.

By integrating predictive analytics, AI enhances risk-based DD by generating applicant risk scores based on geopolitical, financial, and reputational factors, ensuring uniform compliance with FATF Recommendations and other relevant legal instruments. Furthermore, AI-powered blockchain solutions, like Hyperledger Fabric (Hyperledger, 2024), provide immutable records of applicant data and due diligence approvals, preventing manual tampering or politically influenced decision-making. Post-citizenship, AI-driven continuous monitoring systems, such as Darktrace and ThetaRay (Darktrace, 2024; ThetaRay, 2024), track suspicious financial activity among CBI recipients, enabling regulatory authorities to revoke citizenship from individuals linked to financial crime or national security threats.

By leveraging AI, CBI programmes can enforce standardised DD procedures, reduce reliance on inconsistent human-led assessments, and mitigate the risks of regulatory arbitrage, where applicants exploit discrepancies between national regulatory frameworks., and ensure long-term compliance with international anti-money laundering and counter-financing of terrorism (AML/CFT) standards, such as those mandated by the FATF and the 6AMLD. In doing so, AI helps to ensure long-term regulatory alignment resilience against misuse by high-risk applicants (FATF, 2022; European Commission, 2023; Joseph and Turksen, 2022).

9.7 CONCLUSION

To strengthen DD in CBI, it is recommended that CBI host countries implement AI-powered compliance frameworks that integrate automated identity verification,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

transaction monitoring, and adverse media screening amongst other techniques to ensure uniformity across all applications. These countries should mandate that all third-party agents involved in CBI DD register with national AML authorities and adhere to AI-enhanced regulatory standards to prevent weak enforcement. Furthermore, CBI programmes should leverage AI-driven ML solutions to create transparent and tamper-proof applicant records, enhancing accountability and reducing the risk of political interference.

Continuous AI-based post-citizenship monitoring should also be adopted to detect and address emerging risks associated with financial crime and security threats. Ultimately, by fully embracing AI technologies, CBI programmes can enhance transparency, mitigate risks, and maintain compliance with evolving global financial regulations, ensuring that investment migration remains a legitimate and secure pathway to citizenship.

REFERENCES

Abbott, K. and Snidal, D. (2000) Hard and soft law in international governance. *International Organization*, 54(3), pp. 421–456.

Advani, A. et al. (2023). How much tax do the rich really pay? Evidence from the UK. *Oxford Review of Economic Policy*. Vol. 39(3), pp. 406–437.

Ahmad, A. (2024) All-Time High: Antigua & Barbuda CBI Application Volume up 205% Year-On-Year in H1 2024. Investment Migration Insider. Available at: www.imidaily.com/intelligence/all-time-high-antigua-barbuda-cbi-application-volume-up-205-year-on-year-in-h1-2024/ (Accessed 4 February 2025).

Alstadsæter, A., Casi, E., Miethe, J., and Stage, B. (2023) Lost in information: national implementation of global tax agreements. NHH Dept. of Business and Management Science Discussion Paper (2023/22).

Arts, J. and van den Berg, M. (2025) What the Dutch benefits scandal and policy's focus on 'fraud' can teach US about the endurance of empire. *Critical Social Policy*. Vol. 45 Issue 1. pp. 177–187.

Bomare, J. and Le Guern Herry, S. (2022) Will We Ever Be Able to Track Offshore Wealth? Evidence from the Offshore Real Estate Market in the UK (Working Paper No. 4), EU Tax Observatory. Available at: www.taxobservatory.eu/publication/will-we-ever-be-able-to-track-offshore-wealth-evidence-from-the-offshore-real-estate-market-in-the-uk/ (Accessed 4 February 2025).

CS Global Partners (2025) Rising Interest in Caribbean Citizenship by Investment Programmes among Wealthy Americans. (online) CS Global Partners Limited. Available at: https://csglobalpartners.com/news/rising-interest-in-caribbean-citizenship-by-investment-programmes-among-wealthy-americans/ (Accessed 4 February 2025).

Companies House (2023) Companies House. (online) GOV.UK. Available at: www.gov.uk/government/organisations/companies-house (Accessed 4 March 2025).

Complete Professional Services, LLC. (CPS IT Solutions) (2016) FFIEC BSA/AML Assessing Compliance with BSA Regulatory Requirements – Beneficial Ownership Requirements for Legal Entity Customers. (online) Ffiec.gov. Available at: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/03 (Accessed 4 February 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Court of Justice of the European Union (2022) Ruling on public access to beneficial ownership registers. (online) Available at: https://curia.europa.eu/site/upload/docs/application/pdf/2022-11/cp220188en.pdf (Accessed 18 April 2026).
Darktrace (2024) AI for Cybersecurity and Threat Detection. (online) Darktrace. Available at: www.darktrace.com (Accessed 4 April 2025).
Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (2018) OJ L284/22.
Drezner, D. W. (2001) Globalization and policy convergence. *International Studies Review*, 3, pp.53–78.
Dun & Bradstreet (2011) Dun & Bradstreet – Accelerate Growth and Improve Business Performance. (online) Dnb.co.uk. Available at: www.dnb.co.uk/ (Accessed 4 March 2025).
European Commission (2019) EUR-Lex - COM/2019/12 final -EN. (online) EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0012 (Accessed 18 April 2026).
European Commission (2021) EUR-Lex – 52021PC0206 – EN. (online) EUR-Lex. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206 (Accessed 4 February 2025).
European Commission (2021) Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. (online) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (Accessed 4 February 2025).
European Commission (2023) Investor Citizenship and Residence Schemes in the EU. (online) Available at: https://ec.europa.eu (Accessed 1 April 2025).
European Commission (2024a) 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). (online) Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Accessed 15 April 2025).
European Commission (2024b) The EU's Anti-Money Laundering Authority: Stronger Rules to Fight Financial Crime. Available at: https://ec.europa.eu/info/publications/eu-anti-money-laundering-authority_en (Accessed 21 May 2025).
European Parliament (2023) EU AI Act: First Regulation on Artificial Intelligence. (online) Available at: www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (Accessed 4 February 2025).
EU AI Act (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), Article 6. (online) Available at: https://artificialintelligenceact.eu/article/6/ (Accessed 15 April 2025).
FATF (2012) Recommendation 10: Customer Due Diligence. (online) Available at: www.fatf-gafi.org/publications/fatfrecommendations/ (Accessed 4 February 2025).
FATF (2022) Money Laundering and Citizenship by Investment Programmes. (online) Available at: www.fatf-gafi.org (Accessed 4 February 2025).
Feedzai (2024) AI for Financial Crime Prevention. (online) Feedzai. Available at: www.feedzai.com (Accessed 4 April 2025).
FinCEN (2018) Customer Due Diligence Requirements for Financial Institutions, 31 CFR § 1010.230. (online) FinCEN.gov. Available at: www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule? (Accessed 4 February 2025).
García Fresno, M. (2022) Analiza, que no es poco: Herramientas para el Análisis de Operaciones de Blanqueo de Capitales y de Financiación del Terrorismo. Madrid: Fundación Notariado.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Available at: https://publicaciones.notariado.org/p/-papel-analiza-que-no-es-poco-2 (Accessed 4 March 2025).
GDPR (2018) General Data Protection Regulation (GDPR). (online) Available at: https://gdpr-info.eu/ (Accessed 4 February 2025).
Government of Malta (2023) Individual Investor Programme. (online) Available at: https://iip.gov.mt (Accessed 1 April 2025).
Government of Saint Kitts and Nevis (2023) Citizenship by Investment Unit. (online) Available at: www.ciu.gov.kn (Accessed 1 April 2025).
Hearson, M. (2022) Tax Treaties Explorer (Online database), Brighton: International Centre for Tax and Development (ICTD), www.treaties.tax (Accessed 1 April 2025).
Hyperledger (2024) Hyperledger Fabric: A Distributed Ledger Technology for Blockchain Solutions. (online) Hyperledger. Available at: www.hyperledger.org/use/fabric (Accessed 4 April 2025).
IBM (2024) Watson for Financial Services. (online) IBM. Available at: www.ibm.com/watson/financial-services (Accessed 4 April 2025).
Jensen, M. C. and Meckling, W. H. (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), pp. 305–360.
Johannesen, N. and Zucman, G. (2014) The end of bank secrecy? An evaluation of the G20 tax haven crackdown. *American Economic Journal: Economic Policy*, 6, pp. 65–91.
Joseph, J. (2021) Leveraging Artificial Intelligence in Citizenship by Investment Programmes. In Bielicki, D. M., ed., *Regulating Artificial Intelligence in Industry*. New York: Routledge. Available at: www.routledge.com/Regulating-Artificial-Intelligence-in-Industry/Bielicki/p/book/9780367774622 (Accessed 1 February 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. Available at: https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-2-01.pdf (Accessed 1 February 2025).
Jumio (2024) Identity Verification and Compliance Solutions. (online) Jumio Corporation. Available at: www.jumio.com (Accessed 4 April 2025).
Kenton, W. (2024) Anti-Money Laundering (AML): What It Is, Its History, and How It Works. (online) Investopedia. Available at: www.investopedia.com/terms/a/aml.asp? (Accessed 4 February 2025).
Keohane, R. O. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.
Klein, K. (2019) Algorithms, Race, and Reentry: A Review of Sandra G. Mayson's Bias In, Bias Out. (online) Available at: https://ccresourcecenter.org/2019/11/05/algorithms-race-and-reentry-a-review-of-sandra-g-maysons-bias-in-bias-out/ (Accessed 4 February 2025).
LexisNexis (n.d.) LexisNexis. (online) Available at: www.lexisnexis.com (Accessed 4 April 2025).
Mitchell, T. M. (1997) *Machine Learning*. New York: McGraw-Hill.
Moody's (2025) Orbis – BvD Is Now Moody's. (online) Available at: www.moodys.com/web/en/us/capabilities/company-reference-data/orbis.html (Accessed 4 March 2025).
OECD (2017) *Standard for Automatic Exchange of Financial Account Information in Tax Matters*. 2nd ed. Paris: OECD Publishing.
OECD (2018a) Illicit Financial Flows. (online) Available at: www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/illicit-financial-flows_g1g679f5/9789264268418-en.pdf (Accessed 4 February 2025).
OECD (2018b) Preventing the Misuse of Investment Migration Programmes. (online) Available at: www.oecd.org (Accessed 4 February 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

OECD (2019) Model Tax Convention on Income and on Capital. Available at: https://www.oecd.org/en/publications/serials/model-tax-convention-on-income-and-on-capital-full-version_57a089d7.html (Accessed 18 April 2026).
OECD (2023a) CRS Guidance on Investment Migration. (online) Available at: www.oecd.org (Accessed 4 February 2025).
OECD (2023b) Misuse of Citizenship and Residency by Investment Programmes. (online) Available at: www.oecd.org/en/publications/misuse-of-citizenship-and-residency-by-investment-programmes_ae7ce5fb-en.html (Accessed 4 February 2025).
OECD (2023c) Guidelines for MNEs. (online) Available at: https://mneguidelines.oecd.org/ (Accessed 4 February 2025).
OECD (2025) OECD Model Tax Convention on Income and on Capital. Available at: www.oecd.org/en/publications/serials/model-tax-convention-on-income-and-on-capital-full-version_57a089d7.html (Accessed 1 April 2025).
Onfido (2024) Digital Identity Verification Software. (online) Onfido. Available at: www.onfido.com (Accessed 4 April 2025).
PwC (2021) Emerging technologies in anti-financial crime: The role of AI and machine learning. (online) PricewaterhouseCoopers. Available at: www.pwc.com/gx/en/industries/financial-services/publications/emerging-technologies-in-anti-financial-crime.html (Accessed 4 April 2025).
Quantexa (2024) Network Analytics and Data-Driven Decision Making. (online) Quantexa. Available at: www.quantexa.com (Accessed 4 April 2025).
Refinitiv (2024) World-Check: Risk Intelligence. (online) Refinitiv. Available at: www.refinitiv.com/en/products/world-check-risk-intelligence (Accessed 4 April 2025).
Republic of Turkey Ministry of Interior (2023) Turkish Citizenship by Investment. (online) Available at: www.nvi.gov.tr (Accessed 1 April 2025).
Sachoulidou, A. (2023) Going beyond the 'common suspects': To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-023-09347-w (Accessed 4 March 2025).
Samuel, A. L. (1959) Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 3(3), pp. 210–229.
Sanctions Scanner (2026) Homepage. Available at: https://www.sanctionscanner.com (Accessed 18 April 2026).
Sayari (2025) Sayari. (online) Available at: https://sayari.com/ (Accessed 4 March 2025).
Scheuer, F. and Slemrod, J. (2019) Taxation and the Superrich (No. w26207), Cambridge, MA: National Bureau of Economic Research. Available at: www.nber.org/papers/w26207.pdf (Accessed 15 April 2025).
Shachar, A. (2017) *The Birthright Lottery: Citizenship and Global Inequality*. Cambridge, MA: Harvard University Press.
Sophia, I. N. (2022) Report with proposals to the Commission on Citizenship and Residence by Investment Schemes | A9-0028/2022. (online) European Parliament. Available at: www.europarl.europa.eu/doceo/document/A-9-2022-0028_EN.html (Accessed 4 February 2025).
Starcevic, S. (2025) Malta's 'golden passport' scheme is illegal, EU top court rules. *POLITICO*. Available at: www.politico.eu/article/european-court-rules-maltese-golden-passport-scheme-against-eu-law/ (Accessed 30 April 2025).
Strange, S. (1996) *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.
Surak, K. (2021) Marketizing sovereign prerogatives: how to sell citizenship. *Archives Europeennes de Sociologie*, 62(2), 275–308.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Tax Justice Network (2022, May 17) Financial Secrecy Index 2022. Available at: https://fsi.taxjustice.net/ (Accessed 4 April 2025).

The Guardian (2025, April 29) Malta's 'golden passport' scheme ruled to be illegal by EU's top court. Available at: www.theguardian.com/world/2025/apr/29/malta-golden-passport-scheme-ruled-to-be-by-eu-top-court (Accessed 30 April 2025).

ThetaRay (2024) AI-Powered Financial Crime Detection. (online) ThetaRay. Available at: www.thetaray.com (Accessed 4 April 2025).

TRACE (2025) Homepage. Available at: https://trace-illicit-money-flows.eu/ (Accessed 4 February 2025).

Transparency International (2023) Corruption Perceptions Index. (online) Available at: www.transparency.org/en/cpi/2023 (Accessed 26 February 2025).

UNODC (2005) United Nations Convention Against Corruption. (online) Available at: www.unodc.org/unodc/en/corruption/uncac.html (Accessed 4 February 2025).

United Nations (1999) International Convention for the Suppression of the Financing of Terrorism. (online) Available at: www.un.org/law/cod/finterr.htm (Accessed 4 February 2025).

United Nations (2021) Model Double Taxation Convention Between Developed and Developing Countries. Available at: https://financing.desa.un.org/sites/default/files/2023-05/UN%20Model_2021.pdf (Accessed 18 April 2026).

United Nations Secretariat (2024) Proposed text of a Fast-track Instrument to Provide for the Streamlined Amendment of Bilateral Double Taxation Treaties. Available at: https://digitallibrary.un.org/record/4074391?v=pdf (Accessed 18 April 2026).

United Nations (2025) Model Double Taxation Convention between Developed and Developing Countries. Available at: https://desapublications.un.org/publications/united-nations-model-double-taxation-convention-between-developed-and-developing-0 (Accessed 1 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

10

Conclusion

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

This edited volume brings together a rich tapestry of interdisciplinary perspectives to explore the transformative potential of AI tools in the prevention, investigation, and prosecution of financial crime and money laundering. Central to this inquiry is the cross-cutting issue of illicit financial flows, which are increasingly facilitated by complex and opaque financial architectures. Across its chapters, a shared narrative emerges: the convergence of emerging technologies – particularly AI and machine learning – with globalisation and novel financial systems such as decentralised finance (DeFi) presents both unprecedented opportunities for criminal exploitation and powerful new tools for law enforcement and regulatory oversight.

A recurring theme throughout the book is the duality of promise and peril inherent in the deployment of AI systems for law enforcement purposes. This duality raises critical questions about ethics, regulation, and institutional design at both national and supranational levels. The uneven pace of regulatory adaptation to technological innovation, coupled with the challenges of crafting robust governance frameworks, forms an overarching concern across the contributions. Whether examining AI-powered policing tools, anti-money laundering (AML) mechanisms, or citizenship-by-investment (CBI) programs, the chapters underscore the importance of embedding principles such as contextuality, representativeness, transparency, fairness, accountability, and access to effective remedies into the design and deployment of AI systems.

This imperative becomes even more pressing when AI tools are integrated into public governance, where their use can pose significant risks to fundamental rights. Several chapters highlight the need for context-aware regulation, enhanced transparency requirements, and institutionalised training – particularly in law enforcement settings where AI may impact privacy, data protection, non-discrimination, the presumption of innocence, and other core defence rights. At the technical level, these risks suggest that legal safeguards must be complemented by design choices that reflect ethical, cultural, and socio-legal specificities, moving beyond mere risk management to embrace a holistic approach to responsible innovation.

The chapters focusing on financial crime detection and AML reforms articulate a broader ambition: transitioning from reactive compliance models to proactive,

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

evidence-based systems. Proposed frameworks such as geographic risk assessments and suspicious transaction monitoring tools – based on the 'weakest link' methodology – challenge traditional reliance on blacklisting. Instead, they advocate for the use of verifiable secrecy scores to enhance both efficiency and transparency in AML efforts. These contributions also stress the critical importance of interoperability and cross-border cooperation. Whether addressing the technical intricacies of joint investigations or the geopolitical risks posed by fragmented AML oversight (e.g., inconsistent suspicious transaction reporting standards), the book makes a compelling case for harmonised regulatory standards, secure data-sharing infrastructures, and trust-based collaboration among stakeholders. The European Union is presented as a paradigmatic testing ground for such integrative solutions.

Beyond enforcement, the book also examines how AI is reshaping financial ecosystems more broadly. The dual-use nature of emerging technologies – especially in DeFi, blockchain, and the Internet of Things (IoT) – is not treated as an anomaly but as a defining feature of the digital age. Chapters exploring this convergence argue that the question is no longer whether AI and DeFi will transform finance, but rather how regulators, policymakers, and technologists will shape the trajectory of that transformation. One particularly provocative concept is that of embedded supervision, which raises complex questions about reconciling privacy-preserving technologies with lawful access, and the feasibility of regulators deploying AI agents to interact with DeFi protocols in real time. How these tensions are resolved will significantly influence whether financial innovation serves the public interest or evolves into opaque systems that threaten democratic governance.

The future of AI in law enforcement – whether deployed by public authorities or private institutions – hinges not only on technological advancement but also on the normative principles guiding its development, training, and use. As highlighted in chapters on AI adoption in banking and CBI programs, aligning AI deployment with values such as fairness, ethics, accountability, and transparency is essential to building trust, ensuring due diligence, and maintaining compliance across jurisdictions. This edited volume serves as a timely reminder that human agency and institutional investment are indispensable in managing the risks and realising the benefits of AI. From training law enforcement personnel to establishing AI ethics bodies, conducting fundamental rights impact assessments, and promoting transparency in AI procurement, institutions must be equipped not only with tools but also with the values and expertise necessary for responsible use – especially given the inherent power imbalances AI systems may reinforce.

Ultimately, the contributions in this book offer both a diagnosis and a roadmap. They illuminate systemic gaps in regulation, governance, and international cooperation in the realm of automated law enforcement, while also proposing actionable strategies to address these challenges. These include calls for stronger AI governance, harmonisation of cross-border investigative tools, and ethical stewardship of AI technologies. Technological progress, the book argues, is not an inevitability but

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

a means to an end. The impact of AI on law enforcement will be shaped by the frameworks we construct, the institutions we empower, and the values we uphold. In this spirit, the book invites readers and stakeholders not merely to observe the ongoing transformation but to actively participate in shaping it through responsible innovation, interdisciplinary research, and collaborative governance.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Bibliography

Abbott, K. and Snidal, D. (2000) Hard and soft law in international governance. *International Organization*, 54(3), pp.421–456.

Adamyk, B., Benson, V., Adamyk, O. and Liashenko, O. (2025) Risk management in DeFi: analyses of the innovative tools and platforms for tracking DeFi transactions. *Journal of Risk and Financial Management*, 18(1), p.38.

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.

Aden, H. (2016) The role of trust in the exchange of police information in the European multilevel system, in Delpeuch, T. and Ross, J. (eds.) *Comparing the Democratic Governance of Police Intelligence*. Cheltenham: Edward Elgar Publishing, pp.322–344.

Adeyelu, O. O., Ugochukwu, C. E. and Shonibare, M. A. (2024) Ethical implications of ai in financial decision-making: a review with real world applications. *International Journal of Applied Research in Social Sciences*, 6(4), pp.608–630. https://doi.org/10.51594/ijarss.v6i4.1033 (Accessed 11 April 2025).

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

Ahamad, S., Gupta, P., Acharjee, P.B., Kiran, K.P., Khan, Z. and Hasan, M.F (2022) The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market. *Materials Today: Proceedings*, 56, pp.2070–2074.

Ahmad, A. (2024) All-Time High: Antigua & Barbuda CBI Application Volume up 205% Year-On-Year in H1 2024. Investment Migration Insider. www.imidaily.com/intelligence/all-time-high-antigua-barbuda-cbi-application-volume-up-205-year-on-year-in-h1-2024/ (Accessed 4 February 2025).

Akartuna, E.A., Johnson, S.D. and Thornton, A.E. (2023). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*, 36, pp.615–650. https://doi.org/10.1057/s41284-022-00356-z (Accessed 9 September 2025).

Akinrinola, O., Okoye, C.C., Ofodile, O.C. and Ugochukwu, C.E. (2024) Navigating and reviewing ethical dilemmas in ai development: strategies for transparency, fairness, and accountability. *GSC Advanced Research and Reviews*, 18(3), pp.050–058. https://doi.org/10.30574/gscarr.2024.18.3.0088 (Accessed 11 April 2025).

Akter, S., Mccarthy, G., Sajib, S., Michael, K., Dwivedi, Y. K., D'Ambra, J. and Shen, K. N. (2021) Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management*, 60, 102387.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Al Sadawi, A., Hassan, M.S. and Ndiaye, M. (2022) On the integration of blockchain with IoT and the role of oracle in the combined system: *The full picture. IEEE Access*, 10, pp.92532–92558.

Al-Badran, O.R.A (2021) The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal*, 27(6), pp.1–10.

Aldama-Navarrete, D. (2021) Dark banking? Banks and illicit deposit flows. Federal Reserve Bank of Richmond. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811752. (Accessed 8 July 2025).

Alexandre, C. R. and Balsa, J. (2023) Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, 217, 119500.

Ali, V., Norman, A.A. and Azzuhri, S.R.B (2023) Characteristics of blockchain and its relationship with trust. *IEEE Access*, 11, pp.15364–15374.

Almasoud, A.S. and Idowu, J.A. (2024) Algorithmic fairness in predictive policing. *AI and Ethics*, 2025(5), pp.2323–2337.

Almeda, M., Garrett, P. and Zuboff, S. (2021) *Public expectations and the deployment of AI in law enforcement*. Cambridge: Centre for AI and Society.

Almeida, D., Shmarko, K. and Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of AI: a comparative analysis of US, EU, and UK frameworks. *AI and Ethics*, 2(3), pp.377–387.

Alon-Barkat, S. and Busuioc, M (2023) Human–AI interactions in public sector decision making: 'automation bias' and 'selective adherence' to algorithmic advice. *Journal of Public Administration Research and Theory*, 33(1), pp.153–169.

Alstadsæter, A., Casi, E., Miethe, J. and Stage, B. (2023) Lost in information: national implementation of global tax agreements. NHH Dept. of Business and Management Science Discussion Paper (2023/22).

Amini, A., Soleimany, A.P., Schwarting, W., Bhatia, S.N. and Rus, D. (2019) Uncovering and mitigating algorithmic bias through learned latent structure. In Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, pp.289–295.

Amnesty (2025) *Automated racism: How police data and algorithms code discrimination into policing*. www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf (Accessed 25 August 2025).

Apple (2025) *Apple's first spatial computer*. www.apple.com/uk/newsroom/2023/06/introducing-apple-vision-pro/ (Accessed 1 April 2025).

Arner, D.W., Barberis, J.N. and Buckley, R.P (2025) The evolution of Fintech: a new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), pp.1271–1292.

Arreche, O., Guntur, T. and Abdallah, M. (2024) XAI-IDS: toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems. *Applied Sciences*, 14(10), pp. 4170.

Arshad, J., Talha, M., Saleem, B., Shah, Z., Zaman, H. and Muhammad, Z. (2024) A survey of bug bounty programs in strengthening cybersecurity and privacy in the blockchain industry. *Blockchains*, 2(3), pp.195–216.

Arts, J. and Marguerite (2024). What the Dutch Benefits Scandal and Policy's Focus on "Fraud" Can Teach US about the Endurance of Empire. Critical Social Policy.

Ashfaq, A. (2022) Application of Blockchain Technology & IoT Based Smart Sensors in Supply Chain Management via Business Development Approach. https://webthesis.biblio.polito.it/22542/ (Accessed 8 July 2025).

Ates, L., Knobel, A., Lorenzo, F. and Meinzer, M. (2025a) Competition and complementarity of EU and FATF beneficial ownership transparency orders, in Mosquera Valderrama, I.J. et al. (eds.) *Redefining Global Governance*. Cham: Springer Nature Switzerland, pp.85–96.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Ates, L., Knobel, A., Lorenzo, F. and Meinzer, M. (2025b) The transnational legal ordering of beneficial ownership registration. *Transnational Legal Theory*, 16(3), pp.451–476. www.tandfonline.com/doi/abs/10.1080/20414005.2025.2471184. (Accessed 8 July 2025).

Auer, R., Böhme, R., Clark, J. and Demirag, D. (2025) Privacy-enhancing technologies for digital payments: mapping the landscape. www.bis.org/publ/work1242.htm. (Accessed 8 July 2025).

AUSTRAC & Australian Government (2020) *Assessing ML-TF Risk*. www.austrac.gov.au/sites/default/files/2020-08/AUSTRAC%20Insights%20-%20Assessing%20-ML-TF%20Risk.pdf (Accessed 8 July 2025).

Avgouleas, E. and Seretakis, A. (2023) How should crypto lending be regulated under EU law? *European Business Organization Law Review*, 24(3), pp.421–438.

Aziz, L.A.R. and Andriansyah, Y. (2023) The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), pp.110–132. https://core.ac.uk/download/pdf/578755756.pdf (Accessed 11 April 2025).

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

Balcıoğlu, Y.S. (2024) Revolutionizing Risk Management AI and ML Innovations in Financial Stability and Fraud Detection. In Navigating the Future of Finance in the Age of AI. in Pandow, B. A., Masoodi F. S., Iqbal J., and Hussain G. (eds) Navigating the Future of Finance in the Age of AI, Business Science Reference, pp.109–138.

Bank of England (2022) Machine learning in UK financial services. 11 October. www.bankofengland.co.uk/Report/2022/machine-learning-in-uk-financial-services?utm_source=chatgpt.com (Accessed 11 April 2025).

Bank of England (2024) Resolvability assessment of major UK banks: 2024. 6 August. www.bankofengland.co.uk/financial-stability/resolution/resolvability-assessment-framework/resovability-assessment-of-major-uk-banks-2024 (Accessed 11 April 2025).

Bank of England (2025) Financial Stability in Focus: Artificial intelligence in the financial system. Available at: www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025 (Accessed 11 April 2025).

Bank of England and FCA (2024) Artificial intelligence in UK financial services – 2024. Available at: www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024 (Accessed 11 April 2025).

Banks, J. (2014) *Online Gambling and Crime: Causes, Controls and Controversies*. 1st ed. London: Routledge. Available at: https://doi.org/10.4324/9781315598918.

Barabas, C. (2020) Beyond bias: "Ethical AI" in criminal law. In Dubber M., Pasquale F. and Das S. eds., *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press, pp.737–753.

Barclays (2024) From intelligence to ability: how Barclays is harnessing AI. Available at: https://home.barclays/news/2024/01/how-Barclays-is-harnessing-AI/ (Accessed 11 April 2025).

Barocas, S. and Selbst, A.D. (2016) Big data's disparate impact, *California Law Review*, 104, pp.671–732. Available at: https://ssrn.com/abstract=2477899 (Accessed 26 May 2025).

Barocas, S., Hardt, M. and Narayanan, A. (2023) *Fairness and Machine Learning: Limitations and Opportunities*, vol 1, 1st edn, Cambridge, MA: MIT Press.

Basic, G. and Yakhlef, S. (2022) Anomie and collaboration in intelligence and operational police and border guard work in the Baltic Sea area: in-group mentality and construction of the other, *Policing and Society*, 32(9), pp.1103–1123.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Basu, D. and Tetteh, G.K. (2024) Using automation and AI to combat money laundering, Financial Regulation Innovation Lab. Available at: www.strath.ac.uk/media/departments/accountingfinance/fril/whitepapers/Using_Automation_and_AI_to_Combat_Money_Laundering.pdf (Accessed 22 May 2025).

Becker, W. and Saisana, M. (2018) The JRC Statistical Audit of the Financial Secrecy Index 2018. Joint Research Centre of the European Commission. Available at: https://knowledge4policy.ec.europa.eu/sites/default/files/jrc_statistical_audit_of_the_financial_secrecy_index_2018.pdf (Accessed 9 September 2025).

Bello, A. U. and Harvey, J. (2017) From a risk-based to an uncertainty-based approach to anti-money laundering compliance, *Security Journal*, 30(1), pp.24–38.

Benson, V., Adamyk, B., Chinnaswamy, A. and Adamyk, O. (2024) Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. *European Journal of Law and Economics*, 57(1), pp.37–61.

Benson, V., Turksen, U. and Adamyk, B (2023) Dark side of decentralised 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.

Berger, P. (2021) The EU Digital Finance Package. DLA Piper. Available at: www.dlapiper.com/es-pr/insights/publications/2021/01/the-eu-digital-finance-package (Accessed 8 July 2025).

Birdi, K., Griffiths, K., Turgoose, C. and Vonaş, G. (2021) Factors influencing cross-border knowledge sharing by police organisations: an integration of ten European case studies, *Police Practice and Research*, 22(1), pp.3–22.

Bitcoin.org (n.d.) *Bitcoin – Open source P2P money*. Available at: https://bitcoin.org/en/ (Accessed 13 April 2025).

Block, L. (2008) Combating organized crime in Europe: Practicalities of police cooperation, *Policing*, 2(1), pp.74–81.

Block, L. (2010) Bilateral police liaison officers: Practices and European policy, *Journal of Contemporary European Research*, 6(2), pp.194–210.

Bogina, V. et al. (2021) Educating software and AI stakeholders about algorithmic fairness, accountability, transparency and ethics. *International Journal of Artificial Intelligence in Education*, 32. Available at: https://doi.org/10.1007/s40593-021-00248-0 (Accessed 11 April 2025).

Bomare, J., and Le Guern Herry, S. (2022) Will We Ever Be Able to Track Offshore Wealth? Evidence from the Offshore Real Estate Market in the UK (Working Paper No. 4), EU Tax Observatory. Available at: www.taxobservatory.eu/publication/will-we-ever-be-able-to-track-offshore-wealth-evidence-from-the-offshore-real-estate-market-in-the-uk/ (Accessed 4 February 2025).

Borlini, L. and Montanaro, F. (2017) The evolution of the EU law against criminal finance: the "hardening" of FATF standards within the EU, *Georgetown Journal of International Law*, 48(4), pp.1009–1062.

Boyer, P. C. and Kempf, H (2020) Regulatory arbitrage and the efficiency of banking regulation, *Journal of Financial Intermediation*, 41, 100765.

Bravyi, S. et al. (2022) The future of quantum computing with superconducting qubits, *Journal of Applied Physics*, 132(6: 160902).

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. Available at: https://infobrics.org (Accessed 1 April 2025).

Brown, M. (2024) Influence of artificial intelligence on credit risk assessment in banking sector, *International Journal of Modern Risk Management*, 2(1), pp.24–33. Available at: https://doi.org/10.47604/ijmrm.2641 (Accessed 11 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Browne, T.O., Abedin, M. and Chowdhury, M.J.M. (2024) A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications, *International Journal of Information Security*, 23, pp.2911–2938.

Buckley, P. R., Arner, W. D. and Zetzsche, A. D. (2024) *FinTech: Finance, Technology and Regulation – Introduction*, vol 1, 1st ed. Cambridge: Cambridge University Press. Available at: https://doi.org/10.2139/ssrn.448605 (Accessed 23 March 2025).

Buijsman, S., Klenk, M. and Van Den Hoven, J. (2025) Toward a "Design for Values" Approach. In Smuha N. ed., The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Cambridge: Cambridge University Press, pp.59–78.

Burrell, J. (2016) How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), pp.1–12.

Burton, J., Janjeva, A., Moseley, S. and Alice (2025) *AI and Serious Online Crime*. CETaS Research Reports, March. Available at: https://cetas.turing.ac.uk/publications/ai-and-serious-online-crime (Accessed 26 May 2025).

Calvery, J. (2024) Harnessing the power of AI to fight financial crime. HSBC Views. Available at: https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime (Accessed 23 April 2026).

Camargo, A.M. (2023) Integrating blockchain into global finance: a case study of SWIFT's strategic collaboration with Chainlink. *Revista de Gestão e Secretariado*, 14 (12), pp.21723–21738.

Cardao-Pito, T. (2022) An embezzler test for norms, standards and regulations, *Journal of Financial Crime*, 29(3), pp. 878–889.

Cardenas, S. and Vallejo-Cardenas, S.F. (2019) Continuing the conversation on how structural racial and ethnic inequalities affect AI biases. In 2019 IEEE International Symposium on Technology and Society (ISTAS), pp.1–7.

Carlisle, D. (2023) *The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond*. Chichester: Wiley.

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.

Casey, E. (2011) *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Waltham: Academic Press.

Cassetta, A., Pauselli, C., Rizzica, L. and Tonello, M (2014) Exploring Flows to Tax Havens Through Means of a Gravity Model: Evidence from Italy, Rome. Available at: https://papers.ssrn.com/abstract=2575647 (Accessed 8 July 2025).

Cellebrite (n.d.) Cellebrite – Digital Intelligence for a Safer World. Available at: www.cellebrite.com (Accessed 13 April 2025).

CEN-CENELEC (2025) Artificial Intelligence. CEN-CENELEC. Available at: www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/ (Accessed 23 April 2026).

Central Banking Staff (2022) Data quality and staff skills are greatest AI challenges – benchmark respondents. Benchmarking, 24 February. Available at: https://www.centralbanking.com/benchmarking/fintech/7932271/data-quality-and-staff-skills-are-greatest-ai-challenges-benchmark-respondents (Accessed 23 April 2016).

CEPOL (2019) Digital data - Now and tomorrow. European Union Agency for Law Enforcement Training, 9 July. Available at: https://www.cepol.europa.eu/newsroom/partners-news/digital-data-now-and-tomorrow (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Chainalysis (2020) DeFi Regulation and Compliance Requirements Remain Unclear. *Chainalysis*. Available at: www.chainalysis.com/blog/defi-regulation-compliance/ (Accessed 11 April 2025).

Chang, W.L. and Benson, V. (2023) Migration and financial transactions: factors influencing mobile remittance service usage in the pandemic. *Information Technology & People*, 36(5), pp.2112–2136.

Charniak, E. and Mcdermott, D. (2nd ed., 1991) *Introduction to Artificial Intelligence*. Reading, MA: Addison-Wesley.

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

Charter of Fundamental Rights of the European Union (2000/C 364/01).

Chataut, R., Nankya, M. and Akl, R. (2024) 6 G Networks and the AI revolution: Exploring technologies, applications, and emerging challenges, *Sensors*, 24, p.1888.

Chaudhary, P.S., Khurana, M.R. and Ayalasomayajula, M. (2024) Real-world applications of data analytics, big data, and machine learning. In P. Singh, et al., eds. *Data Analytics and Machine Learning. Studies in Big Data*, vol.145. Springer, pp.237–263.

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K. and Lam, K. S. (2018) 'Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review', *Knowledge and Information Systems*, 57(2), pp.245–285.

Cheng, D., et al. (2025) Graph neural networks for financial fraud detection: a review. *Frontiers of Computer Science*, 19, Article 199609.

Choi, N. and Kim, H. (2025) Technological convergence of blockchain and artificial intelligence: a review and challenges. *Electronics*, 14(1), 84. https://doi.org/10.3390/electronics14010084 (Accessed 13 October 2025).

Chowdhary, K.R. and Chowdhary, K.R. (2020) *Introducing Artificial Intelligence: Fundamentals of Artificial Intelligence*. New Delhi: Springer. pp.1–23.

Chugani, S.H. (2008) Benevolent blood money: Terrorist exploitation of Zakat and its complications in the war on terror. *North Carolina Journal of International Law and Commercial Regulation*, 34, p.601.

Clarke, A. (2023) Unleashing the Power of AI in Decentralized Finance: Opportunities and Challenges. Available at: www.nasdaq.com/articles/unleashing-the-power-of-ai-in-decentralized-finance-opportunities-and-challenges (Accessed 9 September 2025).

Clements, R. (2021) Built to fail: The inherent fragility of algorithmic stablecoins. *Wake Forest Law Review Online*, 11, p.131.

Cobham, A., Janský, P. and Meinzer, M. (2015) The Financial Secrecy Index: Shedding new light on the geography of secrecy. *Economic Geography*, 91(3), pp. 281–303.

Cobwebs (2020) Web Forensics for Tackling Terrorism Investigation. Available at: www.cobwebs.com/wp-content/uploads/2020/01/Web-Forensics-for-Tackling-Terrorism-Investigation-White-Paper.pdf (Accessed 26 March 2025).

Colorado General Assembly, 2024. *SB24-205 Consumer Protections for Artificial Intelligence: Concerning consumer protections in interactions with artificial intelligence systems*. (online) 17 May. Available at: https://leg.colorado.gov/bills/sb24-205 (Accessed 8 July 2025).

Companies House (2023) Companies House. (online) GOV.UK. Available at: www.gov.uk/government/organisations/companies-house (Accessed 4 March 2025).

Complete Professional Services, LLC. (CPS IT Solutions), 2016. FFIEC BSA/AML Assessing Compliance with BSA Regulatory Requirements – Beneficial Ownership Requirements for Legal Entity Customers. (online) Ffiec.gov. Available at: https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/03 (Accessed 4 February 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Congressional Research Service (2023) *Law Enforcement Use of Artificial Intelligence and Directives in the 2023 Executive Order*. (online) Available at: https://crsreports.congress.gov/product/pdf/IN/IN12289 (Accessed 8 July 2025).

Cotter, R.S. (2017) Police intelligence: connecting-the-dots in a network society. *Policing and Society*, 27(2), pp. 173–187.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Treaty) OJ L 210, 6 8.2008, pp. 1–11.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') OJ L 283, 31.10.2017, pp. 1–71.

Council of Europe (n.d.) Financing of terrorism. Available at: www.coe.int/en/web/moneyval/implementation/financing-terrorism (Accessed 24 June 2022).

Council of Europe (2017) Algorithms and Human Rights. Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications. Study prepared by the Committee of Experts on Internet Intermediaries (MSI-NET).

Council of the EU (2022) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach. Available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.

Court of Binder Dijker Otte (2022) Justice of the European Union: Ruling on public access to beneficial ownership registers. Available: https://www.bdo.global/en-gb/microsites/tax-newsletters/global-tax-alerts/european-union-cjeu-ends-open-public-access-to-ubo-register (Accessed 23 April 2026).

Crawford, K. (2021) *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. London: Yale University Press.

Creswell, J. W. and Tashakkori, A. (2007) Differing perspectives on mixed methods research. *Journal of Mixed Methods Research* 1(4), pp.303–308.

CS Global Partners (2025) Rising Interest in Caribbean Citizenship by Investment Programmes among Wealthy Americans. (online) CS Global Partners Limited. Available at: https://csglobalpartners.com/news/rising-interest-in-caribbean-citizenship-by-investment-programmes-among-wealthy-americans/ (Accessed 4 February 2025).

CSIS (2024) Significant Cyber Incidents. Available at: www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Accessed 1 April 2025).

Cusack, J. (2022) 'Financial Crime Bank Fines in the 21st Century', Financial Crime News. Available at: http://thefinancialcrimenews.com/financial-crime-bank-fines-in-the-21st-century-by-fcn/ (Accessed 8 July 2025).

Cyber Management Alliance (2025) Top 10 Biggest Cyber Attacks of 2024 & 25, 20 January.

d Young D. (2024) *Are fraudsters (soul)bound to fail? An overview of soulbound tokens and their use in fighting fraud*. Available at: www.penningtonslaw.com/insights/are-fraudsters-soulbound-to-fail-an-overview-of-soulbound-tokens-and-their-use-in-fighting-fraud/ (Accessed 9 September 2025).

Dafoe, A. (2024) 'AI Governance: Overview and Theoretical Lenses'. In: J.B. Bullock, et al. (eds) *The Oxford Handbook of AI Governance*. Oxford Handbooks. (online) Oxford Academic. Available at: https://doi.org/10.1093/oxfordhb/9780197579329.013.2 (Accessed 23 March 2025).

Dalla Pellegrina, L. and Masciandaro, D (2009) The risk-based approach in the new European anti-money laundering legislation: A law and economics view. *Review of Law and Economics*, 5(2), pp. 931–952.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Darktrace, 2024. AI for Cybersecurity and Threat Detection. (online) Darktrace. Available at: www.darktrace.com (Accessed 4 April 2025).
Dash.org, n.d. Dash – Digital Cash. Available: https://www.dash.org (Accessed 23 April 2026).
Datta, P., Whitmore, M. and Nwankpa, J.K (2021) A perfect storm: Social media news, psychological biases, and AI. *Digital Threats: Research and Practice* 2(2), pp.1–21.
Davenport, T. and Ronanki, R (2018) Artificial intelligence for the real world. *Harvard Business Review*, January–February. Available: https://hbr.org/2018/01/artificial-intelligence-for-the-real-world (Accessed 23 April 2026).
David, M. (2023) *Networked Crime: Does the Digital Make the Difference?* (1st ed.). Bristol: Bristol University Press.
Davenport, T.H. and Ronanki, R., 2018. Artificial intelligence for the real world. Harvard Business Review (online).
Davis, J., Purves, D., Gilbert, J., and Sturm, S. (2022) Five ethical challenges facing data-driven policing. *AI and Ethics* 2(1), pp.185–198.
De Gregorio, G. and Dunn, P. (2022) The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, 59(2), pp.473–500.
De Sanctis, F.M. (2019) *Technology-Enhanced Methods of Money Laundering: Internet as Criminal Means*. Cham, Switzerland: Springer.
De Silva, C. (2025) *Advancing Financial Risk Management: AI-Powered Credit Risk Assessment through Financial Feature Analysis and Human-Centric Decision-Making*. MDPI AG. Available at: https://www.preprints.org/manuscript/202502.2059 (Accessed 23 April 2026).
Dean, S. and Waris, A. (2021) Ten truths about tax havens: Inclusion and the "Liberia" problem. *Emory Law Journal*, 70(7). Available at: https://papers.ssrn.com/abstract=3822421. (Accessed 8 July 2025).
Dearing, T. (2025) How AI Is Helping Hackers Hunt for Weaknesses. Securityinfowatch.com. Available at: www.securityinfowatch.com/ai/article/55291093/how-ai-is-helping-hackers-hunt-for-weaknesses (Accessed 23 April 2026).
De Koker, L. (2024) Editorial: FATF greylisting: time to revisit the approach. *Journal of Money Laundering Control*, 27(4), pp. 621–624.
Department for Science, Innovation and Technology (2024). *A pro-innovation approach to AI regulation: government response* (online). Available at: www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response (Accessed 8 July 2025).
Devarajulu, V.S. (2022) Expert take on AI-augmented cybersecurity measures in financial institutions. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 1(3), pp. 1220–1222.
Dewald, S. (2022) Detectives and technological frames: Integrating technology and social media into everyday work. *Policing and Society*, 33, p.111.
De Koker, L. (2009) Identifying and managing low money laundering risk: Perspectives on FATF's risk-based guidance. *Journal of Financial Crime*, 16(4), pp. 334–352.
Dick, S. (2019) Artificial intelligence. *Harvard Data Science Review*, 1(1). Available at: https://hdsr.mitpress.mit.edu/pub/0aytgrau/release/3 (Accessed 23 April 2026).
Dioquino, V. (2025) Real World Asset Tokenization to Hit $50B in 2025: Ozean. Decrypt. Available at: https://decrypt.co/301222/real-world-asset-tokenization-to-hit-50b-in-2025-ozean (Accessed 13 October 2025).
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA OJ L 88, 31.3.2017, pp. 6–21.

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on Combating Money Laundering by Criminal Law (2018) OJ L284/22.

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA PE/64/2019/REV/1 OJ L 186, 11.7.2019, pp. 122–137.

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings PE/3/2023/REV/1 OJ L 191, 28.7..2023, pp. 181–190.

Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA PE/70/2022/REV/2 OJ L 134, 22.5.2023, pp. 1–24.

Divyashree, K.S. and Mishra, A (2025) Blockchain and IoT integration for financial sector revolution. In: Chowdhary, C.L., Tripathy, A.K., Wu, Y. (eds.) *Smart Computing Techniques in Industrial IoT. Studies in Computational Intelligence*, vol. 1172. Singapore: Springer.

Dixon, A. and Birks, D. (2021) 'Improving Policing with Natural Language Processing', in Proceedings of the 1st Workshop on NLP for Positive Impact, NCL Anthology, pp. 115–124 Available at: https://aclanthology.org/2021.nlp4posimpact-1.13/ (Accessed 23 April 2026).

Doddipatla, L. (2024) Ethical and regulatory challenges of using generative AI in banking: Balancing innovation and compliance. *Educational Administration: Theory and Practice*, 30, p.2848.

Dolar, B. and Shughart, W.F. (2011) Enforcement of the USA Patriot Act's anti-money laundering provisions: Have regulators followed a risk-based approach? *Global Finance Journal*, 22(1), pp. 19–31.

Dorwart, C., Lu, X. and Tang, Y. (2025) *China's AI Governance Landscape: A Comparative Study*. Beijing: China AI Policy Research Institute.

Dorwart, H., Qu, H., Brautigam, T. and Gong, J. (2025) Preparing for compliance: Key differences between EU, Chinese AI regulations. Available at: https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations (Accessed 23 April 2026).

Drage, E. and Frabetti, F. (2024) The performativity of AI-powered event detection: How AI creates a racialized protest and why looking for bias is not a solution. *Science, Technology, & Human Values*, 49(5), pp.1045–1072.

Drezner, D.W. (2001) Globalization and policy convergence. *International Studies Review*, 3, pp.53–78.

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.A. and Scanlon, M. (2020) SoK: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In Proceedings of the 15th ARES International Conference on Availability, Reliability and Security, Cornell University, Computer Science, pp.1–10. Available at: https://arxiv.org/abs/2012.01987 (Accessed 23 April 206).

Dubravova, H., Cap, J., Holubova, K. and Hribnak, L. (2024) Artificial intelligence as an innovative element of support in policing. *Procedia Computer Science*, 237, pp.237–244.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Dun & Bradstreet (2011) Dun & Bradstreet – Accelerate Growth and Improve Business Performance. (online) Dnb.co.uk. Available at: www.dnb.co.uk/ (Accessed 4 March 2025).

Durodola, L.O. (2021) Towards a responsible use of artificial intelligence. In Lui, A., & Ryder, N. (eds.) *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention* (1st ed.). London: Routledge. Available at: https://doi.org/10.4324/9781003020998 (Accessed 12 March 2025).

Durodola, O. (2024) 'Artificial Intelligence in Global Financial Institutions Based in the United Kingdom: Ethico-Legal, Corporate Governance and Social Responsibility Perspectives'. PhD Thesis.

Dwivedi, K.Y., et al. (2021) Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy. *International Journal of Information Management*, 57, 101994.

ECORYS (2021) Monitoring the amount of wealth hidden by individuals in international financial centres and impact of recent internationally agreed standards on tax transparency on the fight against tax evasion. Brussels: European Commission DG TAXUD.

EU AI Act (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), Article 6. (online) Available at: https://artificialintelligenceact.eu/article/6/ (Accessed 15 April 2025).

Europol (2017) From Suspicion to Action: Converting financial intelligence into greater operational impact. Available at: www.europol.europa.eu/cms/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf. (Accessed 8 July 2025).

Europol (2020) Beyond the pandemic: how COVID-19 will shape the serious and organised crime landscape in the EU. Available at: www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know (Accessed 27 March 2025).

Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA). Available at: www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (Accessed 19 March 2025).

Europol (2021) Shadow Money: The International Networks of Illicit Finance. Available at: www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf. (Accessed 8 July 2025).

Europol (2023) Internet Organised Crime Threat Assessment (IOCTA). Available at: www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment (Accessed 28 March 2025).

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

Ebers, M. (2022) Standardizing AI. The case of the European Commission's proposal for an 'Artificial Intelligence Act'. In Di Matteo L.A., Poncibò C. and Cannarsa M. eds., *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*. Cambridge: Cambridge University Press, pp.321–344.

Ekundayo, F. (2024) Economic implications of ai-driven financial markets: challenges and opportunities in big data integration. *International Journal of Science and Research Archive*, 13(02), pp.1500–1515.

El Hajj, M. and Hammoud, J. (2023) Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. *Journal of Risk and Financial Management*, 16, p.434.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

El Mestari, S.Z., Lenzini, G. and Demirci, H. (2024) Preserving data privacy in machine learning systems. *Computers & Security* 137, p. 103605. https://doi.org/10.1016/j.cose.2023.103605 (Accessed 9 September 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.

Emehin, O., Emeteveke, I., Adeyeye, O.J. and Akanbi, I., 2024. Generative AI in forensic data analysis: Opportunities and ethical implications for cloud-based investigations. *International Journal of Research Publication and Reviews*, 5(10), pp.2941–2957.

Erken, E. and Turksen, U (2024) *Anti-Money Laundering and the Law: Comparative Approaches to Countering Predicate Crimes*. London: Routledge. European Commission (n.d.1) 'Information exchange'.

Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Euronews (2024) 'What is "spatial computing" and why is Apple pushing the new buzzword?' Available at: https://www.euronews.com/next/2024/02/05/what-is-spatial-computing-and-why-is-apple-pushing-the-new-buzzword (Accessed 22 May 2025).

European Agency for Fundamental Rights (Fra) (2022) The Fundamental Rights Report 2022.

European Banking Authority (2021) Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions. Available at: www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf. (Accessed 8 July 2025).

European Banking Authority (2024) *Special topic: Artificial intelligence*. European Banking Authority. Available at: https://www.eba.europa.eu/publications-and-media/publications/special-topic-artificial-intelligence (Accessed 23 April 2026).

European Commission (2012) Online gambling in the Internal Market, SWD (2012) 345 final. European Commission (2017) Commission Staff Working Document: Risks of Money Laundering and Terrorist Financing, SWD (2017) 241 Final, pp.124–128.

European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. COM/2021/420 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420 (Accessed 8 July 2025).

European Commission (2022) Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554. (Accessed 8 July 2025).

European Commission (2024) COM (2021) 784: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"). Available at: https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:32024R0982 (Accessed 23 April 2026).

European Commission (2025) 'Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act'. (Shaping Europe's digital future, February 4, 2025.) Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (Accessed 23 April 2026).

European Commission (n.d.2) 'European Criminal Records Information System (ECRIS)'. Available at: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en (Accessed 23 April 2026).
European Commission (n.d.3) 'E-evidence – cross-border access to electronic evidence'. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0590R(01) (Accessed 23 April 2026).
European Commission (2021) EUR-Lex – 52021PC0206 – EN. (online) EUR-Lex. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206 (Accessed 4 February 2025).
European Commission (2021) Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. (online) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (Accessed 4 February 2025).
European Commission (2023) Investor Citizenship and Residence Schemes in the EU. (online) Available at: https://ec.europa.eu (Accessed 1 April 2025).
European Commission (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). (online) Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Accessed 15 April 2025).
European Commission (2024) The EU's Anti-Money Laundering Authority: Stronger Rules to Fight Financial Crime. Available at: https://ec.europa.eu/info/publications/eu-anti-money-laundering-authority_en (Accessed 21 May 2025).
European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM (2021) 206 final. 2021/0106 (COD). Available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.
European Commission (2025a) Annex to the Communication to the Commission. Approval of the Content of the Draft Communication from the Commission – Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (Eu) 2024/1689 (Ai Act). C (2025) 924 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (Accessed 23 April 2026).
European Commission (2025b) Annex to the Communication to the Commission. Approval of the Content of the Draft Communication from the Commission – Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act). C (2025) 884 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (Accessed 23 April 2026).
European Council (2022) Taxes in Europe Database v2. European Commission. Available at: https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax (Accessed 24 June 2022).
European Council (2023) Council adopts EU laws on better access to electronic evidence. Press Release. Available at: www.consilium.europa.eu/en/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/ (Accessed 19 March 2025).
European Council (2024) Better access to e-evidence to fight crime, 11 January. Available at: www.consilium.europa.eu/en/policies/e-evidence/ (Accessed 19 March 2025).
European Council (2024) 'Anti-money laundering: Council adopts package of rules', Press Release, 30 May. Available at: www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/ (Accessed 8 July 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

European Council (n.d.) Taxes in Europe Database v2. Available at: https://ec.europa.eu/taxation_customs/tedb/legacy/taxDetail.html?id=134/1424159159&taxType=Other+indirect+tax (Accessed 24 June 2022).
European Court of Human Rights (ECtHR) (2024) Guide on Article 6 of the European Convention on Human Rights. Right to a fair trial (criminal limb). Available at: https://ks.echr.coe.int/web/echr-ks/all-case-law-guides (Accessed 23 April 2026).
European Parliament (2023) Lessons learnt from the Pandora Papers and other revelations (Resolution No. P9_TA (2023)0249). Brussels: European Parliament. Available at: www.europarl.europa.eu/doceo/document/TA-9-2023-0249_EN.pdf. (Accessed 8 July 2025).
European Parliament (2023) Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)).
European Parliament and Council (2024) Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Available at: http://data.europa.eu/eli/dir/2015/849/2021-06-30/eng. (Accessed 8 July 2025).
European Parliament and Council (2024) Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Available at: http://data.europa.eu/eli/reg/2024/1624/oj/eng. (Accessed 8 July 2025).
European Parliament and Council (2016) Directive (EU) 2016/680 of 27 April 2016 (Law Enforcement Directive). Official Journal of the European Union, L119/89.
European Parliament and Council (2016) Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119.
European Parliament and Council (2024) Regulation (EU) 2024/1689 of 13 June 2024 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.
European Parliament (2023) EU AI Act: First Regulation on Artificial Intelligence. (online) Available at: www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (Accessed 4 February 2025).
European Parliament (2024) United States approach to artificial intelligence. (online) Available at: www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf (Accessed 8 July 2025).
European Parliament (2021) Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2021(INI)). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_132_R_0003 (Accessed 23 April 2026).
European Parliamentary Research Service (2017) Die Kapazität der Mitgliedstaaten zur Bekämpfung von Steuerstraftaten: Ex post Folgenabschätzung. Available at: https://data.europa.eu/doi/10.2861/9432 (Accessed 10 May 2022).
European Police Chiefs (2022) Joint Declaration on the AI Act (as approved by the European Police Chiefs during their informal meeting in Berlin on 24 May 2022).
European Union (2023) High risk third countries and the international context content of anti-money laundering and countering the financing of terrorism. Available at: https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en (Accessed 23 April 2026).
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. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (Accessed 18 March 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

European Union (n.d.4) Stepping up cross-border cooperation – the Prüm decision. EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:jl0005 (Accessed 26 May 2025).
European Union Agency for Fundamental Rights (2020) Getting the future right. Artificial intelligence and fundamental rights. Available at: https://fra.europa.eu/en/publication/2020/artificialintelligence-and-fundamental-rights (Accessed 23 April 2026).
European Union and United Kingdom (2019) Agreement on the withdrawal of the UK from the EU. Official Journal of the European Union, C 384 I/01.
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).
Europol (2020e) Malicious uses and abuses of artificial intelligence. European Cybercrime Centre (EC3). Available at: www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf (Accessed 26 May 2025).
Europol (2024d) AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Europol Innovation Lab. Available at: www.europol.europa.eu/publication-events/main-reports/ai-and-policing (Accessed 26 May 2025).
Europol (2025) *European Union Serious and Organised Crime Threat Assessment: The Changing DNA of Serious and Organised Crime*. Luxembourg: Publications Office of the European Union.
Europol (2025) *Assessing Technologies in Law Enforcement. A Method for Ethical Decision-Making*. Luxembourg: Publications Office of the European Union.
Europol (2016) Does crime still pay? Criminal Asset Recovery in the EU. (online) Available at: www.europol.europa.eu/cms/sites/default/files/documents/criminal_asset_recovery_in_the_eu_web_version.pdf (Accessed 9 June 2025).
Europol (2020a) Europol launches the European Financial and Economic Crime Centre. (online) Available at: www.europol.europa.eu/media-press/newsroom/news/europol-launches-european-financial-and-economic-crime-centre (Accessed 9 June 2025).
Executive Office of the President (2019) Maintaining American Leadership in Artificial Intelligence. Federal Register, 11 February. (online) Available at: www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence (Accessed 8 July 2025).
Executive Office of the President (2023) Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Federal Register, 30 October. (online) Available at: www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (Accessed 8 July 2025).
Executive Office of the President (2025) Strengthening and Promoting Innovation in the Nation's Cybersecurity. Federal Register, 16 January. (online) Available at: www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity (Accessed 8 July 2025).
Ezeh, A., Widgery, M. and Canada, K. (2025) *AI Technologies in US Law Enforcement*. Washington, DC: National Institute of Justice.
Ezeh, N., Widgery, A. and Canada, C. (2025) Artificial Intelligence and Law Enforcement: The Federal and State Landscape. NCSL. (online) Available at: www.ncsl.org/civil-and-criminal-justice/artificial-intelligence-and-law-enforcement-the-federal-and-state-landscape (Accessed 8 July 2025).
FATF (1990) *The Forty Recommendations of the Financial Action Task Force on Money Laundering*. Paris: Financial Action Task Force. Available at: www.fatf-gafi.org/media/fatf/

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf. (Accessed 8 July 2025).
FATF (2007) *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures*. Paris: FATF. Available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html (Accessed 8 July 2025).
FATF (2012) *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Paris: FATF. Available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. (Accessed 8 July 2025).
FATF (2012) Recommendation 10: Customer Due Diligence. (online) Available at: www.fatf-gafi.org/publications/fatfrecommendations/ (Accessed 4 February 2025).
FATF (2013) *National Money Laundering and Terrorist Financing Risk Assessment*. Paris: FATF. Available at: www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf. (Accessed 8 July 2025).
FATF (2019) *Anti-money Laundering and Counter-terrorist Financing Measures: Turkey Mutual Evaluation Report*. Paris: FATF. Available at: www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-Turkey-2019.pdf. (Accessed 8 July 2025).
FATF (2019) Terrorist Financing Risk Assessment Guidance. Available at: www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf (Accessed 22 May 2025).
FATF (2022) Money Laundering and Citizenship by Investment Programmes. (online) Available at: www.fatf-gafi.org (Accessed 4 February 2025).
FATF (2022) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2012 – Updated 2022). Paris: FATF. Available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
FATF (2024) FATF's Assessment of the United States. Available at: www.fatf-gafi.org/en/countries/detail/United-States.html. (Accessed 8 July 2025).
FATF (n.d.) FATF's Assessment of Luxembourg. Available at: www.fatf-gafi.org/en/countries/detail/Luxembourg.html. (Accessed 8 July 2025).
FATF-GAFI (2016) United States' measures to combat money laundering and terrorist financing. Available at: www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-United-States-2016.pdf.coredownload.inline.pdf. (Accessed 8 July 2025).
FATF-GAFI (2022) Report on the State of Effectiveness and Compliance with the FATF Standards. April. Available at: www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html (Accessed 23 April 2026).
FATF-GAFI (2003) The Forty Recommendations. Paris: FATF. Available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf. (Accessed 8 July 2025).
FBI (2024) Criminal Use of Generative Artificial Intelligence to Facilitate Financial Fraud. Public Service Announcement, Alert Number: I-120324-PSA, 3 December.
FCA (2022) PS22/9: A new Consumer Duty. Available at: https://www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty (Accessed 23 April 2026).
FCA (2025) Financial Crime Guide: A firm's guide to countering financial crime risks (FCG), April 2025. Available at: www.handbook.fca.org.uk/handbook/FCG.pdf (Accessed 25 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

FTSG (2025) 2025 Tech Trends Report. Available at: https://ftsg.com/wp-content/uploads/2025/03/FTSG_2025_TR_FINAL_LINKED.pdf (Accessed 23 April 2026).
Farber, H.B. and Vyas, A. (2025) Truth and technology: Deepfakes in law enforcement interrogations. *University of Pennsylvania Journal of Constitutional Law*, 27(5), pp.1–47.
Fauzi, F., Szulczyk, K. and Basyith, A. (2018) Moving in the right direction to fight financial crime: prevention and detection. *Journal of Financial Crime*, 25(2), pp.362–368.
Federal Department of Foreign Affairs (FDFA) (2025) Police cooperation (Prüm decisions). Available at: www.europa.eda.admin.ch/en/police-cooperation-prum-decisions (Accessed 26 May 2025).
Feedzai (2024) AI for Financial Crime Prevention. (online) Feedzai. Available at: www.feedzai.com (Accessed 4 April 2025).
Ferguson, A.G. (2024) Generative suspicion and the risks of AI-assisted police reports. *Northwestern Law Review* 120(2), pp.1–63.
Ferguson, A.G. (2024) Policing and artificial intelligence: The legal and ethical framework. *Stanford Law Review*, 76(2), pp.345–371.
Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M. and Criado, N. (2021) Bias and discrimination in AI: A cross-disciplinary perspective. *IEEE Technology and Society Magazine*, 40(2), pp.72–80.
Fiedler, I. (2014) Online gambling as a game changer to money laundering? In Ötsch, W.O. et al. (eds.) *The Political Economy of Offshore Jurisdictions*. Marburg: Metropolis Verlag, pp. 79–98.
Fiedler, I. et al. (2017) *Das Geldwäscherisiko verschiedener Glücksspielarten*. Wiesbaden: Springer. Available at: http://link.springer.com/10.1007/978-3-658-16625-0 (Accessed 28 March 2025).
Fiedler, I. et al. (2020) *Regulierung von Onlineglücksspielen*. Available at: https://doi.org/10.1007/978-3-658-29846-3 (Accessed 28 March 2025).
FinCEN (2024) FinCEN Year in Review for FY 2023. Washington DC: US Treasury. Available at: www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf (Accessed 23 April 2026).
FinCEN (2018) Customer Due Diligence Requirements for Financial Institutions, 31 CFR § 1010.230. (online) FinCEN.gov. Available at: www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule? (Accessed 4 February 2025).
Financial Conduct Authority (2025) Assessing and reducing the risk of Money Laundering Through the Markets (MLTM). Available at: www.fca.org.uk/publication/corporate/money-laundering-through-markets-review-january-2025.pdf (Accessed 22 May 2025).
Financial Times (2019) London properties worth £80m targeted in 'dirty money' probe, 29 May. Available at: www.ft.com/content/9b1a3e7a-814d-11e9-b592-5fe435b57a3b (Accessed 24 June 2022).
Finocchario, G. (2024) *AI Regulation in the UK: A Sector-Specific Approach*. London: Institute for Technology and Law.
Finocchiaro, G. (2024) The regulation of artificial intelligence. *AI & Society*, 39, pp.1961–1968.
Forbes (2018) Criminals are using your dream home to clean dirty money, 21 November. Available at: www.forbes.com/sites/vishalmarria/2018/11/21/criminals-are-filling-your-dream-home-with-dirty-money (Accessed 24 June 2022).
Forbes (2024) Detecting deepfakes: Fighting AI with AI, 6 August. Available at: www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/ (Accessed 31 March 2024).
Fosch-Villaronga, E., Poulsen, A., Søraa, R.A. and Custers, B.H.M. (2021) A little bird told me your gender: Gender inferences in social media. *Information Processing & Management*, 58(3), 102541.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Fouche, G. and Solsvik, T. (2019) Aluminum maker Hydro battles to contain ransomware attack. Reuters, 19 March. Available at: www.reuters.com/article/us-norsk-hydro-cyber/aluminum-maker-hydro-battles-to-contain-ransomware-attack-idUSKCN1R00NJ (Accessed 28 March 2025).

Franssen, V. and Berrendorf, A. (2021) The use of AI tools in criminal courts: Justice done and seen to be done? In Vermeulen, G., Peršak, N. and Recchia, N. eds., *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*. Antwerpen: Maklu, pp.199–224.

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

Frey, W.R., Patton, D.U., Gaskell, M.B. and Mcgregor, K.A (2020) Artificial intelligence and inclusion: Formerly gang-involved youth as domain experts for analysing unstructured twitter data. *Social Science Computer Review*, 38(1), pp.42–56.

Fritz-Morgenthal, S., Hein, B. and Papenbrock, J (2022) Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in Artificial Intelligence*, 5.

GDPR (2018) General Data Protection Regulation (GDPR). (online) Available at: https://gdpr-info.eu/ (Accessed 4 February 2025).

García Fresno, M. (2022) *Analiza, que no es poco: Herramientas para el Análisis de Operaciones de Blanqueo de Capitales y de Financiación del Terrorismo*. Madrid: Fundación Notariado. Fundación Notariado. Available at: https://www.fundacionnotariado.org/portal/-/analiza-que-no-es-poco-1 (Accessed 23 April 2026).

García Fresno, M. (2022) *Analiza, que no es poco: Herramientas para el Análisis de Operaciones de Blanqueo de Capitales y de Financiación del Terrorismo*. Madrid: Fundación Notariado. Available at: https://publicaciones.notariado.org/p/-papel-analiza-que-no-es-poco-2 (Accessed 4 March 2025).

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

Garud, S. (2025) AI-driven risk management in financial services from theory to practice in Smart Education. In Sorayyaei Azar, A., Gupta, S.K., Al Bataineh, K.B., Maurya, N. and Somani, P. (eds.) *Smart Education and Sustainable Learning Environments in Smart Cities*. Hershey, PA: IGI Global Scientific Publishing, pp. 77–92.

Gebru, T. (2020) Race and gender. In Dubber, M.D., Pasquale, F. and Das, S. (eds), *The Oxford Handbook of Ethics of AI* (online edn) Oxford Academic, 9 July.

Gentzel, M. (2021) Biased face recognition technology used by government: A problem for liberal democracy. *Philosophy & Technology*, 34(4), pp.1639–1663.

George, S. (2024) Finance 4.0: The Transformation of Financial Services in the Digital Age. *Partners Universal Innovative Research Publication*, 2(3), pp.104–125. https://doi.org/10.5281/zenodo.11666694 (Accessed 13 October 2025).

Gertenbach, W., Botha, J. and Leenen, L. (2024) A Proposed High-Level Methodology on how OSINT is Applied in Blockchain Investigations. In Van Niekerk, B. 19th International Conference on Cyber Warfare and Security: ICCWS 2024. Available at: https://books.google.co.uk/books?hl=en&id=WxAXEQAAQBAJ&pg=PA75 (Accessed 22 May 2025).

GetMonero.org (n.d.) Monero – Private Digital Currency. Available at: www.getmonero.org/ (Accessed 13 April 2025).

Ghai, B. and Mueller, K. (2022) D-bias: A causality-based human-in-the-loop system for tackling algorithmic bias. *IEEE Transactions on Visualization and Computer Graphics*, 29(1), pp.473–482.

Gless, S. (2020) AI in the courtroom: A comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, 51(2), pp.195–253.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Global Financial Integrity (2025) Illicit Financial Flows. Available at: https://gfintegrity.org/issue/illicit-financial-flows/ (Accessed 23 April 2026).

Goldbarsht, D. (2023) Leveraging AI to mitigate money laundering risks in the banking system. In Z. Bednarz and M. Zalnieriute (eds.), *Money, Power, and AI: Automated Banks and Automated States*. Cambridge: Cambridge University Press, pp.51–69.

González Fuster G. (2020) Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. Study requesttheby the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)656295 (Accessed 25 August 2025).

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

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

Gottschalk, S. (2023) International financial regulation of cryptoassets and asset-backed tokens. In Kim S-J. *Fintech, Pandemic, and the Financial System: Challenges and Opportunities*. Emerald Publishing Limited, pp.145–181.

Government of Malta (2023) Individual Investor Programme. (online) Available at: https://iip.gov.mt (Accessed 1 April 2025).

Government of Saint Kitts and Nevis (2023) Citizenship by Investment Unit. (online) Available at: www.ciu.gov.kn (Accessed 1 April 2025).

Grand View Research (2019) Online gambling market size, share & trends analysis report. Available at: www.grandviewresearch.com/industry-analysis/online-gambling-market (Accessed 28 March 2025).

Griffiths, K., Birdi, K., Andrei, D. and Mouhanna, C. (2016) Knowledge sharing practices and issues in policing contexts: a systematic review of the literature. *European Journal of Policing Studies*, 3(3), pp.267–291.

Grimmelikhuijsen, S. and Meijer, A (2022) Legitimacy of algorithmic decision-making: Six threats and the need for a calibrated institutional response. *Perspectives on Public Management and Governance*, 5(3), pp.232–242.

Grondona, V., Meinzer, M., Monkam, N., Schultz, A. and Villanueva, G. (2025) Which money to follow? Evaluating country-specific vulnerabilities to illicit financial flows. *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-024-09610-z.

Grosso, C. M., O'Brien, B., Taylor, A. and Woodworth, G. (2014) Race discrimination and the death penalty: An empirical and legal overview. In C. S. Lanier, R. Bohm, and J. Acker (eds.), *America's Experiment with Capital Punishment* (3rd ed.). Durham, NC: Carolina Academic Press, pp.525–576.

Guille, L. (2010) Policing in Europe: An ethnographic approach to understanding the nature of the cooperation and the gap between policy and practice. *Journal of Contemporary European Research*, 6(2), pp.257–272.

Gummadi, J.C.S (2023) IoT security in the banking sector: Mitigating the vulnerabilities of connected devices and smart ATMs. *Asian Business Review*, 13(3), pp.95–102.

Guo, Z. and Kennedy, L. (2023) Policing based on automatic facial recognition. *Artificial Intelligence and Law*, 31(2), pp.397–443.

Gutowska, A. (2024) What are AI Agents. IBM, Available at: https://www.ibm.com/think/topics/ai-agents (Accessed 23 April 2026).

H.R.2575 – AI in Government Act of 2020. (online) Available at: www.congress.gov/bill/116th-congress/house-bill/2575 (Accessed 8 July 2025).

H.R.3935 – FAA Reauthorization Act of 2024. (online) Available at: www.congress.gov/bill/118th-congress/house-bill/3935 (Accessed 8 July 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

H.R.4346 – CHIPS and Science Act. (online) Available at: www.congress.gov/bill/117th-congress/house-bill/4346 (Accessed 8 July 2025).
H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019. (online) Available at: www.congress.gov/bill/115th-congress/house-bill/5515 (Accessed 8 July 2025).
H.R.6216 – National Artificial Intelligence Initiative Act of 2020. (online) Available at: www.congress.gov/bill/116th-congress/house-bill/6216 (Accessed 8 July 2025).
HSBC (n.d.) 'Fighting financial crime.' Available at: https://www.hsbc.com/who-we-are/esg-and-responsible-business/fighting-financial-crime (Accessed 23 April 2026).
Halliday, T. C. and Shaffer, G. (eds.), (2015) *Transnational Legal Orders*. Cambridge: Cambridge University Press. doi:10.1017/CBO9781107707092.
Haring, W. and Zapf, D. (2025) Unsubstantiated suspicious transaction reports. White & Chase. Available at: https://www.whitecase.com/insight-alert/unsubstantiated-suspicious-transaction-reports (Accessed 23 April 2026).
Harvey, C.R. and Rabetti, D. (2024) International business and decentralized finance. *Journal of International Business Studies*, 55(7), pp.840–863.
Hasan, Z., et al. (2023) Can artificial intelligence (AI) manage behavioural biases among financial planners? *Journal of Global Information Management*, 31(2), pp.1–18.
Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M. and Hussain, A. (2024) Interpreting black-box models: a review on explainable artificial intelligence. *Cognitive Computation*, 16(1), pp.45–74.
Haugeland, J. (2000) *Artificial Intelligence: The Very Idea*. Cambridge, MA: MIT Press.
Hearson, M. (2022) Tax Treaties Explorer (Online database), Brighton: International Centre for Tax and Development (ICTD), www.treaties.tax (Accessed 1 April 2025).
Hilal, W., Gadsden, S.A. and Yawney, J. (2022) Financial fraud: a review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, p.116429.
Hodgson, G.S. and Jiang, S. (2021) *Online Money Laundering: Methods and Countermeasures*. Cheltenham, UK: Edward Elgar Publishing.
Home Office (2018) UK Anti-corruption Strategy: 2017 to 2022. Available at: https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022 (Accessed 23 April 2026).
Hopkins, M. and Shelton, N. (2019) Identifying money laundering risk in the United Kingdom: Observations from national risk assessments and a proposed alternative methodology. *European Journal on Criminal Policy and Research*, 25(1), pp.63–82.
Houston, J. F., Lin, C. and Ma, Y. (2012) Regulatory arbitrage and international bank flows. *The Journal of Finance*, 67(5), pp.1845–1895.
Hua, S.S. and Belfield, H. (2023) 'Effective Enforceability of EU Competition Law Under AI Development Scenarios'. Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society. ACM.
Huang, J. and Kisgen, J.D. (2013) Gender and corporate finance: Are male executives overconfident relative to female executives? *Journal of Financial Economics*, 108, p.822.
Hufnagel, S. (2017) Regulation of cross-border law enforcement: 'Locks' and 'dams' to regional and international flows of policing. *Global Crime*, 18(3), pp.218–236.
Hufnagel, S. and Mccartney, C. (eds.) (2017) *Trust in International Police and Justice Cooperation*. Oxford: Hart Publishing.
Hung, T.W. and Yen, C.P (2021) On the person-based predictive policing of AI. *Ethics and Information Technology*, 23, pp.165–176.
Hutiri, W. T. and Ding, A. Y. (2022) Bias in automated speaker recognition. In Proceedings of the 2022 ACM conference on fairness, accountability, and transparency, pp.230–247.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Hutter, R. and Hutter, M. (2021) Chances and risks of artificial intelligence: A concept of developing and exploiting machine intelligence for future societies. *Applied System Innovation*, 4(2), 37.

Hyperledger (2024) Hyperledger Fabric: A Distributed Ledger Technology for Blockchain Solutions. (online) Hyperledger. Available at: www.hyperledger.org/use/fabric (Accessed 4 April 2025).

i2 Analyst's Notebook (n.d.) IBM i2 Analyst's Notebook. Available at: https://i2group.com/solutions/i2-analysts-notebook (Accessed 23 April 2026).

IBM (2018) 'Introducing AI Fairness 360'. Available at: https://research.ibm.com/blog/ai-fairness-360 (Accessed 23 April 2026).

IBM (2023) What are large language models (LLMs)? 2 November.

IBM (2024) Watson for Financial Services. (online) IBM. Available at: www.ibm.com/watson/financial-services (Accessed 4 April 2025).

ICIJ (2020) 'Explore the FinCEN Files data', International Consortium of Investigative Journalists (ICIJ), 20 September. Available at: www.icij.org/investigations/fincen-files/explore-the-fincen-files-data/ (Accessed 23 April 2026).

IMF (2022) Global Financial Stability Report: Navigating the High-Inflation Environment. International Monetary Fund. Available at: https://www.imf.org/en/publications/gfsr/issues/2022/10/11/global-financial-stability-report-october-2022 (Accessed 23 April 2026).

InfoZoom (n.d.) InfoZoom – Data Analysis and Visualization Software. Available at: https://infozoom.nemo-ai.com/en/ (Accessed 23 April 2026).

Innreg (2025) Markets in Crypto-Assets Regulation (MiCA) Updated Guide (2025), InnReg. Available at: www.innreg.com/blog/mica-regulation-guide (Accessed 1 June 2025).

International Association for Impact Assessment (IAIA) (2015) Social Impact Assessment. Guidance for assessing and managing the social impacts of projects.

International Monetary Fund (2020) What are illicit financial flows? Available at: https://www.imf.org/en/about/factsheets/sheets/2023/fight-against-illicit-financial-flows (Accessed 23 April 2026).

Interpol (2023) Digital forensics in combating cybercrime. Available at: https://www.interpol.int/How-we-work/Innovation/Digital-forensics (Accessed 23 April 2026).

Ismayilov, G. and Özturan, C. (2025) PTTS: Zero-knowledge proof-based private token transfer system on Ethereum blockchain and its network flow based balance range privacy attack analysis. *Journal of Network and Computer Applications*, 233, p.104045.

Jackson, G., Markevych, M., Bardin, P. and Thomas, I (2023) *Nordic-Baltic Regional Technical Assistance Report: Financial Flows Analysis, AML/CFT Supervision, and Financial Stability*. Washington DC: International Monetary Fund. Available at: www.imf.org/-/media/Files/Publications/CR/2023/English/1EUREA2023003.ashx. (Accessed 8 July 2025).

Jamil, A. H., et al. (2021) The covid-19 impact on financial crime and regulatory compliance in Malaysia. *Journal of Financial Crime*, 29(2), pp.491–505.

Janský, P., Meinzer, M. and Palanský, M (2022) Is Panama really your tax haven? Secrecy jurisdictions and the countries they harm. *Regulation & Governance*, 16(3), pp.673–704.

Jarovsky, L. (2025) DeepSeek's Legal Pitfalls: Emerging AI Governance Challenges. Luiza's Newsletter,. Available at: https://www.luizasnewsletter.com/p/deepseeks-legal-pitfalls (Accessed 23 April 2026).

Jensen, M.C. and Meckling, W.H. (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), pp.305–360.

Jensen, R. I. T. and Iosifidis, A. (2023) Fighting money laundering with statistics and machine learning. *IEEE Access*, 11, pp. 8889–8903.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Jofre, M., Bosisio, A. and Riccardi, M. (2024) Financial crime risk assessment: Machine learning insights into ownership structures in secrecy firms. *Global Crime*, 25, p.242.
Joh, E.E. (2024) Police technology experiments. *Columbia Law Review Forum*, 125(1), pp.1–28.
Joh, E.E. (2024) The risks of gunshot detection and predictive AI in policing. *Yale Journal of Law & Technology*, 26(1), pp.89–110.
Johannesen, N. and Zucman, G. (2014) The end of bank secrecy? An evaluation of the G20 tax haven crackdown. *American Economic Journal: Economic Policy*, 6, pp.65–91.
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. Available at: https://jelt.padovauniversitypress.it/system/files/papers/JELT-2022-2-01.pdf (Accessed 1 February 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), 3-26.
Joseph, J. (2021) Leveraging artificial intelligence in citizenship by investment programmes. In: Bielicki, D.M. (ed.), *Regulating Artificial Intelligence in Industry*. New York: Routledge. Available at: www.routledge.com/Regulating-Artificial-Intelligence-in-Industry/Bielicki/p/book/9780367774622 (Accessed 1 February 2025).
Jumio (2024) Identity Verification and Compliance Solutions. (online) Jumio Corporation. Available at: www.jumio.com (Accessed 4 April 2025).
KPMG (2023) 2023 Fraud Outlook Report. Available at: https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2024/02/fraud-barometer-2023.pdf (Accessed 23 April 2026).
Kyc360 (2025) 'TD Bank AML Failures What Went Wrong?'. KYC360. Available at: https://kyc360.com/knowledge-hub/resources/td-bank-failures-what-went-wrong (Accessed 23 April 2026).
Kan, Y. (2024) The impact of AI on the development of manufacturing, logistics, and financial company from capital market perspectives. *Advances in Economics, Management and Political Sciences*, 115, pp.120–125.
Kanamori, S., et al. (2022) Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks. *Journal of Information Processing*, 30, p.789.
Kanupriya (2024) Opportunities and challenges of AI in financial risk management: A brief labour-centric analysis. *Forum for Economic and Financial Studies*, 2(2) 1758.
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.
Kenton, W. (2024) Anti-Money Laundering (AML): What It Is, Its History, and How It Works. (online) Investopedia. Available at: www.investopedia.com/terms/a/aml.asp? (Accessed 4 February 2025).
Keohane, R.O. (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.
Kethineni, S., Cao, Y. and Dodge, C (2017) Use of cryptocurrency in money laundering: Examining Bitcoin transactions. *International Criminal Justice Review*, 27(4), pp. 355–372.
Khan, B., Goh, K., Khan, A., Zuhairi, M. and Chaimanee, M. (2024) Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. *Processes*, 12(9), 1825.
Khullar, K. (2025) World's first 'body in a box' biological computer uses human brain cells with silicon-based computing. Tom's Hardware. Available at: https://www.tomshardware.com/tech-industry/worlds-first-body-in-a-box-biological-computer-uses-human-brain-cells-with-silicon-based-computing (Accessed 23 April 2026).
Kimery, A. (2025) Trump's new executive order on AI underemphasizes privacy, security issues. Biometric Update. Available at: https://www.biometricupdate.com/202501/trumps-new-executive-order-on-ai-underemphasizes-privacy-security-issues (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Kimery, A. (2025) US retreat from AI ethics leaves global vacuum. *Tech Policy Journal*, (online) Available at: https://techpolicyjournal.org/2025/kimery-ai-ethics (Accessed 8 July 2025).

King, C. T., et al. (2021) Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. In Floridi, L. (ed.), *Ethics, Governance and Policies in Artificial Intelligence*. Philosophical Studies Series, vol 144. Cham, Switzerland: Springer International Publishing.

King, T.C., Aggarwal, N., Taddeo, M. and Floridi, L. (2019) Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 25, pp.1–29.

Kipker, D.-K. and Bruns, H. (2022) Encrochat und die 'Chain of Custody': Digitale Ermittlungen alsBewährungsprobe für ein Recht auf faires Verfahren? *MMR*, 363–368.

Kishore, S.S. (2025) AI in risk management in finance. In Derbali, A.M.S (ed)., *Artificial Intelligence for Financial Risk Management and Analysis*. Hershey, PA: IGI Global Scientific Publishing, pp. 471–498.

Klein, K. (2019) Algorithms, race, and reentry: A review of Sandra G. Mayson's bias. In *Bias Out* (online) Available at: https://ccresourcecenter.org/2019/11/05/algorithms-race-and-reentry-a-review-of-sandra-g-maysons-bias-in-bias-out/ (Accessed 4 February 2025).

Kmieliauskas, L. (2025). Europol labels crypto and AI as a 'money laundering cloak'. Available at: https://cybernews.com/crypto/europol-crypto-money-laundering-ai. (Accessed 9 September 2025).

Kmet, C.T. (2018) How Blockchain, AI, and IoT are reshaping finance. Available at: www.icpas.org/information/copy-desk/insight/article/winter-2018/how-blockchain-ai-and-iot-are-reshaping-finance (Accessed 23 April 2026).

Knapp, E.D. and Langill, J.T. (2015) *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. 2nd edn. Cambridge, USA: Elsevier.

Kornaros, G. (2022) Hardware-assisted machine learning in resource-constrained IoT environments for security: Review and future prospective. *IEEE Access*, 10, pp.58603–58622.

Kothinti, K.G. (2025) AI-powered identity verification & risk analysis: The future of fraud prevention in financial services. *European Journal of Computer Science and Information Technology*, 13(9), pp.23–55.

Kranjec, J. (2025) Total value locked in DeFi soars 137% YoY to a staggering $129 billion. FOCUS ON Business. Available at: https://focusonbusiness.eu/en/news/total-value-locked-in-defi-soars-137-yoy-to-a-staggering-129-billion/6554 (Accessed 13 October 2025).

Kreissl, R. (2017) Will more data bring more security? In Carrera S. and Mitsilegas, V. (ed.), *Constitutionalising the Security Union*, Brussels: CEPS, pp.93–99.

Kurshan, E. and Shen, H. (2020) Graph computing for financial crime and fraud detection: Trends, challenges and outlook. *International Journal of Semantic Computing*, 14(04), pp.565–589.

Kurshan, E. et al. (2021) 'On the Current and Emerging Challenges of Developing Fair and Ethical AI Solutions in Financial Services'. In Proceedings of the Second ACM International Conference on AI in Finance. ACM.

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

Kuzmenko, O., Yarovenko, H. and Perkhun, L. (2023) Assessing the maturity of the current global system for combating financial and cyber fraud. *Statistics in Transition New Series*, 24(1), pp.229–258.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Kute, D.V., Pradhan, B., Shukla, N. and Alamri, A. (2021) Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review. *IEEE Access*, 9, pp.82300–82317.

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).

Laghari, A.A., Wu, K., Laghari, R.A., Ali, M. and Khan, A.A. (2021) A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, pp.1–19.

Lakhchini, W., Wahabi, R. and Kabbouri, M.E. (2022) Artificial Intelligence & Machine Learning in Finance: A literature review. *International Journal of Accounting, Finance, Auditing, Management and Economics*, 3(6-1), pp.437–455.

Landers, R.N. and Behrend, T.S. (2023) Auditing the AI auditors: A framework for evaluating fairness and bias in high stakes AI predictive models. *American Psychologist*, 78(1), pp.36–49.

Lando, S. and Landry, M. (2023) The production and use of financial intelligence to counter terrorism and terrorist financing. In *Countering the Financing of Terrorism*. International Monetary Fund. Available at: www.elibrary.imf.org/display/book/9798400204654/CH003.xml. (Accessed 8 July 2025).

Lane, L. (2022) Clarifying human rights standards through artificial intelligence initiatives. *International and Comparative Law Quarterly*, 71(4), pp.915–944.

Lannoo, K. and Parlour, R. (2021) Anti-Money Laundering in the EU – CEPS. Brussels: CEPS. Available at: www.ceps.eu/ceps-publications/anti-money-laundering-in-the-eu/. (Accessed 8 July 2025).

Laperuque, J. (2025) Status of state laws on facial recognition surveillance. Tech Policy Press. Available at: https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/ (Accessed 23 April 2026).

Lebid, O. and Veits, O. (2020) Search for statistically approved criteria for identifying money laundering risk. *Banks and Bank Systems*, 15(4), pp.150–163.

Lee, Y., Bradford, B. and Posch, K. (2024) The effectiveness of big data-driven predictive policing: Systematic review. *Justice Evaluation Journal*, 7(2), pp.127–160.

Lefebvre, S. (2003) The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and Counterintelligence*, 16(4), pp.527–542.

Leitner, G., Singh, J., Van Der Kraaij, A. and Zsámboki, B. (2024) *The Rise of Artificial Intelligence: Benefits and Risks for Financial Stability*. European Central Bank – Financial Stability Review.

Leone, M. (2021) From fingers to faces: Visual semiotics and digital forensics. *International Journal for the Semiotics of Law-Revue internationale de sémiotique juridique*, 34(2), pp.579–599.

Leslie, D. (2020) Understanding Bias in Facial Recognition Technology. The Alan Turing Institute. Available at: https://www.turing.ac.uk/news/publications/understanding-bias-facial-recognition-technologies (Accessed 23 April 2026).

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

Levi, M., Reuter, P. and Halliday, T. (2018) Can the AML system be evaluated without better data? *Crime, Law and Social Change*, 69(2), pp.307–328.

Lewis, J. (2024) The role of AI in law enforcement report writing. *Criminal Justice Ethics Review*, 43(1), pp.23–39.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Lewis, S. (2024) How artificial intelligence is changing the reports US police write. The Guardian, Available at: https://www.theguardian.com/technology/2024/oct/03/artificial-intelligence-police-reports (Accessed 23 April 2026).
LexisNexis (n.d.) LexisNexis. Available at: www.lexisnexis.com (Accessed 4 April 2025).
Liberty (2019) Report: Policing by Machine. Available at: https://www.libertyhumanrights.org.uk/issue/policing-by-machine/ (Accessed 23 April 2026).
Lim, T. (2023) Environmental, social, and governance (ESG) and artificial intelligence in finance: state-of-the-art and research takeaways. *Research Square*, pp.1–45.
Littler, A. (2020) How the EU's regulatory approach to gambling is failing. *Maastricht Journal of European and Comparative Law*, 27(1), pp.56–72.
Liu, X. (2023) New characteristics of AI analysis of financial risks and their transmission traceability paths. *International Journal of Big Data Intelligent Technology*, 4(1). Available at: https://doi.org/10.38007/ijbdit.2023.040105 (Accessed 11 April 2025).
Liu, Y., Tian, M. and Shao, Y. (2022) *Cybercrimes and Financial Crimes in the Global Era*. Singapore: Springer.
Lloyds Banking Group (2025) Lloyds Banking Group bolsters AI capabilities by appointing Head of Responsible AI. Available at: www.lloydsbankinggroup.com/media/press-releases/2025/lloyds-banking-group-2025/lloyds-banking-group-bolsters-ai-capabilities-by-appointing-head.html?utm_source=chatgpt.com (Accessed 11 April 2025).
Loring, B. and Lee, R. (2024) Governor Newsom Vetoes California AI Bill. San Francisco Chronicle. 20 December. Available at: https://sfchronicle.com/2024/ai-bill-veto (Accessed 8 July 2025).
Loring, J.M. and Lee, A.R. (2024) California poised to further regulate artificial intelligence. *The National Law Review*, 17 September. Available at: https://natlawreview.com/article/california-poised-further-regulate-artificial-intelligence-focusing-safety (Accessed 3 February 2025).
Lucero, K. (2019) Artificial intelligence regulation and China's future. *Columbia Journal of Asian Law*, 33(1), pp.94–171.
Lucero, L. (2019) China's AI regulatory philosophy and its global impact. *Georgetown Journal of International Affairs*, 20(2), pp.45–58.
Lugo, G. and Faiella, G. (2020) Cryptocurrencies and money laundering: An overview. Bank of Italy Occasional Paper No. 559.
Lynskey, O. (2019) Criminal justice profiling and EU data protection law. *International Journal of Law in Context*, 15(2), pp.162–176.
Lynskey, O. (2019) *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.
Mi5 (2023) Threats to the UK: espionage, cyber attacks and terrorism. Available at: www.mi5.gov.uk/threats-to-the-uk (Accessed 20 March 2025).
Machado, H. and Granja, R. (2019) Police epistemic culture and boundary work with judicial authorities and forensic scientists: The case of transnational DNA data exchange in the EU. *New Genetics and Society*, 38(3), pp.289–307.
Madiega, T. (2023) Generative AI and watermarking. European Parliamentary Research Service Briefing. Available at: www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf (Accessed 3 February 2025).
Mahadevkar, S.V., et al. (2024) Exploring AI-driven approaches for unstructured document analysis and future horizons. *Journal of Big Data*, 11, p.92.
Malhotra, D., Saini, P. and Singh, A.K. (2022) How blockchain can automate KYC: Systematic review. *Wireless Personal Communications*, 122(2), pp.1987–2021.
Mantelero, A. (2018) AI and Big Data: A blueprint for a human right, social and ethical impact assessment. *Computer Law & Security Review*, 34, pp.754–772.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Mantelero, A. (2022) *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*. Information Technology and Law Series. The Hague: Springer.
Mantelero, A. and Fanucci, F. (2024) Governing AI: From Principles to Implementation in a Global World. Task Force 05 – Inclusive Digital Transformation. Policy Briefs. G20 – Brazil.
Mantelero, A. and Marí, J. (2025) FRIA model: Guide and use cases. FRIA methodology for AI design and development. Barcelona: DPD Xarxa,.
Mao, Y. and Shi-Kupfer, K. (2021) *Algorithm Governance in China: Between Regulation and Innovation*. Berlin: MERICS.
Mao, Y. and Shi-Kupfer, K. (2021) Online public discourse on artificial intelligence and ethics in China: context, content, and implications. *AI & Society*, 38(1), pp.373–389.
Marcus, A. and Hargrave, T. (2021) The role of stakeholders in ethical decision-making. In Marcus, A. A. and Hargrave T. J. *Managing Business Ethics: Making Ethical Decisions*. Thousand Oaks, CA: SAGE Publications, pp. 242–275.
Maree, C., Modal, E.J. and Omlin, W.C (2020) Towards responsible ai for financial transactions. 2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp.16–21.
Mastercard (2024) Mastercard transforms the fight against scams with latest AI tech. Available at: www.mastercard.com/news/press/2024/april/mastercard-transforms-the-fight-against-scams-with-latest-ai-tech/#:~:text=They%20just%20need%20to%20trick,them%20before%20money%20is%20lost. (Accessed 11 April 2025).
Matejic, N. and Wilson, C. (2024) Crimes of influence: Generative artificial intelligence-led crime as a service. *The Commonwealth Cyber Journal*, n.v.(n.i.), pp.75–95.
Matthews, D. (2023) The AI rules that US policymakers are considering, explained. Vox, 1 August. Available at: https://www.vox.com/future-perfect/23775650/ai-regulation-openai-gpt-anthropic-midjourney-stable (Accessed 23 April 2026).
Matthews, T. (2023) AI and congressional gridlock in the United States. *Journal of American Politics*, 58(3), pp.299–315.
Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H. (2023) Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet*, 15(2), p.83.
Meijer, A. and Wessels, M. (2019) Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), pp.1031–1039.
Meinzer, M. (2016) Towards a common yardstick to identify tax havens and to facilitate reform. In Rixen, T. and Dietsch, P. (eds.) *Global Tax Governance – What is Wrong with it, and How to Fix it*. Colchester: ECPR Press, pp.255–288.
Meinzer, M. and Harari, M. (2023) 'Transforming our flagship indexes to be even more responsive and timely', Tax Justice Network, 13 June. Available at: https://taxjustice.net/2023/06/13/transforming-our-flagship-indexes-to-be-even-more-responsive-and-timely/ (Accessed 23 April 2026).
Meinzer, M., Harari, M., Lorenzo, F. and Knobel, A. (2023) Comparative report on SWIFT data in the EU27. *SSRN Electronic Journal*. doi: http://dx.doi.org/10.2139/ssrn.4346192. (Accessed 8 July 2025).
Mészáros, E.L. (2016) The evaluation of police cooperation between Hungary and Romania in the fight against cross-border financial criminal activities. *Eurolimes*, 21, pp.143–156.
Metelski, D. and Sobieraj, J. (2022) Decentralized finance (DeFi) projects: A study of key performance indicators in terms of DeFi protocols' valuations. *International Journal of Financial Studies*, 10(4), p.108.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Milojević, N. and Redzepagic, S. (2021) Prospects of artificial intelligence and machine learning application in banking risk management. *Journal of Central Banking Theory and Practice*, 10(3), pp.41–57.
Milon, M.N.U. (2024) Gravitating towards artificial intelligence on anti-money laundering: A PRISMA based systematic review. *International Journal of Religion*, 5(7), pp.303–315.
Ministerio De Hacienda Y Función Pública (2023) Orden HFP/115/2023, de 9 de febrero, por la que se determinan los países y territorios, así como los regímenes fiscales perjudiciales, que tienen la consideración de jurisdicciones no cooperativas.
Mitchell, T.M. (1997) *Machine Learning*. New York: McGraw-Hill.
Mittelstadt, B.D., Allo, P., Taddeo, D., Wachter, S. and Floridi, L. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society*, pp.1–21.
Mittelstadt, B.D., et al. (2016) The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2).
Mohan, M.B.R. (2024) AI in fraud detection: Evaluating the efficacy of artificial intelligence in preventing financial misconduct. *Journal of Electrical Systems*, 20(3s), pp.1332–1338.
Moldovan, D. (2023) Algorithmic decision making methods for fair credit scoring. *IEEE Access*, 11, pp.59729–59743.
Moody's (2025) Orbis – BvD Is Now Moody's. (online) Available at: www.moodys.com/web/en/us/capabilities/company-reference-data/orbis.html (Accessed 4 March 2025).
Mosaic (2024) Research reveals two thirds of banks struggle with data quality and integrity. London, 29 January 2024.
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, p.297.
Nagaraj, C.T., Anand, M.C.J., Priyadharshini, S.S. and Aparna, P. (2024) 'GCNXG: Detecting Fraudulent Activities in Financial Networks: A Graph Analytics and Machine Learning Fusion', in Gundebommu, S.L., Sadasivuni, L. and Malladi, L.S. (eds.) *Renewable Energy, Green Computing, and Sustainable Development. REGS 2023*. Communications in Computer and Information Science, vol. 2081. Cham: Springer. pp. 17–32. Available at: https://doi.org/10.1007/978-3-031-58607-1_2 (Accessed 11 April 2025).
Nama, P., Reddy, P. and Pattanayak, K.S. (2024) Artificial intelligence for self-healing automation testing frameworks: Real-time fault prediction and recovery. *Cineforum*, 64 (3S), p.111.
Nandivada, S.N. and Haan, J.H. (2025) Kickstarting AI in the Federal Government: OMB's Policy to Implement Executive Order 14179. Morrison Foerster, 15 April. Available at: https://www.mofo.com/resources/insights/250415-kickstarting-ai-in-the-federal (Accessed 23 April 2026).
Nandivada, V. and Haan, D. (2025) *Implementing Trump's EO on AI: OMB Guidelines*. Washington, DC: Office of Management and Budget.
Narajala, V.S. and Narayan, O. (2025) Securing agentic AI: A comprehensive threat model and mitigation framework for generative AI agents. arXiv preprint arXiv:2504.19956.
Nash, I., Kennedy-Mayo, D., Swire, P. and Antón, A. (2024) Legal issues in reconciling data protection, AI, and cybersecurity under EU law. *Missouri Law Review*, 89(3), pp.871–939.
Nash, K., Turner, S. and Greaves, L. (2024) *Understanding the EU AI Act*. Brussels: Centre for European Policy Studies.
Natwest Group (2025) 'Innovation and digitalisation'. Available at: https://www.natwestgroup.com/sustainability/society/innovation-and-digitisation.html (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

National Crime Agency (NCA) (2021) National Strategic Assessment of Serious and Organised Crime 2021. Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file (Accessed 23 April 2026).

National Crime Agency (NCA) (2025) Money laundering and illicit finance. Available at: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance?highlight=WyJtb25leSIsIidtb25leSIsImxhdW5kZXJpbmciLCJsYXVuZGVyIiwibGF1bmRlcmVkIiwibGF1bmRlcmVycyIsImxhdW5kZXJlciIsImxhdW5kZXJlcidzIiwibGF1bmRlcnMiLCJsYXVuZGVyZXIiwibW9uZXkgbGF1bmRlcmluZyJd (Accessed 23 April 2026).

National Institute of Standards and Technology (NIST) (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (Available at: Accessed 23 April 2026).

National Police Chiefs' Council (2023) *Covenant for Using AI in Policing*. London: NPCC.

National Police Chiefs' Council (2023) Covenant for Using Artificial Intelligence (AI) in Policing, Version 1.1. Office of the Police Chief Scientific Adviser.

Nduka, B., Okenyebuno, E. and Sechap, G. (2021) Refocusing designated non-financial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance. *Journal of Money Laundering Control*, 24(4), pp.693–711.

Nerantzi, E. and Sartor, G. (2024) Hard AI crime: The deterrence turn. *Oxford Journal of Legal Studies*, 44(3), pp.673–698.

Nguyen, D.K., Sermpinis, G. and Stasinakis, C. (2023) Big data, artificial intelligence and machine learning: A transformative symbiosis in favour of financial technology. *European Financial Management*, 29(2), pp.517–548.

Nikolakopoulos, A. et al. (2024) Large language models in modern forensic investigations. In: 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE), pp.1–5.

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

O'Neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

OECD (2022) Tax Crime Investigation Maturity Model. Available at: https://www.oecd.org/en/topics/sub-issues/comparative-analysis-of-tax-administrations/tax-maturity-models.html (Accessed 23 April 2026).

OECD (2014) Illicit Financial Flows from Developing Countries: Measuring OECD Responses. Available at: https://www.oecd.org/en/publications/measuring-oecd-responses-to-illicit-financial-flows-from-developing-countries_9789264203501-en.html (Accessed 23 April 2026).

OECD (2017) *Standard for Automatic Exchange of Financial Account Information in Tax Matters*. 2nd edn. Paris: OECD Publishing.

OECD (2018) Illicit Financial Flows. (online) Available at: www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/illicit-financial-flows_g1g679f5/9789264268418-en.pdf (Accessed 4 February 2025).

OECD (2018) Preventing the Misuse of Investment Migration Programmes. (online) Available at: www.oecd.org (Accessed 4 February 2025).

OECD (2023) CRS Guidance on Investment Migration. (online) Available at: www.oecd.org (Accessed 4 February 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

OECD (2023) Guidelines for MNEs. (online) Available at: https://mneguidelines.oecd.org/ (Accessed 4 February 2025).
OECD (2023) Misuse of Citizenship and Residency by Investment Programmes. (online) Available at: www.oecd.org/en/publications/misuse-of-citizenship-and-residency-by-investment-programmes_ae7ce5fb-en.html (Accessed 4 February 2025).
OECD (2025) OECD Model Tax Convention on Income and on Capital. Available at: www.oecd.org/en/publications/serials/model-tax-convention-on-income-and-on-capital-full-version_57a089d7.html (Accessed 1 April 2025).
OHCHR (2020) UN Human Rights Report 2020. Available at: https://www.ohchr.org/en/publications/annual-report/ohchr-report-2020 (Accessed 23 April 2026).
Ocampo, D., Branzoli, N. and Cusmano, L. (2023) Crypto, tokens and DeFi: navigating the regulatory landscape. Bank for International Settlements. Available at: https://www.bis.org/fsi/publ/insights49.htm (Accessed 23 April 2026).
Odeyemi, O., et al. (2024) Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, 11(01), pp.2101–2110.
Odilla, F. (2023) Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime, Law and Social Change*, 80(4), pp.353–396.
Oerlemans, J.-J. and Royer, S. (2023) The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 14(4), pp.434–458.
Ogbeide, H., Thomson, M.E., Gonul, M.S., Onkal, D., Bhowmick, S. and Bello, A.U. (2024) Rethinking experts' perceptions in money laundering risk assessment. *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-024-09586-w (Accessed 8 July 2025).
Ogbeide, H., Thomson, M.E., Gonul, M.S., Pollock, A.C., Bhowmick, S. and Bello, A.U. (2023) The anti-money laundering risk assessment: A probabilistic approach. *Journal of Business Research*, 162, 113820.
Olowu, O., et al. (2024) AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *GSC Advanced Research and Reviews*, 21(02), pp.227–237.
Omar, N. and Johari, Z. A. (2015) An international analysis of FATF recommendations and compliance by DNFBPS. *Procedia Economics and Finance*, 28, pp.14–23.
Onfido (2024) Digital Identity Verification Software. (online) Onfido. Available at: www.onfido.com (Accessed 4 April 2025).
Oosthoek, K. (2021) Flash crash for cash: Cyber threats in decentralized finance. arXiv preprint. Cornell University. Available at: https://arxiv.org/abs/2106.10740 (Accessed 23 April 2026).
Ostmann, F. and Dorobantu, C. (2021) AI in financial services. Alan Turing Institute.
Owolabi, O.S., et al. (2024) Ethical implication of artificial intelligence (AI) adoption in financial decision making. *Computer and Information Science*, 17(1), p.49.
Oyeniyi, L.D., Ugochukwu, C.E. and Mhlongo, N.Z. (2024) Implementing AI in banking customer service: a review of current trends and future applications. *International Journal of Science and Research Archive*, 11(2), pp. 1492–1509.
Oyewole, A.T., et al. (2024) Promoting sustainability in finance with AI: A review of current practices and future potential. *World Journal of Advanced Research and Reviews*, 21(3), pp.590–607.
Palmer, C. (2021) *Digital Forensics: The Fascinating World of Forensic Science*. New York: Rosen Publishing.
Palmiotto, F (2021) The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings. In Ebers, M. and Cantero Gamito, M. (eds.), *Algorithmic*

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law. Cham: Springer, pp.49–70.

Papadopoulos, P., Pitropakis, N. and Buchanan, W.J (2022) Decentralized privacy: A distributed ledger approach. In *Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0*.Cham: Springer International Publishing, pp. 1805–1830.

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.

Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pavlidis, G. (2023) Deploying artificial intelligence for anti–money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, 26(7), pp. 155–166.

Pearsall, B. (2010) Predictive policing: The future of law enforcement. *National Institute of Justice Journal*, (266), pp.16–19.

Penney, J.W. (2022) Understanding chilling effects. *Minnesota Law Review*, 106, pp.1451–1530.

Peršak, N. (2021) Automated justice and its limits: Irreplaceable human(e) dimensions of criminal justice. In Vermeulen G., Peršak, N. and Recchia N. (eds.), *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*. Apeldoorn, The Netherlands: Maklu, pp.225–241.

Peters, M., Vanderhallen, M. and Nelen, H. (2016) Cross-border criminal investigation in the Meuse-Rhine Euroregion: International policing and the theory of (inter-)organisational conflict. *European Journal on Criminal Policy and Research*, 22, pp.41–60.

Pillai, V. (2023) Integrating AI-driven techniques in big data analytics: Enhancing decision-making in financial markets. *International Journal of Engineering and Computer Science*, 12(07), pp.25774-25787.

Ping, H. (2005) The suspicious transactions reporting system. *Journal of Money Laundering Control*, 8(3), pp.252–259.

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

Press, G. (2024) Detecting Deepfakes: Fighting AI with AI. Forbes, 06 August. Available at: https://www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/ (Accessed 23 April 2026).

Purves, D. (2022) Fairness in algorithmic policing. *Journal of the American Philosophical Association*, 8(4), pp.741–761.

PwC (2022) Bitcoin, cryptocurrency, blockchain … So what does it all mean? Available at: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (Accessed 23 April 2026).

PwC (2024) Global Economic Crime and Fraud Survey 2024. Available at: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (Accessed 23 April 2026).

PwC (2021) Emerging technologies in anti-financial crime: The role of AI and machine learning. (online) PricewaterhouseCoopers. Available at: www.pwc.com/gx/en/industries/financial-services/publications/emerging-technologies-in-anti-financial-crime.html (Accessed 4 April 2025).

Pwc (2025) PwC Global Crypto Regulation Report 2025. (Legal.pwc.de, 2025). Available at: https://legal.pwc.de/content/services/global-crypto-regulation-report/ (Accessed 9 September 2025).

Quantexa (2024) Network Analytics and Data-Driven Decision Making. (online) Quantexa. Available at: www.quantexa.com (Accessed 4 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Raji, I.D., Kumar, I.E., Horowitz, A. and Selbst, A.D. (2022) The fallacy of AI functionality. In: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22). ACM, pp.610–623.

Ramaliba, T. and Jacobs, L (2024) Artificial intelligence technology to enhance data quality management practices in the banking industry in South Africa. *SA Jnl Libs & Info Sci*, 90(2).

Ranchordas, S. (2021) Experimental Regulations for AI: Sandboxes for Morals and Mores. University of Groningen Faculty of Law Research Paper, 7/2021. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744 (Accessed 23 April 2026).

Rane, N., Choudhary, S. and Rane, J. (2024) Artificial Intelligence (AI), Internet of Things (IoT), and blockchain-powered chatbots for improved customer satisfaction, experience, and loyalty. Available at: https://ssrn.com/abstract=4847274 (Accessed 9 September 2025).

Rashid, A.B. and Kausik, A.K. (2024) AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, 7, p.100277.

Rayner, B. (2024) 2025 Trends in AML and Financial Crime Compliance: A Data-Centric Perspective and Deep Dive into Transaction Monitoring. Available at: www.silenteight.com/blog/2025-trends-in-aml-and-financial-crime-compliance-a-data-centric-perspective-and-deep-dive-into-transaction-monitoring. (Accessed 23 April 2026).

Rebovich, D.J., Kim, J. and Layne, M. (2021) The changing face of financial crime: New technologies, new offenders, new victims, and new strategies for prevention and control. *Victims & Offenders*, 16(5), pp.617–636.

Refinitiv (2024) World-Check: Risk Intelligence. (online) Refinitiv. Available at: www.refinitiv.com/en/products/world-check-risk-intelligence (Accessed 4 April 2025).

Regnier, T. (2024) Artificial Intelligence – Questions and Answers. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_168. (Accessed 23 April 2026).

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings PE/4/2023/REV/1 OJ L 191, 28 7..2023, pp.118–180.

Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 (Prüm II Regulation) PE/75/2023/REV/1 OJ L 2024/982, 5.4.2024.

Republic of Turkey Ministry of Interior (2023) Turkish Citizenship by Investment. (online) Available at: www.nvi.gov.tr (Accessed 1 April 2025).

Reuter, P. and Riccardi, M. (2024) Introduction to Special Issue on 'Understanding Money Laundering: Empirical and Theoretical Insights into Offenders, Typologies, and Determinants of Criminal Behaviour'. *European Journal on Criminal Policy and Research*, 30(3), pp.327–332.

Reuters (2024) Elon Musk's Neuralink implants brain chip in first human. Reuters, 30 January.

Riccardi, M. and Reuter, P. (2024) The varieties of money laundering and the determinants of offender choices. *European Journal on Criminal Policy and Research*, 30(3), pp. 333–358.

Rice, A., Lamont, E. and Francis, T. (2024) Colorado's groundbreaking AI law: Implications for the US and beyond. *Denver Law Review*, 101(2), pp.201–229.

Rice, T., Lamont, K. and Francis, J. (2024) The Colorado Artificial Intelligence Act: FPF U.S. Legislation Policy Brief. Future of Privacy Forum, July. Available at: https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf (Accessed 23 April 2026).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Richardson, B., Williams, D. and Mikkelsen, D. (2019) Network analytics and the fight against money laundering, McKinsey. Available at: www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering (Accessed 8 July 2025).

Rizinski, M., et al. (2022) Ethically responsible machine learning in fintech. *IEEE Access*, 10, pp.97531–97554.

Roberts, H. et al. (2021) The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society*, 36, pp.59–77.

Roberts, H., Cowls, J. and Floridi, L. (2021) China's AI governance: Balancing ethics and control. *AI & Society*, 36(4), pp.987–1001.

Roodt, C. and Benson, B. (2015) Databases for stolen art. *SA Crime Quarterly*, June, No. 52.

Ross, S. and Hannan, M. (2007) Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, 10(1), pp.106–115.

Rouhollahi, Z. (2021) 'Towards Artificial Intelligence Enabled Financial Crime Detection'. Cornell University. Available at: https://arxiv.org/abs/2105.10866 (Accessed 23 April 2026).

RsCase (n.d.) rsCase – Investigation Case Management Software. Available at: www.rstech.de/en/products/rscase/ (Accessed 13 April 2025).

Russell, S. and Norvig, P. (2018) *Artificial Intelligence: A Modern Approach*. Harlow: Prentice Hall.

Ryan, M., Brey, P., Machnish, K., Hatzakis, T., King, O., Maas, J., Haasjes, R., Fernandez, A., Martorana, S., Oluoch, I., Eren, S. and Van Der Puil, R. (2019) D1.4 – Report on ethical tensions and social impacts. SHERPA project.

Ryan-Mosley, T. and Heikkilä, M. (2023) Inside Biden's sweeping AI executive order. *MIT Technology Review*. (online) Available at: https://technologyreview.com/2023/biden-ai-order (Accessed 8 July 2025).

Ryan-Mosley, T. and Heikkilä, M. (2023) Three things to know about the White House's executive order on AI. *MIT Technology Review*, 30 October. Available at: https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/ (Accessed 23 April 2026).

Ryan-Mosley, T. (2023) New York's AI hiring law may set national precedent. *MIT Technology Review* (online). Available at: https://technologyreview.com/2023/ai-hiring-law (Accessed 8 July 2025).

Ryan-Mosley, T. (2023) Why everyone is mad about New York's AI hiring law? *MIT Technology Review*, 10 July. Available at: https://www.technologyreview.com/2023/07/10/1076013/new-york-ai-hiring-law/ (Accessed 23 April 2026).

S.2892 – Algorithmic Accountability Act of 2023. (online) Available at: www.congress.gov/bill/118th-congress/senate-bill/2892 (Accessed 8 July 2025).

S.B. 149 – Artificial Intelligence Amendments. (online) Available at: https://le.utah.gov/~2023/bills/static/SB0149.html (Accessed 8 July 2025).

SB 1047 – Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. (online) Available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1047 (Accessed 8 July 2025).

SB24-205 – 2024 Consumer Protections for Artificial Intelligence. Available at: https://leg.colorado.gov/bills/sb24-205 (Accessed 23 April 2026).

Sachoulidou, A. (2023) Going beyond the 'common suspects': To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. doi:10.1007/s10506-023-09347-w. (Accessed 8 July 2025).

Sachoulidou A. (2026) A Typology of Automated Law Enforcement Systems Under EU Law: What Standards for Defence Rights? *European Papers*, 11(1), pp. 595–630.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Sachoulidou, A. (2024) Harnessing AI for law enforcement: Solutions and boundaries from the forthcoming AI Act. *New Journal of European Criminal Law*, 15(2), pp.117–125.
Sachoulidou, A. and Vavoula, N. (2025) Artificial intelligence and surveillance. In Lucarelli, S. and Sperling, J. (eds.), *Handbook of European Union Governance*. Cheltenham: Elgar, pp.156–170.
Sachoulidou, A., Rego Oliveira, C., Kordoni, A., Hughes, J., Nidhi Shiji, A. and Nathan, C. (2024) D8.2 – The project's ethical, data protection and societal impact assessment. TRACE project.
Sakshi, S. and Wadhwa, M. (2023) Enhancing Digital Investigation: Leveraging ChatGPT for Evidence Identification and Analysis in Digital Forensics. In: 2023 IEEE International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India.
Salem, A.H., et al. (2024) Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 11, article number 105.
Salom Lucas, A. and Llambés Sánchez, M.I. (2021) Mutual legal assistance on criminal matters: when theory meets practice – a real story. *ERA Forum*, 22(2), pp.337–349.
Samuel, A.L. (1959) Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 3(3), pp.210–229.
Sandotra, N. and Arora, B. (2024) A comprehensive evaluation of feature-based AI techniques for deepfake detection. *Neural Computing & Applications*, 36, pp. 3859–3887 (Accessed 6 April 2025).
Sari, Y. and Indrabudiman, A. (2024) The role of artificial intelligence (ai) in financial risk management. *Formosa Journal of Sustainable Research*, 3(9), pp.2073–2082.
Sarker, I.H. (2021) Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2, p.160.
Sarzaeim, P., Ahmadi, H., Alipour, M. and Borumand, M. (2023) A systematic review of using machine learning and natural language processing in smart policing. *Computers*, 12(12), p.255.
Sathye, M. and Islam, J. (2011) Adopting a risk-based approach to AMLCTF compliance: The Australian case. *Journal of Financial Crime*, 18(2), pp.169–182.
Savona, E.U., Riccardi, M., Shelton, N. and Kleemans, E. R (2017) Assessing the Risk of Money Laundering in Europe: Final Report of Project IARM. Available at: www.academia.edu/33455865/Assessing_the_Risk_of_Money_Laundering_in_Europe_Final_Report_of_Project_IARM. (Accessed 8 July 2025).
Sayari (2025) Sayari. (online) Available at: https://sayari.com/ (Accessed 4 March 2025).
Scheuer, F., and Slemrod, J. (2019) Taxation and the Superrich (No. w26207), Cambridge, MA: National Bureau of Economic Research. Available at: www.nber.org/papers/w26207.pdf (Accessed 15 April 2025).
Sciurba, M. (2018) The heart of know your customer requirements: The discriminatory effect of AML and CTF policies in times of counter-terrorism in the UK. *European Journal of Crime, Criminal Law and Criminal Justice*, 26(3), pp.222–235.
Sedlmeir, J., Lautenschlager, J., Fridgen, G. and Urbach, N. (2022) The transparency challenge of blockchain in organizations. *Electronic Markets*, 32(3), pp.1779–1794.
Selten, F., Robeer, M. and Grimmelikhuijsen, S. (2023) 'Just like I thought': Street-level bureaucrats trust AI recommendations if they confirm their professional judgment. *Public Administration Review*, 83(2), pp.263–278.
Shachar, A. (2017) *The Birthright Lottery: Citizenship and Global Inequality*. Cambridge, MA: Harvard University Press.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Shami, S. and Rohatgi, S. (2024) Understanding and mitigating advanced persistent threats in a dynamic cyber landscape. In Shrivastava, G. et al. (eds.) *Emerging Threats and Countermeasures in Cybersecurity*. Beveryly, USA: Scrivener Publishing LLC.
Sharma, R. (2026) Decentralized finance (DeFi) definition and use cases. Investopedia. Available at: https://www.investopedia.com/decentralized-finance-defi-5113835 (Accessed 23 April 2026).
Sharman, J.C. (2010) Dysfunctional policy transfer in national tax blacklists. *Governance*, 23(4), pp.623–639.
Sheehan, M. (2023) China's AI regulations and how they get made. *Horizons: Journal of International Relations and Sustainable Development*, 24, pp.108–125.
Sheehan, S. (2023) Algorithm regulation in China: The March 2022 framework. *Asia Tech Law Bulletin*, 12(1), pp.66–84.
Shepardson, D. (2025) Trump Revokes Biden's AI Order but Leaves Key Infrastructure Orders Intact. Reuters. (online) Available at: https://reuters.com/2025/trump-ai-orders (Accessed 8 July 2025).
Shepardson, D. (2025) Trump revokes Biden executive order on addressing AI risks. Reuters, 21 January. Available at: https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/ (Accessed 23 April 2026).
Sheptycki, J.W.E. (2007) Transnational crime and transnational policing. *Sociology Compass*, 1, pp. 485–498.
Shiel, F. and Starkman, D (2020) 'About the FinCEN Files investigation', International Consortium of Investigative Journalists (ICIJ), 19 September. Available at: www.icij.org/investigations/fincen-files/about-the-fincen-files-investigation/ (Accessed 8 July 2025).
Silva, S. and Kenney, M. (2019) Algorithms, platforms, and ethnic bias. *Communications of the ACM*, 62(11), pp.37–39.
Singh, K. and Best, P. (2019) Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, 34, 100418.
Slaby, J. R. (2018) Understanding the true, hidden costs of ransomware attacks on the business. Acronis. Available at: https://www.acronis.com/en/blog/posts/costs-of-ransomware-attacks/ (Accessed 23 April 2026).
Sommerer, L. (2025) *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control. A Study of Person-based Predictive Policing and the Algorithmic Turn*. Baden-Baden: Nomos.
Sophia, I.N. (2022) Report with proposals to the Commission on Citizenship and Residence by Investment Schemes | A9-0028/2022. (online) European Parliament. Available at: www.europarl.europa.eu/doceo/document/A-9-2022-0028_EN.html (Accessed 4 February 2025).
Stanford University Human-Centred Artificial Intelligence (2022) AI Index Report 2022. Stanford: Stanford University.
Stanford University Human-Centred Artificial Intelligence (2022) What The CHIPS and Science Act means for Artificial Intelligence. Explainer, August.
Starcevic, S. (2025) Malta's 'golden passport' scheme is illegal, EU top court rules. POLITICO. Available at: www.politico.eu/article/european-court-rules-maltese-golden-passport-scheme-against-eu-law/ (Accessed 30 April 2025).
Stoykova, R. (2023) Encrochat: The hacker with a warrant and fair trials? *Forensic Science International: Digital Investigation*, 46, 301602.
Strange, S. (1996) *The Retreat of the State: The Diffusion of Power in the World Economy* Cambridge: Cambridge University Press.
Straus, J. (2021) Artificial intelligence: Challenges and chances for Europe. *European Review*, 29(1), pp.142–158.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Strikwerda, L. (2021) Predictive policing: The risks associated with risk assessment. *The Police Journal*, 94(3), pp.422–436.
Stryker, C. (2023) What are large language models (LLMs)? IBM. Available at: https://www.ibm.com/think/topics/large-language-models (Accessed 23 April 2026).
Sumner, J. (2025) The AI-Crypto Nexus: Navigating the Risks and Rewards of a Transformative Convergence. GRC World Forums. Available at: www.grcworldforums.com/risk-digital-north-america/the-ai-crypto-nexus-navigating-the-risks-and-rewards-of-a-transformative-convergence/10023.article (Accessed 23 April 2026).
TRACE (n.d.) Developing AI solutions to disrupt illicit money flows. Available at: https://trace-illicit-money-flows.eu/ (Accessed 23 April 2026).
TRACE (2025) Homepage. Available at: https://trace-illicit-money-flows.eu/ (Accessed 4 February 2025).
TRM (2025) The Rise of AI-Enabled Crime: Exploring the evolution, risks, and responses to AI-powered criminal enterprises. TRM Insights. Trmlabs.com. Available at: www.trmlabs.com/resources/blog/the-rise-of-ai-enabled-crime-exploring-the-evolution-risks-and-responses-to-ai-powered-criminal-enterprises (Accessed 23 April 2026).
Takáts, E. (2007) *A Theory of 'Crying Wolf': The Economics of Money Laundering Enforcement*. Washington, DC: International Monetary Fund.
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), p.9637.
Tangem (2025) Top 10 Real World Assets (RWA) Crypto in April 2025. Tangem Blog. Available at: https://tangem.com/en/blog/post/real-world-assets-rwa/ (Accessed 23 April 2026).
Tax Justice Network (2025) Financial Secrecy Index 2025.Tax Justice Network, 3 June. Available at: https://fsi.taxjustice.net/#scoring_id=268 (Accessed 23 April 2026).
Turksen, U., Benson, V. and Adamyk, B. (2024) Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*. doi:10.1057/s41261-024-00233-2 (Accessed 8 July 2025).
Tax Justice Network (2022, May 17) Financial Secrecy Index 2022. Available at: https://fsi.taxjustice.net/ (Accessed 4 April 2025).
Taylor, E. (2023) The CHIPS Act and US AI Leadership. *Washington Journal of Policy and Innovation*, 11(3), pp.173–198.
Taylor, M. (2023) The US CHIPS and Science Act of 2022. *MRS Bulletin*, 48.
Temelkov, Z. (2023) Overview of artificial intelligence (AI) application in the banking industry. *International Journal of Economics, Management and Tourism*, 3(2), pp.43–51.
Texas Responsible AI Governance Act (TRAIGA). (online) Available at: https://capitol.texas.gov/ (Accessed 8 July 2025).
The Danish Institute for Human Rights (2020) *Human Rights Impact Assessment Guidance and Toolbox*. Available at: www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox (Accessed 25 August 2025).
The Guardian (2025, April 29) Malta's 'golden passport' scheme ruled to be illegal by EU's top court. Available at: www.theguardian.com/world/2025/apr/29/malta-golden-passport-scheme-ruled-to-be-by-eu-top-court (Accessed 30 April 2025).
The Law Society (2020) Warning signs of money laundering. Available at: https://www.lawsociety.org.uk/topics/anti-money-laundering/money-laundering-warning-signs (Accessed 23 April 2026).
ThetaRay (2024) AI-Powered Financial Crime Detection. (online) ThetaRay. Available at: www.thetaray.com (Accessed 4 April 2025).

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Thomas, G. (2024) Politicians Move to Limit Predictive Policing After Years of Controversial Failures. Tech Policy Press, 15 October. Available at: https://www.techpolicy.press/politicians-move-to-limit-predictive-policing-after-years-of-controversial-failures/ (Accessed 23 April 2026).
Tigard, D. (2022) Embedded ethics as preparatory regulation of technology: A new solution to the Collingridge Dilemma? In Lawrence D. R. and Morley S. *Novel Beings*. Cheltenham: Edward Elgar Publishing, pp.12–28.
Tilmes, N. (2022) Disability, fairness, and algorithmic bias in AI recruitment. *Ethics and Information Technology*, 24(2), p.21.
Tombul, F. and Cakar, B. (2015) Police use of technology to fight against crime. *European Scientific Journal*, 11, pp. 286.
Transparency International (2023) Corruption Perceptions Index. (online) Available at: www.transparency.org/en/cpi/2023 (Accessed 26 February 2025).
Trmlabs.Com (2022) Illicit Crypto Ecosystem Report. Available at: https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022 (Accessed 23 April 2026).
Truby, J., Brown, R. D. and Dahdal, A. (2020) Banking on AI: Mandating a proactive approach to ai regulation in the financial sector. *Law and Financial Markets Review*, 14(2), pp.110–120.
Tsapa, J. A. (2023) Artificial Intelligence use cases for banking anti-money laundering. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 1, p.259.
Turksen, U. et al. (2023) *Tax Crimes and Enforcement in the European Union: Solutions for Law, Policy and Practice*. Oxford: Oxford University Press.
Turksen, U. et al. (2024a) 'D7.6: Recommendations for streamlining evidence collection procedures for transborder crimes' (No 101022004 – TRACE, 2024).
Turksen, U., Benson, V. and Adamyk, B. (2024) Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*, 25(4), pp.359–377.
US Congress (2024) United States Code, 2018 Edition, Supplement 5, Title 31 – Money and Finance, 31 U.S.C. 310.
US Department of Homeland Security (2024) AI Roadmap and Use Case Inventory. Washington, DC: DHS.
US Department of Homeland Security (2024) Department of Homeland Security Artificial Intelligence Roadmap 2024. Available at: https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf (Accessed 23 April 2026).
US Department of Homeland Security (2025) Artificial Intelligence Use Case Inventory Library. Available at: https://www.dhs.gov/publication/ai-use-case-inventory-library (Accessed 23 April 2026).
US Department of Justice (2024) AI in Criminal Justice: Best Practices and Cautions. Washington, DC: DOJ.
US Department of Justice (2024) Artificial Intelligence and Criminal Justice: Final Report. (online) 3 December. Available at: https://www.justice.gov/olp/media/1381796/dl (Accessed 23 April 2026).
US Department of the Treasury (2024) National Strategy for Combatting Terrorist and Other Illicit Financing. (online) May. Available at: https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf (Accessed 23 April 2026).
US House of Representatives (2024) Bipartisan House Task Force on Artificial Intelligence. (online) December. Available at: https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf (Accessed 23 April 2026).
US Treasury Department (2024) AI Use in Federal Investigations and Financial Crime. Washington, DC: US Treasury.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

UK Ministry of Defence (2018) Human-Machine Teaming, Joint Concept Note 1/18, p. 11. (online) Available at: www.gov.uk/government/publications/human-machine-teaming-jcn-118 (Accessed 9 June 2025).

UK National Cyber Security Centre (2024) *Heightened threat of state-aligned groups against western critical national infrastructure*, 1 January. Available at: www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups (Accessed 1 April 2025).

UNESCO (2023) Ethical Impact Assessment. A tool of the Recommendation on the Ethics of Artificial Intelligence. Available at: www.unesco.org/en/articles/ethical-impact-assessment-tool-recommendation-ethics-artificial-intelligence (Accessed 25 August 2025).

UNODC (2005) United Nations Convention Against Corruption. (online) Available at: www.unodc.org/unodc/en/corruption/uncac.html (Accessed 4 February 2025).

Ugwudike, P. (2022) AI audits for assessing design logics and building ethical systems: The case of predictive policing algorithms. *AI and Ethics*, 2(1), pp.199–208.

Unger, B. (2023) Reforming EU blacklisting: How to increase the effectiveness and avoid politicisation of the EU list of high-risk jurisdictions for anti-money laundering and counter-terrorism financing: US experience and considerations for EU reform. Brussels: European Parliament Committee on Economic and Monetary Affairs (ECON).

United Nations (n.d.) goAML: Anti-Money Laundering System. Available at: https://www.unodc.org/unodc/en/global-it-products/goaml.html (Accessed 23 April 2026).

United Nations (1999) International Convention for the Suppression of the Financing of Terrorism. (online) Available at: www.un.org/law/cod/finterr.htm (Accessed 4 February 2025).

United Nations (2025) Model Double Taxation Convention between Developed and Developing Countries. Available at: https://desapublications.un.org/publications/united-nations-model-double-taxation-convention-between-developed-and-developing-0 (Accessed 1 April 2025).

Uyar, T. (2024) ASI as the new god: Technocratic theocracy. *Computers and Society*, 23 March.

Vaigandla, K.K., Karne, R., Siluveru, M. and Kesoju, M. (2023) Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. *Mesopotamian Journal of CyberSecurity*, 2023, pp.73–84.

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.

Van Duyne, P.C. (2016) Money laundering: Estimates in fog. *Trends in Organized Crime*, 19, pp.199–213.

Vanclay, F. (2003) International principles for social impact assessment. *Impact Assessment and Project Appraisal*, 21(1), pp.5–12.

Vaseashta, A. (2025) Intrinsic and existential risks associated with emerging security threats from dual-use technologies. In Rocha A. and Vaseashita A. (eds). *Multidisciplinary International Conference of Research Applied to Defense and Security*. Singapore: Springer Nature Singapore, pp. 125–137.

Vasishta, P., Dhiman, A., Smith, S. and Singla, A. (2025) How can DeFi improve the quality, affordability, access and usage of financial services? A systematic literature review. *Journal of Economic and Administrative Sciences*.

Vecchietti, G., Liyanaarachchi, G. and Viglia, G. (2025) Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research*, 186, 115010.

Vedrenne, G. (2023) 'STR Volumes Rise Again in Europe, Finland Notwithstanding', ACAMS Moneylaundering.com, 22 November.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Venema, A.E. (2020) The sum of all friends: Improving cross-border intelligence sharing in Europe – the case of the Benelux. *The International Journal of Intelligence, Security, and Public Affairs*, 22(1), pp.5–19.
Vionis, P. and Kotsilieris, T. (2024) The potential of blockchain technology and smart contracts in the energy sector: A review. *Applied Sciences*, 14 (1), p.253.
Vurubindi, P. and Narahari, S.C. (2024) Encryption and decryption algorithms in private AI. In Maheswari, U.V. and Aluvalu, R. (eds.), *Sustainable Development Using Private AI: Security Models and Applications*. Boca Raton: CRC Press.
Wang, L., Xu, Y. and He, T. (2025) *Sectoral AI Regulation in China: Finance, Biometrics and Beyond*. Beijing: Tsinghua University Press.
Wang, S.X. (2024) The application of artificial intelligence-based risk management models in financial markets. *Open Journal of Social Sciences*, 12, pp.274–284.
Wang, T., Zhao, J., Yatskar, M., Chang, K.W. and Ordonez, V. (2019) Balanced datasets are not enough: Estimating and mitigating gender bias in deep image representations. In Proceedings of the IEEE/CVF international conference on computer vision, pp.5310–5319.
Wang, W.W., Zhu, L., Wang, X., Di, X. and Zhu, Y. (2025) Artificial intelligence 'law(s)' in China: Retrospect and prospect. *Journal of AI Law and Regulation*, 2(1), pp.29–36.
Wang, Y., et al. (2024) Quantum computing in community detection for anti-fraud applications. *Entropy*, 26(12), p.1026.
Werner, J. (2024) *God-Like AI and the Decentralized Internet*. Forbes, 19 June.
West, J. and Bhattacharya, M. (2016) Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, pp.47–66.
White & Case (2024) AI Watch: Global regulatory tracker – United States. Available at: https://www.jdsupra.com/legalnews/ai-watch-global-regulatory-tracker-2931403/
White & Case (2024) *The US AI Regulatory Landscape: A 2024 Review*. New York: White & Case LLP.
White & Case (2025) *State-Level AI Legislation: Trends and Impacts*. New York: White & Case LLP.
Wiggins, C. and Jones, M.L. (2023) *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. New York: W. W. Norton & Company.
World Bank (2016) Do Digital Technologies Facilitate Illicit Financial Flows? Available at: https://openknowledge.worldbank.org/entities/publication/024d74b5-a00c-51fd-aefd-60a17d491bbc (Accessed 23 April 2026).
World Bank (2017) Illicit Financial Flows. Available at: https://openknowledge.worldbank.org/entities/publication/651c0a67-39a4-5189-8bff-a2f8659d699b (Accessed 23 April 2026).
World Bank (2023) Global GDP. Available at: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (Accessed 23 April 2026).
World Economic Forum (2023) Global Cybersecurity Outlook 2023. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2023/ (Accessed 23 April 2026).
Xiang, A. (2022) Being 'seen' versus 'mis-seen': Tensions between privacy and fairness in computer vision. *Harvard Journal of Law & Technology*, 36(1), pp.1–60.
Xiang, D., Lin, Y., Nie, L., Zheng, Y., Xu, Z., Ding, Z. and Liu, Y. (2024) An empirical study of attack-related events in DeFi projects development. *Empirical Software Engineering*, 29(2), p.49.
Xue, Y.-W. and Zhang, Y.-H. (2016) 'Research on money laundering risk assessment of customers – based on the empirical research in China', *Journal of Money Laundering Control*, 19(3) pp. 249–263.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Yakhlef, S. (2023) Humour, trust, and tacit knowledge of police and border officers in international police collaboration. *Journal of Policing, Intelligence and Counter Terrorism*, 18(2), pp.174–188.

Yan, S., Kao, H. T. and Ferrara, E. (2020) Fair class balancing: Enhancing model fairness without observing sensitive attributes. In Proceedings of the 29th ACM International Conference on Information & Knowledge Management. New York: Association for Computing Machinery, pp.1715–1724.

Yao, S., Ni, H., Ma, S., Schiff, N., Myers, A.C. and Cecchetti, E. (2025) A language for smart contracts with secure control flow (technical report). arXiv.org.

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

Yeung, K., Howes, A. and Pogrebna, G. (2020) AI governance by human rights-centered design, deliberation, and oversight: An end to ethics washing. In Dubber, M., Pasquale, F. and Das, S. (eds.), *The Oxford Handbook of Ethics of AI*. Oxford: Oxford University Press, pp.76–106.

Yun, Y. and Wood, A. (2025) Timeline: How Bybit's lost Ethereum went through North Korea's washing machine. Cointelegraph. Available at: https://cointelegraph.com/news/timeline-bybit-lost-ethereum-north-korea-money-launder (Accessed 13 October 2025).

Zajko, M. (2021) Conservative AI and social inequality: conceptualizing alternatives to bias through social theory. *AI & Society* 36(3), pp.1047–1056.

Zhang, C.J., et al. (2025) AI-based identity fraud detection: A systematic review. Available at: https://doi.org/10.48550/arXiv.2501.09239.

Zhang, H.A. (2024) The promise and perils of China's regulation of artificial intelligence. *Columbia Journal of Transnational Law*, 63(1), pp.102–157.

Zhou, X. (2023) Challenges and countermeasures of artificial intelligence technology in the application of financial industry. *Advances in Economics, Management and Political Sciences*, 63(1), pp.77–82.

Zhuk, A. (2025) Beyond the blockchain hype: Addressing legal and regulatory challenges. *SN Social Sciences*, 5(2), pp.1–37.

Zilka, M., Fogliato, R., Hron, J., Butcher, B., Ashurst, C. and Weller, A. (2023) The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. New York: Association for Computing Machinery, pp.1553–1569.

Zilka, M., Sargeant, H. and Weller, A. (2022) Transparency, governance and regulation of algorithmic tools deployed in the criminal justice system: a UK case study. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society. New York: Association for Computing Machinery, pp.880–889.

Zimperium.Com (2025) Multisig Wallets. Available at: https://zimperium.com/glossary/multisig-wallets (Accessed 23 April 2026).

Zola, F., Segurola-Gil, L., Bruse, J.L., Galar, M. and Orduna-Urrutia, R. (2022) Attacking Bitcoin anonymity: Generative adversarial networks for improving Bitcoin entity classification. *Applied Intelligence*, 52(15), pp.17289–17314.

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

Index

accountability, 5, 17, 43, 59, 78, 92, 128, 153, 179, 202
AI Act, 13, 67, 101, 127, 152, 166, 203, *See* European Union (EU); regulation
ALESs, 5
algorithmic bias, 8, 78, 112, 150, 175, 204
anti-money laundering (AML), 1, 35, 141, 168, 191, 214
artificial intelligence (AI), 2, 3, 6, 12, 35, 121, 139, *See also* AIA; AI Act
Artificial Intelligence Act, 140, 203, *See also* AI Act; AIA

banking, 37, 69, 146, 169, 173, 179, 181, 194, 205, 215, *See also* financial crime risk management (FCRM)
beneficial ownership, 34, 193, 196
bias detection, 7, 26, 101, 111
bias mitigation, 111, 113, 114, 115
biometric identification, 13, 14, 203
biometrics, 12, 16, 20, 21, 22, 193, 204, *See also* facial recognition technology
blacklist, 37
blockchain, 5, 7, 72, 83, 123, 139, 140, 142, 145, 146, 149, 155, 156, 159, 160, 208, *See also* decentralised finance (DeFi); smart contracts

CBI, 8, 189, 191, 192, 198, 207, *See also* due diligence; investment migration
CBI due diligence, 203
China, 12, 15, 21, 26
crime analytics, 7, 100, 103, 106, 108, 110, 115
cross-border cooperation, 2, 17, 65, 134, 215, *See also* cross-border investigations
cross-border investigations, 7, 121, 134, 135, *See* cross-border cooperation
cryptocurrency, 5, 47, 72, 86, 151, 159
cybersecurity, 16, 73, 79, 93, 108, 157

data governance, 108, 176, 203
data protection, 13, 17, 101, 127, 176, 214, *See also* GDPR; privacy, GDPR; privacy
data quality, 22, 168, 175, 181
decentralised finance (DeFi), xi, 7, 140
deepfakes, 15, 78, 177
defence rights, 101, 102, 214
digital forensics, 21, 71, 112
dual-use technologies, 140
due diligence, 2, 8, 72, 74, 174, 191, 192, 193, 196, 202, 205, 207, *See also* citizenship by investment programmes; Know Your Customer; enhanced due diligence

enhanced due diligence, 204
European Union (EU), 1, 12, 175, 189
Europol, 1, 48, 61, 122, 133, 149, 157
evidence evaluation, 21
explainability, 17, 19, 152, 168, 180, *See also* transparency

Facial Recognition Technology (FRT), 22
fairness, 16, 17, 59, 107, 112, 113, 114, 127, 176, 179, *See* Fairness, Education, Accountability, and Transparency
Fairness, Education, Accountability, and Transparency, 8, 168
Financial Action Task Force (FATF), 33, 154, 190
financial crime, 1, 7, 8, 42, 44, 52, 60, 61, 75, 88, 90, 92, 148, 175, *See also* money laundering; crime analytics
Financial Crime Risk Management (FCRM), 8, 167
Financial Intelligence Units (FIUs), 2, 33, 35, 193
financial secrecy, 6, 33, 38
Financial Secrecy Index (FSI), 34, 43, *See also* geographic risk assessment; financial secrecy

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145

FinCEN, 6, 34, 40, 49
fraud detection, 139, 171, 174, 207
fundamental rights, xi, 13, 79, 101, 106, 115, *See also* human rights

General Data Protection Regulation (GDPR), 13, 176, 203
generative AI, 12, 16, 21, 174
geographic risk assessment, 33, 48, 215, *See also* Financial Secrecy Index (FSI); suspicious transaction reports

human oversight, 27, 151
human rights, 5, 7, 22, 107, *See also* fundamental rights

illicit financial flows, 3, 33, 192, 214
including artificial intelligence (AI), 100
information exchange, 64, 125, 126, 133
internet of things, 126, 139
interoperability, 127, 132, 155
investment migration, 192, 205

Know Your Customer, 8, 168, 191
knowledge graph, 70, 73, 75

law enforcement agencies, 2, 17, 122, 157
Law Enforcement Directive (LED), 13, 105

machine learning, 7, 36, 76, 83, 156, 204
matching exercise, 5, 107
money laundering, 33, 47, 72, 82, 172, 192, *See also* anti-money laundering (AML); financial crime

policing tools, 112, 113, 114
predictive policing, 5, 21
privacy, 6, 22, 110, 127, 150, 152, 160
profiling, 14, 39, 85, 123, 202

quantum computing, 85, 93, 123

red flags, 6, 206
regulation, 4, 18, 104, 153
risk-based approach, 13, 106, 197

safeguards, 9, 22, 114, 126, 203, 214
sanctions, 82, 149, 192, 208
Secrecy Indicators, 39, 42, 49
smart contracts, 83, 139, 142, 146, 151, 153
suspicious transaction reports, 6, 33, 59, 148

tax compliance, 190, 192, 200, 205, 206
tax evasion, 3, 36, 42, 200
TRACE project, 6, 40, 60, 79, 111, 126, 129, 134
transaction monitoring, 33, 38, 169, 215
transparency, 9, 15, 27, 42, 78, 114, 143, 145, 180, 215

United Kingdom, 12
United States of America, 12, 190

virtual assets, 2, 159

weakest link approach, 39, 49

Downloaded from https://www.cambridge.org/core. UIN Maulana Malik Ibrahim Malang, on 05 Nov 2026 at 07:25:07, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://www.cambridge.org/core/product/CF721A4CCF15C048B4E80003C398D145