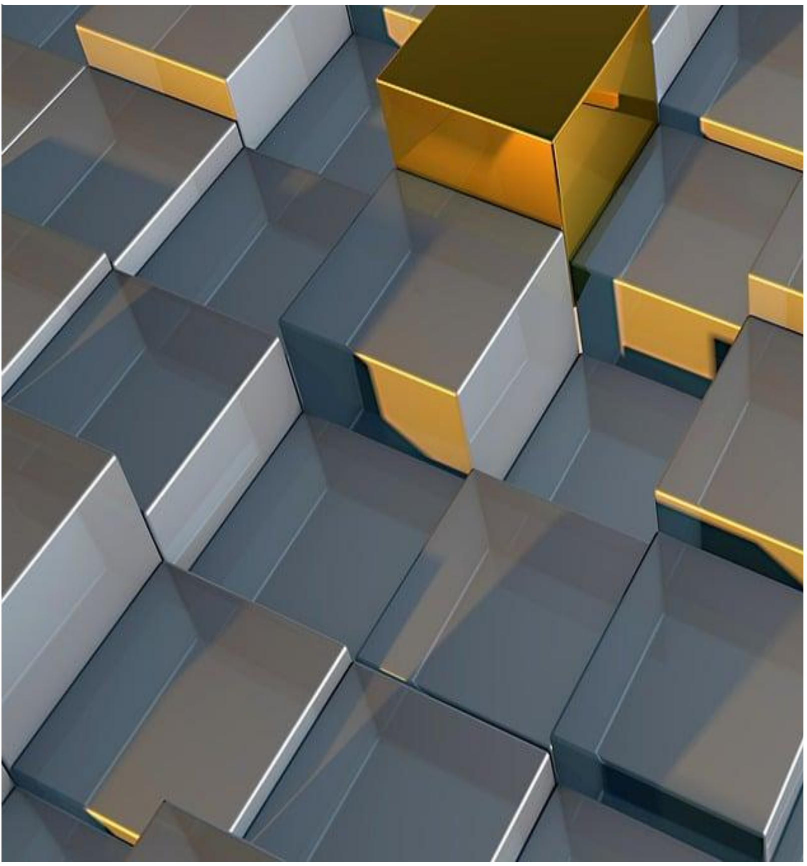
Co-funded by
the European Union

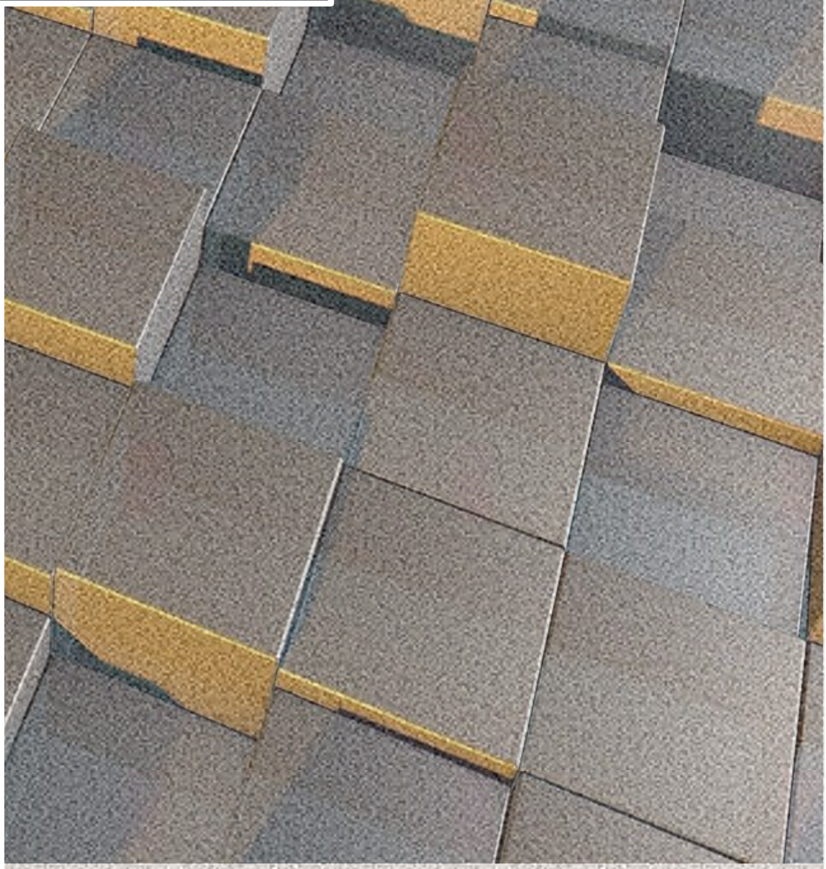
Neapolis University Pafos

Jean Monnet Center of Excellence

AI-2-TRACE-CRIME

RESEARCH HANDBOOK





Neapolis University Pafos, Cyprus
AI-2-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by
the European Union

2025

Copy Editor: G. Pavlidis

© AI-2-TRACE CRIME

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

Frontpage picture: Royalty-free picture from Pixabay

The support of the European Commission for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors; the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Table of Abbreviations

This table provides an overview of abbreviations used throughout the Research Handbook, ensuring clarity and ease of reference for readers and for team members of this research project.

Abbreviation	Full Term	Description
AI	Artificial Intelligence	A field of computer science focused on creating systems capable of performing tasks requiring human intelligence.
AML	Anti-Money Laundering	Measures and regulations aimed at detecting and preventing the laundering of illicit funds.
AMLD	Anti-Money Laundering Directive	EU legislative instruments addressing the prevention of money laundering and terrorist financing.
AROs	Asset Recovery Offices	National bodies tasked with tracing and recovering illicit assets in EU member states.
BSA	Bank Secrecy Act	U.S. legislation requiring financial institutions to report suspicious activities to combat financial crime.
CNN	Convolutional Neural Network	A type of deep learning algorithm commonly used for image recognition and processing.
DeFi	Decentralized Finance	Blockchain-based financial systems without traditional intermediaries such as banks or brokerages.
DOI	Digital Object Identifier	A unique alphanumeric string assigned to digital documents for identification and access.
EU	European Union	A political and economic union of 27 European countries.
FATF	Financial Action Task Force	An intergovernmental organization that develops policies to combat money laundering and terrorist financing.
FIU	Financial Intelligence Unit	A national agency responsible for receiving, analyzing, and disseminating financial information related to suspicious transactions.
GDPR	General Data Protection Regulation	The EU's comprehensive data protection law governing the processing of personal data.

GNN	Graph Neural Network	A type of AI model designed to analyze data represented as graphs, such as networks of transactions.
ML	Machine Learning	A subset of AI focused on developing algorithms that enable systems to learn from and make predictions based on data.
NIS Directive	Directive on Security of Network and Information Systems	An EU directive aimed at improving the cybersecurity resilience of critical infrastructure.
NLP	Natural Language Processing	A field of AI focused on the interaction between computers and human language.
SAR	Suspicious Activity Report	A report filed by financial institutions detailing potentially suspicious transactions or activities.
UNODC	United Nations Office on Drugs and Crime	A UN agency tasked with combating drugs, organized crime, corruption, and terrorism.
XAI	Explainable Artificial Intelligence	AI systems designed to provide clear and interpretable explanations for their decisions and outputs.

1. Introduction

1.1 Purpose and Scope of the Research Handbook

The Research Handbook is a deliverable of the AI-2-TRACE-CRIME project, designed to serve as a comprehensive guide to the research activities, methodologies, and key insights of the Jean Monnet Center of Excellence at Neapolis University Pafos. Its primary purpose is to document, synthesize, and disseminate the directions of interdisciplinary research conducted within the scope of the project. By doing so, the Handbook supports the overarching goal of advancing the responsible and effective use of Artificial Intelligence (AI) in asset recovery, anti-money laundering (AML), and the broader fight against crime.

The Handbook addresses a diverse audience, including academic researchers, legal practitioners, policymakers, and professionals in AI and cybersecurity. It aims to bridge the gap between theory and practice, offering insights that inform policy formulation, guide technical advancements, and enhance professional practice in the fields of AI regulation and financial crime prevention. By presenting well-researched analyses and actionable recommendations, the Handbook seeks to contribute to the development of trustworthy AI applications that uphold ethical standards, ensure accountability, and safeguard human rights.

The scope of the Research Handbook encompasses three thematic streams, which reflect the core research areas of the AI-2-TRACE-CRIME project:

1. AI and Law: This stream focuses on the legal frameworks and ethical considerations surrounding AI deployment in AML and crime prevention. The Handbook explores issues such as transparency, accountability, and compliance with human rights standards. It also examines existing legislative instruments, such as the EU's AI Act and AML Directives, and offers policy recommendations for ensuring the responsible use of AI in these contexts.

2. AI Technical Aspects: This stream delves into the technological dimensions of AI-enabled crime detection and asset recovery. The Handbook presents research on machine learning models, natural language processing, and other advanced AI techniques that can support financial institutions and law enforcement in combating financial crimes. Practical applications, such as the identification of suspicious transaction patterns and the tracing of illicit assets, are highlighted.

3. AI and Security: This stream addresses the cybersecurity implications and global security risks associated with AI. Topics include the malicious use of AI in cyberattacks, the role of AI in transnational crime, and strategies to mitigate associated risks (Blauth, Gstrein, and Zwitter, 2022). The Handbook provides a comprehensive analysis of these challenges and offers recommendations for safeguarding critical infrastructures.

In addition to these thematic streams, the Handbook integrates insights from cross-cutting issues such as interdisciplinary collaboration, stakeholder engagement, and the socio-economic impact of AI technologies. It emphasizes the need for a holistic approach to addressing the complexities of AI regulation and application in financial crime prevention.

Ultimately, the Research Handbook serves as both a compass for the project's research activities and a resource for ongoing scholarship and professional development. It aspires to inspire further research and innovation, fostering a community of practice that is committed to leveraging AI for the common good while mitigating its risks.

1.2 Alignment with AI-2-TRACE-CRIME Objectives

The Research Handbook is intricately aligned with the core objectives of the AI-2-TRACE-CRIME project, ensuring that its research activities and outcomes reinforce the overarching mission of the Jean Monnet Center of Excellence. This alignment ensures that the Handbook serves a strategic tool that advances the project's goals.

The first objective of the AI-2-TRACE-CRIME project is to enhance knowledge and awareness among students, professionals, and stakeholders. The Research Handbook contributes to this goal by providing a detailed and accessible analysis of the project's key themes: responsible AI, AML, asset recovery, and crime prevention. It translates complex academic and technical concepts into actionable insights, making them accessible to a broad audience. By doing so, the Handbook fosters a deeper understanding of the potential and challenges of AI in combating financial crimes.

The second objective focuses on contributing to the development of consistent and coherent regulations and principles in the realms of AI, AML, and crime prevention. The Handbook addresses this objective by synthesizing research directions. It critically examines existing legislative frameworks, identifies gaps and inconsistencies, and proposes forward-looking solutions that promote the responsible deployment of AI. By engaging with regulatory developments such as the EU's AI Act and AML Directives, the Handbook positions itself as a vital resource for policymakers and legal professionals.

The third objective aims to develop specialized and useful skills among future legal, IT, and AI professionals. The Research Handbook supports this by including interdisciplinary methodologies that can be directly integrated into educational programs. By emphasizing practical applications of AI technologies in AML and crime prevention, the Handbook equips readers with the knowledge and tools necessary for effective implementation in their respective fields.

Finally, the Handbook aligns with the project's objective of strengthening synergies and collaborations between academia, industry, and policymakers. It reflects the project's commitment to interdisciplinary research by incorporating contributions from law, computer science, and security studies. Moreover, the Handbook highlights collaborative efforts, such as partnerships with industry stakeholders and input from the Advisory Board, ensuring that its content is informed by diverse perspectives and expertise.

In essence, the Research Handbook is not a standalone document but a dynamic reflection of the AI-2-TRACE-CRIME project's vision and objectives. It bridges academic research with real-world applications, providing a roadmap for leveraging AI responsibly in the fight against financial crime.

1.3 Key Themes Addressed

The Research Handbook is structured around the central themes of the AI-2-TRACE-CRIME project, providing an interdisciplinary exploration of the intersection between AI, AML, asset recovery, and crime prevention. These themes are grounded in the project's three thematic streams, ensuring a comprehensive and focused approach to addressing the challenges and opportunities in these fields.

1.3.1. AI and Law

This theme examines the legal and regulatory frameworks that govern the use of AI in AML and crime prevention (Blount, 2024). Key areas of focus include:

- **Transparency and Accountability**: Exploring how AI systems can be designed and deployed to meet ethical and legal requirements for transparency and accountability.
- **Human Rights Compliance**: Analyzing the compatibility of AI technologies with fundamental human rights, including data protection, privacy, and non-discrimination (Kusche, 2024).
- **Policy and Legislative Development**: Evaluating current EU legislative instruments such as the AI Act, AML Directives, and Confiscation Directive, while proposing enhancements to ensure effective governance of AI technologies (Pagallo and Quattrocolo, 2018).

1.3.2. AI Technical Aspects

This theme delves into the technological innovations that support AML and crime prevention efforts. It highlights:

- **Machine Learning and Pattern Recognition**: Investigating AI algorithms that detect suspicious financial transactions and trace illicit assets.
- **Natural Language Processing (NLP)**: Addressing how AI can analyze large volumes of text-based data for detecting money laundering schemes.
- **Real-Time Monitoring and Automation**: Exploring tools for real-time analysis and reporting of financial anomalies, which enhance the efficiency of financial institutions and law enforcement agencies.

1.3.3. AI and Security

This theme addresses the cybersecurity and global security challenges posed by AI technologies. The focus areas include:

- **Mitigating AI-Driven Threats**: Assessing the risks of malicious AI applications, such as cyberattacks, AI-assisted fraud, and disruptions to critical infrastructures.
- **Strategic Safeguards**: Proposing strategies for governments, organizations, and law enforcement to protect against AI-enabled threats (Caldwell, 2020).
- **Geopolitical Implications**: Analyzing the role of AI in the broader context of transnational crime and security policies, particularly in combating organized criminal networks and rogue state actions.

1.3.4. Cross-Cutting Issues

In addition to the thematic streams, the Handbook addresses several overarching and interdisciplinary issues:

- **Ethical Considerations**: Emphasizing the need for AI development and deployment to adhere to ethical principles.
- **Stakeholder Engagement**: Highlighting the importance of collaboration between policymakers, industry, academia, and civil society in addressing the complexities of AI and AML (Cancela-Outeda, 2024).
- **Global Perspectives**: Offering comparative insights by examining legal, technological, and policy frameworks in jurisdictions outside the EU, such as the United States and the United Kingdom.

The Handbook's structure reflects these themes, ensuring that it provides not only theoretical insights but also practical tools and recommendations. By addressing these key themes, the Handbook equips its readers with a nuanced understanding of the opportunities and challenges at the nexus of AI and financial crime prevention, contributing to the development of responsible and effective solutions in this rapidly evolving domain.

1.4 Audience and Use

The Research Handbook is designed to serve a wide-ranging and interdisciplinary audience, ensuring its relevance and applicability across academic, professional, and policy-making domains. By tailoring its content to meet the needs of these diverse stakeholders, the Handbook aims to maximize its impact and foster meaningful contributions to the fields of AI, AML, asset recovery, and crime prevention.

1.4.1. Primary Audiences

1. **Academic Researchers and Scholars:** The Handbook provides a comprehensive resource for researchers in law, computer science, security studies, and related disciplines. It offers in-depth analyses, case studies, and comparative frameworks that facilitate further academic exploration. By presenting a synthesis of interdisciplinary research, the Handbook supports scholarship on AI ethics, AML regulation, and financial crime prevention strategies.
2. **Legal Practitioners and Policymakers**: Designed to inform the development and implementation of effective legal and policy frameworks, the Handbook addresses the practical challenges faced by lawyers, judges, regulators, and policymakers. It provides actionable insights, legislative analyses, and policy recommendations that can guide decision-making processes in AML, asset recovery, and the ethical use of AI technologies.
3. **AI and IT Professionals**: For technologists working in AI development, cybersecurity, and financial technology, the Handbook offers guidance on integrating ethical and legal principles into technical solutions. It highlights cutting-edge AI techniques for detecting financial crimes and provides insights into the broader implications of AI deployment in high-stakes environments.
4. **Students and Educators**: As a foundational resource for higher education, the Handbook is intended to support teaching and learning in disciplines such as law, AI, and security studies. It includes case studies, practical applications, and discussion points that can be integrated into curricula or used as supplementary material for specialized training programs.
5. **Industry Stakeholders and Civil Society**: The Handbook also targets stakeholders from the private sector and civil society who are interested in understanding the implications of AI in AML and crime prevention. The Handbook fosters dialogue between academic experts and non-academic audiences, ensuring its practical relevance.

1.4.2. Applications and Uses

1. **Policy Development and Advocacy:** Policymakers can use the Handbook to gain a clearer understanding of the legal, ethical, and technical dimensions of AI in AML and crime prevention. Its policy recommendations serve as a roadmap for developing regulatory frameworks that align with best practices and international standards.
2. **Research and Innovation:** The Handbook acts as a reference for ongoing and future research, encouraging innovation in both academic and professional spheres. By identifying gaps in existing knowledge and offering insights into emerging challenges, it supports the development of new methodologies, tools, and frameworks.
3. **Professional Training and Capacity Building**: Legal, technical, and law enforcement professionals can use the Handbook as part of their training programs to build skills in areas such as AI-enabled crime detection, ethical compliance, and regulatory analysis. The practical examples and case studies included in the Handbook provide valuable learning tools for professionals seeking to deepen their expertise.
4. **Public Awareness and Engagement:** For civil society and the general public, the Handbook serves as an educational tool to raise awareness of the opportunities and risks associated with AI in AML and crime prevention. Its accessible language and clear structure ensure that its findings can be understood and appreciated by non-specialist audiences.

By addressing the needs of these varied audiences, the Research Handbook establishes itself as an indispensable resource for advancing knowledge, shaping policy, and promoting collaboration in the responsible use of AI technologies to combat financial crime.

2. Research Framework

2.1 Overview of Thematic Streams

The Research Handbook is structured around three thematic streams that represent the core areas of research within the AI-2-TRACE-CRIME project. Each thematic stream explores specific aspects of the interdisciplinary nexus between AI, law, and crime prevention, ensuring a holistic approach to addressing the project's objectives.

2.1.1 AI and Law

This thematic stream focuses on the legal and regulatory frameworks governing the use of AI in AML, asset recovery, and crime prevention. It examines how existing legal instruments can adapt to address the ethical, social, and practical challenges posed by AI technologies.

Key Topics:

1. **Accountability and Transparency**: Analyzing how AI systems can meet requirements for explainability and accountability, particularly in high-stakes applications like AML (Pavlidis, 2023).
2. **Human Rights Compliance**: Investigating the alignment of AI technologies with data protection laws, privacy regulations, and anti-discrimination principles.
3. **Legislative Instruments**: Examining relevant EU regulations, including the AI Act, AML Directives, and Confiscation Directive, to assess their adequacy in addressing AI-related risks and opportunities.
4. **Ethical Governance**: Proposing frameworks to ensure the ethical deployment of AI while balancing innovation and risk mitigation.

Objectives:

- Develop policy recommendations for a coherent legal framework.
- Address gaps in legislation related to the deployment of AI in financial crime prevention.
- Highlight best practices for ensuring the responsible and human-centric use of AI.

2.1.2 AI Technical Aspects

This stream delves into the technological dimensions of AI as applied to AML, asset recovery, and crime detection. It focuses on leveraging advanced AI tools to enhance the effectiveness of financial institutions and law enforcement agencies.

Key Topics:

1. **AI Algorithms and Models**: Exploring machine learning techniques, such as deep learning and natural language processing (NLP), for identifying suspicious financial transactions and patterns of illicit activity.
2. **Data-Driven Decision Making**: Evaluating the role of AI in automating and improving decision-making processes in financial crime detection.
3. **Technical Challenges**: Addressing issues like bias in AI models (Barabas, 2020), data quality, and the scalability of AI solutions for diverse operational contexts.
4. **AI in Real-Time Applications**: Investigating how AI can support real-time monitoring, anomaly detection, and automatic reporting for financial institutions.

Objectives:

- Advance the technical capabilities of AI tools for crime prevention.
- Bridge gap between AI developers and end-users, financial institutions, law enforcement.
- Explore novel approaches to tracing and recovering illicit financial assets.

2.1.3 AI and Security

The third thematic stream focuses on the implications of AI in cybersecurity and global security contexts, particularly in its application to combating transnational and organized crime (Helm and Hagendorff, 2021).

Key Topics:

1. **Cybersecurity Threats**: Assessing risks such as AI-driven cyberattacks, fraud, and disruption of critical infrastructures.
2. **Malicious Use of AI**: Exploring how rogue states, terrorist organizations, and criminal networks exploit AI for unlawful activities.
3. **Mitigation Strategies**: Proposing defensive strategies and frameworks to safeguard against AI-driven threats.
4. **Geopolitical Implications**: Examining the role of AI in shaping international security policies and transnational crime prevention.

Objectives:

- Evaluate the global security risks associated with AI applications.
- Propose actionable strategies to mitigate cybersecurity threats.

2.1.4 Cross-Cutting Themes

Although each thematic stream has a distinct focus, they are interconnected through cross-cutting themes that address overarching challenges and opportunities:

1. **Interdisciplinary Integration**: Combining insights from law, computer science, and security studies to provide holistic solutions.
2. **Ethical and Social Implications**: Highlighting the need for AI systems that prioritize fairness, inclusivity, and societal well-being.
3. **Comparative Analysis**: Drawing lessons from regulatory and technological frameworks in jurisdictions beyond the EU, such as the United States and the United Kingdom.

The thematic streams collectively ensure that the Research Handbook provides a thorough exploration of the key dimensions of AI and its application in combating financial crime. By addressing these areas, the Handbook aligns with the project's goals of fostering interdisciplinary research, developing policy frameworks, and advancing technical innovation.

2.2 Guiding Research Objectives

The Research Handbook is driven by a set of guiding research objectives that align with the overarching aims of the AI-2-TRACE-CRIME project. These objectives reflect the interdisciplinary nature of the project, ensuring that the research is comprehensive, relevant, and impactful in addressing the challenges and opportunities at the nexus of AI, AML, asset recovery, and crime prevention.

2.2.1. Advance Knowledge on AI Governance

The Handbook aims to deepen the understanding of regulatory and ethical frameworks governing AI applications in AML and crime prevention. This includes:

- **Identifying Legal Gaps**: Analyzing existing legislative instruments to highlight areas that require refinement or augmentation.
- **Proposing Policy Recommendations**: Offering actionable suggestions to create coherent and robust governance frameworks that balance innovation with ethical and legal compliance.
- **Fostering Human-Centric AI**: Emphasizing the importance of transparency, accountability, and human rights in the deployment of AI technologies.

2.2.2 Enhance Technological Effectiveness

The Handbook focuses on advancing the technical capabilities of AI to address financial crimes effectively. The research objectives include:

- **Developing Advanced Tools**: Investigating cutting-edge AI techniques, such as machine learning and natural language processing, to improve the detection of financial anomalies and illicit activities.
- **Exploring Real-Time Applications**: Identifying ways to integrate AI into real-time systems for crime detection, monitoring, and reporting.
- **Addressing Technical Challenges**: Tackling issues related to AI biases, data quality, and the scalability of solutions in diverse environments.

2.2.3. Mitigate Security Risks

The Handbook addresses the global and cybersecurity risks associated with AI technologies. Research in this area seeks to:

- **Assess Malicious Use of AI**: Investigate how AI could be exploited by rogue states, criminal organizations, and other malicious actors.
- **Develop Mitigation Strategies**: Propose frameworks and best practices to safeguard against AI-driven threats, including cyberattacks and fraud (King et al, 2020)
- **Evaluate Global Implications**: Analyze the broader geopolitical impact of AI in crime prevention and security, fostering international collaboration to combat transnational challenges.

2.2.4. Foster Interdisciplinary Collaboration

Recognizing the complexity of the challenges addressed, the Handbook promotes a collaborative approach that bridges multiple disciplines, including law, computer science, and security studies. Objectives include:

- **Integrating Perspectives**: Combining insights from different fields to provide comprehensive solutions.
- **Encouraging Stakeholder Engagement**: Actively involving policymakers, industry leaders, and civil society in shaping the research agenda.
- **Promoting Capacity Building**: Equipping researchers and professionals with interdisciplinary tools and methodologies.

2.2.5. Contribute to Policy and Practice

The Handbook seeks to translate academic research into practical applications that influence both policy and professional practice. Specific objectives include:

- **Providing Practical Insights**: Offering actionable recommendations that can inform decision-making processes.
- **Supporting Professional Development**: Enhancing the skills of legal, IT, and AML professionals through insights into AI-enabled tools and strategies.
- **Raising Awareness**: Educating the public and stakeholders about the ethical, legal, and technical dimensions of AI in crime prevention.

These guiding research objectives ensure that the Handbook not only contributes to academic scholarship but also supports improvements in governance, technology, security, and professional practice. By aligning these objectives with the thematic streams of the AI-2-TRACE-CRIME project, the Handbook becomes a useful resource for addressing the challenges of deploying AI responsibly and effectively in combating financial crime.

2.3 Methodological Approaches

The Research Handbook adopts a comprehensive methodological framework to address the interdisciplinary challenges of AI in AML, asset recovery, and crime prevention. The chosen methodologies reflect the need for a balanced integration of legal, technical, and policy-oriented perspectives, ensuring that the research is both rigorous and applicable.

2.3.1 Interdisciplinary Elements

Interdisciplinary research is an important element of the AI-2-TRACE-CRIME project. The Handbook emphasizes collaboration between diverse fields, including law, computer science, and security studies, to provide holistic insights and solutions.

Key Approaches:

1. **Cross-Disciplinary Dialogue**: Regular workshops, seminars, and collaborative research sessions involving experts from varied domains to integrate their perspectives.
2. **Integrated Frameworks**: Combining legal analysis with technical insights to develop comprehensive models for AI regulation and application.
3. **Joint Outputs**: Producing outputs, such as case studies and policy briefs, that reflect contributions from multiple disciplines.

2.3.2 Quantitative and Empirical Research

Quantitative methodologies form a critical part of the Handbook, focusing on the statistical and data-driven dimensions of AI in AML and crime prevention.

Key Approaches:

1. **Data Analysis**: Examining trends and typologies of financial crimes using datasets from institutions such as Financial Intelligence Units (FIUs) and Asset Recovery Offices (AROs).
2. **AI Performance Metrics**: Evaluating the effectiveness and accuracy of AI tools in detecting and tracing illicit activities.
3. **Impact Assessment**: Using empirical methods to assess the socio-economic and operational impact of AI technologies in AML and crime prevention (Nerantzi and Sartor, 2024).

2.3.3 Qualitative Research

Qualitative methods complement quantitative approaches, offering a deeper understanding of the legal, ethical, and societal implications of AI.

Key Approaches:

1. **Doctrinal Legal Analysis**: Systematic examination of existing legislative instruments, case law, and regulatory frameworks related to AI and financial crimes (Lagioia and Sartor, 2020).
2. **Ethical Evaluations**: Investigating the moral dimensions of AI deployment, including privacy concerns, fairness, and human-centric design.
3. **Stakeholder Interviews**: Conducting qualitative interviews with policymakers, legal practitioners, and industry professionals to gather insights on challenges and best practices.

2.3.4 Comparative Analysis

Comparative research is important for evaluating the effectiveness of AI regulations and applications across jurisdictions.

Key Approaches:

1. **EU vs. Non-EU Jurisdictions**: Comparing EU legislative frameworks with those in the United States, the United Kingdom, and other regions to identify best practices and lessons learned.
2. **Cross-Cultural Perspectives**: Assessing how cultural and legal differences influence the adoption and governance of AI technologies.
3. **Benchmarking**: Using comparative data to establish benchmarks for evaluating AI performance and regulatory adequacy.

2.3.5 Collaborative and Participatory Methods

Engagement with stakeholders is central to the Handbook's methodology, ensuring that research outputs are practical and informed by real-world perspectives.

Key Approaches:

1. **Advisory Board Input**: Leveraging expertise from the project's Advisory Board to guide research priorities and validate findings.
2. **Stakeholder Workshops**: Organizing participatory sessions with financial institutions, law enforcement, and regulatory bodies to refine methodologies and outputs.
3. **Public Consultations**: Involving civil society and industry representatives to ensure the inclusivity and relevance of research conclusions.

2.3.6 Risk-Based Approach

Given the dynamic nature of AI and its applications, a risk-based methodology is essential for anticipating and addressing potential challenges.

Key Approaches:

1. **Risk Identification**: Analyzing potential risks associated with AI, including biases in algorithms, cybersecurity vulnerabilities, and ethical dilemmas (Chiappetta, 2023).
2. **Scenario Planning**: Developing hypothetical scenarios to test the resilience and adaptability of proposed AI frameworks.
3. **Mitigation Strategies**: Proposing actionable measures to address identified risks and ensure the safe deployment of AI technologies.

3. Research Themes and Areas

3.1 Legal and Ethical Dimensions of AI in AML and Asset Recovery

AI has emerged as a transformative tool in the fight against financial crime, offering unprecedented capabilities for detecting and mitigating illicit activities. However, its deployment in AML and asset recovery efforts raises significant legal and ethical concerns. This section addresses these dimensions, emphasizing the need for robust governance frameworks that ensure AI's responsible use while safeguarding fundamental rights.

3.1.1. Legal Dimensions

AI technologies in AML and asset recovery operate within a complex legal landscape that must balance innovation with compliance. Key considerations include:

Transparency and Accountability

- **Challenges**: Many AI systems, particularly those using machine learning, function as "black boxes," making their decision-making processes opaque. This lack of transparency complicates regulatory oversight and challenges principles of accountability.
- **Proposed Solutions**: Implementing explainability requirements, where AI systems must provide clear, understandable justifications for their outputs. This can be supported by provisions in the EU's AI Act that address high-risk AI systems (Bomhard and Merkle, 2021).

Compliance with Data Protection Laws

- **Challenges**: AI systems in AML often process large volumes of personal data, raising concerns about compliance with data protection regulations such as the EU General Data Protection Regulation (GDPR).
- **Proposed Solutions**: Adopting privacy-by-design approaches to AI system development, ensuring that data minimization, purpose limitation, and security measures are embedded from the outset.

Anti-Discrimination and Fairness

- **Challenges**: Bias in AI algorithms can lead to discriminatory practices, disproportionately affecting certain groups based on race, ethnicity, or socioeconomic status.
- **Proposed Solutions**: Conducting bias audits and impact assessments to identify and mitigate potential sources of discrimination in AI systems.

Legal Certainty and Harmonization

- **Challenges**: The rapid evolution of AI technologies often outpaces legislative developments, creating uncertainty for stakeholders.
- **Proposed Solutions**: Developing consistent legal frameworks at the EU level, such as the harmonization efforts reflected in the AI Act, AML Directives, and the Confiscation Directive (Veale and Borgesius, 2021; Wachter, 2023).

3.1.2. Ethical Dimensions

Ethical considerations are integral to the deployment of AI in AML and asset recovery, as these technologies significantly impact individual rights and societal trust.

Respect for Human Rights

- **Challenges**: AI systems must align with fundamental rights, such as privacy, freedom from discrimination, and due process (Pehlivan, 2024)
- **Proposed Solutions**: Establishing ethical guidelines and oversight mechanisms to ensure that AI systems respect human rights in both design and operation.

Balancing Efficiency and Privacy

- **Challenges**: AI can enhance efficiency in detecting financial crimes but often at the cost of increased surveillance and reduced individual privacy.
- **Proposed Solutions**: Employing privacy-preserving AI techniques, such as federated learning and differential privacy, to strike a balance between operational efficiency and personal privacy.

Public Trust and Perception

- **Challenges**: The use of AI in sensitive domains like AML can erode public trust if perceived as intrusive or unfair.
- **Proposed Solutions**: Enhancing transparency, public communication, and stakeholder engagement to build trust and demonstrate the benefits of AI technologies.

Ethical Governance and Oversight

- **Challenges**: Ensuring that AI systems operate within ethical boundaries requires ongoing monitoring and governance.
- **Proposed Solutions**: Establishing multidisciplinary ethics committees and advisory boards to oversee AI deployment and ensure alignment with societal values.

3.1.3. Integrative Approaches

The legal and ethical dimensions of AI in AML and asset recovery are deeply interconnected. For AI technologies to achieve their full potential while minimizing risks, stakeholders must adopt integrative approaches that embed legal compliance and ethical considerations into every stage of the AI lifecycle—from design to deployment and monitoring.

By addressing these dimensions, this section underscores the critical importance of a human-centric approach to AI governance, ensuring that the use of AI in AML and asset recovery not only complies with legal standards but also promotes fairness, accountability, and societal trust.

3.2 Advanced AI Techniques for Crime Detection

AI offers powerful tools for enhancing the detection and prevention of financial crimes, such as money laundering and illicit asset transfers. This section explores advanced AI techniques that have been developed or adapted for crime detection, emphasizing their application in AML and asset recovery contexts. It also highlights the technical challenges and innovations that define this rapidly evolving field.

3.2.1. Key AI Techniques

The following advanced AI methods have proven instrumental in detecting complex patterns and anomalies associated with financial crimes:

Machine Learning and Predictive Analytics

- **Application**: Machine learning (ML) models can analyze vast amounts of transactional data to identify patterns indicative of money laundering or fraud.
- **Examples**:
    - **Anomaly Detection**: ML algorithms flag unusual transaction patterns that may indicate illicit activity.
    - **Predictive Models**: These models assess the likelihood of future criminal behavior based on historical data (Joseph, 2025; Perrot, 2017).
- **Advancements**: Use of unsupervised learning techniques, such as clustering, to detect previously unknown patterns of financial crime.

Natural Language Processing (NLP)

- **Application**: NLP enables the analysis of unstructured textual data, such as regulatory reports, customer reviews, and news articles, to uncover insights relevant to AML and asset recovery.
- **Examples**:
    - Extracting entities (e.g., names, organizations) from documents to trace illicit actors.
    - Analyzing Suspicious Activity Reports (SARs) for trends or common elements.
- **Advancements**: Improved NLP models enable more accurate and context-aware analysis.

Graph-Based Analysis

- **Application**: Graph-based techniques model relationships between entities (e.g., individuals, accounts, organizations) to uncover networks of criminal activity.
- **Examples**:
    - Constructing relationship graphs to identify connections between seemingly unrelated transactions.
    - Detecting money laundering rings or shell companies through graph traversal algorithms.
- **Advancements**: Integration of graph neural networks (GNNs) for more sophisticated analysis of large, interconnected datasets.

Computer Vision

- **Application**: Computer vision is used in the context of asset recovery to analyze images, videos, or other visual data.
- **Examples**:
  - Identifying luxury assets (e.g., real estate, vehicles, artwork) linked to financial crimes.
  - Monitoring physical locations for evidence of illicit activities.
- **Advancements**: Use of deep learning models for high-accuracy image recognition and classification.

Real-Time Monitoring and Automation

- **Application**: AI systems enable the continuous monitoring of transactions and the automation of reporting processes.
- **Examples**:
  - Real-time flagging of high-risk transactions for further review.
  - Automatic generation of compliance reports for regulatory bodies.
- **Advancements**: Combining AI with blockchain technology to ensure transparency and immutability in transaction monitoring.

3.2.2. Challenges in Implementation

While AI techniques offer significant benefits, their deployment in crime detection is not without challenges:

- **Data Quality and Availability**: AI systems require access to large, high-quality datasets, which may not always be available due to privacy regulations or inconsistent reporting practices.
- **Bias and Fairness**: Algorithms may inadvertently reflect biases present in the training data, leading to unfair or inaccurate outcomes (Hacker, 2021).
- **Scalability**: Adapting AI systems to handle the growing complexity and volume of financial transactions is a technical hurdle.
- **Explainability**: Ensuring that AI systems provide interpretable results is critical for regulatory compliance and stakeholder trust (Pavlidis, 2024)

3.2.3. Opportunities and Innovations

Despite these challenges, ongoing innovations in AI are expanding its potential in crime detection:

1. **Federated Learning**: Enabling collaborative model training across institutions without sharing sensitive data.
2. **Differential Privacy**: Incorporating mechanisms to protect individual privacy while allowing for robust data analysis.
3. **Hybrid Models**: Combining rule-based systems with machine learning to leverage the strengths of both approaches.
4. **AI-Augmented Human Review**: Using AI to pre-screen and prioritize cases for human investigators, improving efficiency and accuracy.

3.2.4. Future Directions

Research and development in this area are expected to focus on:

- Enhanced interoperability between AI systems and existing AML frameworks.
- Development of domain-specific AI models tailored to financial crime detection.
- Collaboration between AI researchers, financial institutions, and regulatory bodies to standardize best practices.

By leveraging these advanced techniques, the fight against financial crime can become more proactive and effective, ultimately reducing illicit activities and enhancing the integrity of global financial systems.

3.3 Cybersecurity Risks and Responses to AI Exploitation

The integration of AI in AML, asset recovery, and crime prevention introduces significant cybersecurity challenges. AI systems, while offering powerful tools to combat financial crimes, can also be exploited by malicious actors. This section examines the cybersecurity risks associated with AI, including the malicious use of AI technologies, and proposes strategies to mitigate these threats and strengthen resilience.

3.3.1. Cybersecurity Risks Associated with AI

AI technologies, like any other transformative tools, can become double-edged swords when misused. Key risks include:

Malicious Use of AI

- **AI-Driven Cyberattacks**: Threat actors use AI to automate and enhance cyberattacks, such as phishing campaigns, malware deployment, and denial-of-service (DoS) attacks.
- **Deepfakes and Disinformation**: AI-generated fake content, such as videos or documents, can be used to manipulate public perception, commit fraud, or discredit individuals and organizations.
- **AI-Assisted Evasion Tactics**: Criminals use AI to evade detection by learning the patterns of AML and monitoring systems.

Vulnerabilities in AI Systems

- **Data Poisoning**: Adversaries manipulate training datasets to introduce biases or vulnerabilities in AI models, leading to incorrect predictions or outcomes.
- **Model Inference Attacks**: These attacks exploit AI systems to extract sensitive information about the underlying data or model.
- **Adversarial Attacks**: Malicious actors craft inputs designed to deceive AI systems, causing them to misclassify or fail.

Exploitation by Transnational Criminal Networks

- **Coordination of Criminal Activities**: AI enables the optimization of logistics for illicit activities, such as trafficking or money laundering, across borders.
- **Weaponization by Rogue States**: AI-powered cyberweapons can disrupt critical infrastructure, financial systems, and national security frameworks.

3.3.2. Responses to AI Exploitation

To address these risks, proactive and collaborative strategies are essential. Key responses include:

Strengthening AI System Security

- **Robust Model Training**: Ensuring the use of high-quality, unbiased datasets and implementing rigorous validation processes to detect and mitigate vulnerabilities.
- **Adversarial Testing**: Regularly testing AI systems against adversarial attacks to identify weaknesses and strengthen defenses.
- **Encryption and Privacy Mechanisms**: Using techniques like homomorphic encryption and differential privacy to protect sensitive data in AI systems.

Regulatory and Policy Frameworks

- **Establishing Standards**: Developing international standards for the secure development and deployment of AI technologies, ensuring interoperability and compliance.
- **AI-Specific Cybersecurity Policies**: Introducing policies that address the unique risks of AI, such as mandatory reporting of AI-related breaches and incidents.
- **Alignment with Existing Frameworks**: Integrating AI-specific measures with broader cybersecurity regulations, such as the EU's NIS Directive and GDPR.

Collaboration and Information Sharing

- **Public-Private Partnerships**: Encouraging collaboration between governments, industry, and academia to share knowledge, resources, and best practices for securing AI systems.
- **International Cooperation**: Facilitating cross-border collaboration to address the global nature of AI-related threats and harmonize cybersecurity standards.
- **Threat Intelligence Sharing**: Establishing platforms for real-time exchange of threat intelligence related to AI exploitation.

Development of Defensive AI Tools

- **AI for Threat Detection**: Deploying AI systems that monitor networks for anomalies and detect potential cyber threats in real time.
- **AI for Cybersecurity Training**: Using AI to simulate attack scenarios and train cybersecurity professionals in identifying and responding to threats.
- **AI-Enhanced Incident Response**: Leveraging AI to automate parts of the incident response process, reducing reaction times and mitigating damage.

3.3.3. Future Directions and Recommendations

1. **Investment in Research**: Supporting research on AI security, particularly in understanding and mitigating adversarial and poisoning attacks.
2. **Cybersecurity-By-Design**: Embedding security measures into the development process of AI systems to prevent vulnerabilities from emerging.
3. **Education and Awareness**: Training stakeholders, including developers, policymakers, and end-users, on the risks and responsibilities of using AI technologies.
4. **Resilience Planning**: Developing contingency plans for scenarios involving AI exploitation, including coordinated responses to large-scale incidents.

By addressing these cybersecurity risks and implementing robust defenses, stakeholders can ensure that AI technologies contribute positively to AML, asset recovery, and crime prevention efforts. This approach not only safeguards the integrity of AI systems but also strengthens trust and resilience in the broader digital ecosystem (Pavlidis, 2021).

3.4 Comparative Analysis: EU vs. Non-EU Jurisdictions

The regulation and application of AI in AML, asset recovery, and crime prevention vary significantly across jurisdictions. A comparative analysis between the European Union (EU) and non-EU jurisdictions, such as the United States (US) and the United Kingdom (UK), highlights differences in legislative frameworks, regulatory approaches, and operational practices. This section explores these differences and identifies lessons that can be drawn to enhance AI governance and deployment globally.

3.4.1. AI Regulation and Governance Frameworks

European Union (EU)

- **Legislative Instruments**: The EU's **AI Act** establishes a risk-based approach to AI regulation, categorizing AI systems into unacceptable, high-risk, and lower-risk categories (Ebers, 2025). AML and crime prevention systems are typically classified as high-risk. The **AML Directives** and the **Confiscation Directive** provide a robust legal foundation for tackling financial crimes, including provisions for integrating AI tools.
- **Focus on Ethics and Human Rights**: The EU emphasizes human-centric AI, with strong protections for data privacy (e.g., GDPR) and accountability mechanisms. Transparency and fairness are prioritized, requiring high-risk AI systems to meet stringent explainability and bias mitigation standards.

United States (US)

- **Sectoral Approach**: The US lacks a comprehensive AI regulatory framework, relying instead on sector-specific laws and guidelines. For example, financial institutions use AI under the oversight of agencies such as the Financial Crimes Enforcement Network (FinCEN). The **Bank Secrecy Act (BSA)** mandates reporting and monitoring for AML purposes but does not provide AI-specific guidance.
- **Innovation-Centric Focus**: US regulation leans towards promoting innovation and competitiveness, often prioritizing economic considerations over strict ethical or human rights requirements. AI governance often relies on industry-led standards and self-regulation, which may lack uniformity.

United Kingdom (UK)

- **Hybrid Approach**: The UK combines elements of the EU's regulatory rigor and the US's innovation-driven ethos. It is developing its own AI-specific strategies post-Brexit. The UK's **Economic Crime Plan** highlights the integration of AI into AML strategies while emphasizing accountability and oversight.
- **Regulatory Sandboxes**: The UK promotes innovation through sandboxes allowing safe testing of AI technologies for financial crime detection.

3.4.2. Comparative Insights

Approach to Risk Management

- **EU**: A risk-based, precautionary approach that ensures strict oversight of high-risk AI applications (Neuwirth, 2023).
- **US**: A reactive approach focused on addressing risks as they arise, with minimal preemptive regulation.
- **UK**: A balanced approach that encourages safe experimentation while ensuring accountability.

Privacy and Data Protection

- **EU**: Comprehensive privacy regulations under GDPR, imposing stringent controls on data collection and processing.
- **US**: Patchy privacy protections, with variations across states and sectors, resulting in less consistency.
- **UK**: Maintains GDPR-aligned standards post-Brexit, ensuring strong privacy protections alongside flexibility for innovation.

Ethical Considerations

- **EU**: Prioritizes ethical AI deployment, integrating principles of fairness, non-discrimination, and respect for fundamental rights.
- **US**: Ethical considerations are often secondary to economic and technological priorities, relying on voluntary ethical guidelines.
- **UK**: Adopts a pragmatic approach, emphasizing ethics but allowing flexibility to accommodate industry needs.

3.4.3. Best Practices and Lessons Learned

1. **Comprehensive Regulation (EU)**: The EU's holistic regulatory framework ensures consistency and clarity, providing a model for balancing innovation with accountability. Non-EU jurisdictions can adopt risk-based classification systems for AI applications, tailored to their specific legal and operational contexts.
2. **Innovation-Driven Strategies (US)**: The US approach encourages rapid technological advancements by minimizing regulatory barriers. The EU and UK can incorporate elements of this innovation-centric focus by promoting regulatory sandboxes (Buocz, Pfotenhauer and Eisenberger, 2023) and public-private partnerships.
3. **Balanced Flexibility (UK)**: The idea to use sandboxes and targeted AI strategies strikes a balance between innovation and regulation. Both the EU and US can benefit from such initiatives to test and refine AI tools in controlled environments.

3.4.4. Future Directions for Harmonization

1. **International Standards**: Developing global AI standards under the auspices of organizations like the Financial Action Task Force (FATF) and the International Telecommunication Union (ITU).
2. **Cross-Border Collaboration**: Encouraging dialogue and cooperation among jurisdictions to share knowledge, best practices, and regulatory innovations.
3. **Adapting to Emerging Trends**: Regularly updating legal and technical frameworks to address the evolving challenges of AI in AML and asset recovery.

By examining the strengths and weaknesses of AI governance and application in different jurisdictions, this comparative analysis underscores the need for adaptive, collaborative, and globally informed approaches to AI regulation. Such strategies can ensure the effective and ethical use of AI technologies in the fight against financial crime.

4. Key Insights

4.1 Proposed Legal Frameworks and Policies

The effective deployment of AI in AML, asset recovery, and crime prevention necessitates robust legal frameworks and policies that address the unique challenges posed by these technologies. This section outlines proposed legal frameworks and policy recommendations developed within the AI-2-TRACE-CRIME project, focusing on fostering innovation while ensuring compliance, fairness, and accountability.

4.1.1. Key Principles for AI Legal Frameworks

The following principles must underpin the relevant legal frameworks and policies:

1. **Transparency**: AI systems used in AML and crime prevention must be transparent, enabling regulators, stakeholders, and the public to understand their processes and outcomes. This includes requirements for explainability and interpretability of AI models.
2. **Accountability**: Clear accountability mechanisms are essential to ensure that entities deploying AI can be held responsible for its outcomes. This includes assigning liability in cases of errors, biases, or system failures.
3. **Proportionality**: Legal measures should balance the need for effective crime prevention with respect for individual rights, avoiding excessive surveillance or infringement on privacy.
4. **Adaptability**: Frameworks must be flexible to accommodate the rapid evolution of AI technologies, ensuring relevance and effectiveness over time.

4.1.2. Proposed Legal Frameworks

Risk-Based Regulation

- **Description**: A framework that categorizes AI systems based on the risks they pose to individuals, institutions, and society.
- **Application in AML**: High-risk systems, such as those monitoring large financial transactions, must be subject to stricter regulatory oversight, including regular audits and impact assessments (Novelli et al, 2024b).
- **Examples**: Aligning with the EU's AI Act, this approach ensures proportionality by focusing regulatory efforts on the most critical applications (Novelli et al, 2024a)

Privacy-Enhancing Frameworks

- **Description**: Policies that embed data protection principles into the design and operation of AI systems.

- **Provisions**: Ensuring compliance with GDPR through data minimization, purpose limitation, and secure processing; promoting privacy-preserving technologies such as federated learning and differential privacy to protect individual data.
- **Outcomes**: Enhanced trust and reduced resistance to AI adoption in sensitive domains.

Bias Mitigation and Fairness

- **Description**: Legal obligations to identify, disclose, and mitigate biases in AI systems.
- **Key Measures**: Mandatory bias audits for AI tools used in financial crime detection; requirements for diverse and representative training datasets.
- **Impact**: Increased fairness and reduced risk of discriminatory practices.

Accountability and Governance Structures

- **Description**: Establishing governance frameworks to oversee the ethical and legal use of AI.
- **Key Components**: Independent oversight bodies to monitor AI systems and enforce compliance; clear guidelines on liability and redress mechanisms for affected parties (Hallevy, 2015).
- **Outcomes**: Greater confidence in AI systems and their operators.

4.1.3. Policy Recommendations

Harmonization Across Jurisdictions

- **Challenge**: Inconsistent regulations across regions create barriers to the global deployment of AI technologies.
- **Recommendation**: Promote international alignment through frameworks such as the Financial Action Task Force (FATF) and bilateral agreements between the EU, US, and UK.

Incentivizing Ethical Innovation

- **Challenge**: Overly restrictive regulations may stifle innovation.
- **Recommendation**: Introduce regulatory sandboxes to allow for experimentation with AI applications under controlled conditions while ensuring adherence to ethical principles.

Capacity Building and Education

- **Challenge**: Limited understanding of AI among regulators and policymakers can hinder effective governance.
- **Recommendation**: Invest in training programs and resources for regulators, focusing on the technical, ethical, and legal dimensions of AI.

Stakeholder Engagement

- **Challenge**: Exclusion of key stakeholders may result in frameworks that are impractical or misaligned with industry needs.

- **Recommendation**: Encourage inclusive consultations with financial institutions, AI developers, civil society, and the public during the drafting of policies.

4.1.4. Implementation Strategies

To ensure the effective adoption of these frameworks and policies:

1. **Legislative Alignment**: Integrate AI-specific provisions into existing AML directives and financial crime regulations.
2. **Dynamic Monitoring**: Establish adaptive regulatory bodies that can respond to technological advancements and emerging threats.
3. **International Collaboration**: Leverage global forums to share knowledge, harmonize standards, and address transnational challenges.

By adopting these proposed frameworks and policies, jurisdictions can create a supportive yet secure environment for AI innovation in AML and crime prevention. These measures will enhance the integrity of financial systems, safeguard fundamental rights, and promote public trust in AI technologies.

4.2 AI Models for Financial Crime Detection

AI models are at the forefront of technological innovations in detecting and combating financial crimes, including money laundering, fraud, and illicit asset transfers (Yeoh, 2019; Hayward and Maas, 2021). This section highlights key AI models used in financial crime detection, their applications, challenges, and opportunities for enhancing their effectiveness within the contexts of AML and asset recovery.

4.2.1. Key AI Models and Their Applications

Several AI models have been developed or adapted to address the complexities of financial crime detection. These models leverage data analysis, machine learning, and automation to identify suspicious patterns and activities (Raja, Yuvaraj and Kousik, 2021).

Supervised Learning Models

- **Description**: These models are trained on labeled datasets, enabling them to predict outcomes based on known patterns.
- **Applications**: Detecting fraudulent transactions by learning from historical data; identifying high-risk customers based on previous suspicious activity reports (SARs).
- **Examples**: Logistic regression and decision trees for binary classification tasks (e.g., flagging transactions as fraudulent or legitimate); random forests and gradient boosting models for more complex classification problems.

Unsupervised Learning Models

- **Description**: These models analyze data without predefined labels, making them ideal for uncovering unknown patterns.
- **Applications**: Detecting anomalies in transaction data that may indicate money laundering schemes; clustering accounts or entities to identify networks involved in illicit activities.
- **Examples**: K-means clustering for grouping similar transactions; autoencoders for anomaly detection.

Deep Learning Models

- **Description**: Advanced neural network architectures capable of processing large and complex datasets.
- **Applications**: Natural language processing (NLP) for analyzing textual data, such as SARs and regulatory filings; image recognition for identifying luxury assets or documents linked to illicit activities.
- **Examples**: Transformer-based models for NLP tasks; convolutional neural networks (CNNs) for visual data analysis.

Graph-Based Models

- **Description**: These models represent data as nodes and edges, enabling the analysis of relationships between entities.

- **Applications**: Mapping networks of transactions to uncover money laundering rings or shell companies; identifying central actors in criminal networks for targeted investigations.
- **Examples**: Graph neural networks (GNNs) for predicting relationships and detecting anomalies within transaction graphs.

Hybrid Models

- **Description**: Combining rule-based systems with machine learning models to leverage the strengths of both approaches.
- **Applications**: Using machine learning to identify patterns while relying on rule-based systems for compliance with regulatory requirements.
- **Examples**: Integrating decision trees with rule-based transaction monitoring systems.

4.2.2. Challenges in AI Model Deployment

Despite their potential, AI models face several challenges when deployed for financial crime detection:

Data Quality and Availability

- Inconsistent, incomplete, or biased data can reduce the accuracy and reliability of AI models.
- Sensitive financial data is often siloed due to privacy regulations, limiting access for training and validation.

Model Interpretability

- Complex models, such as deep learning networks, often function as “black boxes,” making their outputs difficult to explain.
- Lack of interpretability can hinder regulatory approval and stakeholder trust.

Scalability

- Adapting models to handle the growing volume and complexity of global financial transactions is a technical challenge.
- Real-time detection requires high computational power and robust infrastructure.

Ethical and Legal Concerns

- AI models may inadvertently introduce biases, leading to unfair or discriminatory outcomes.
- Data privacy regulations, such as GDPR, impose restrictions on data usage and sharing, complicating model development.

4.2.3. Opportunities for Enhancing AI Models

To address these challenges and maximize the potential of AI models, the following strategies are recommended:

Federated Learning

Enables collaborative model training across institutions without sharing sensitive data, enhancing both privacy and performance.

Explainable AI (XAI)

Developing interpretable models or incorporating explainability tools to ensure that outputs are understandable and justifiable to stakeholders.

Data Enrichment and Standardization

Standardizing data collection and reporting practices to improve data quality and availability for AI training and leveraging external datasets, such as open financial crime databases, to enrich training data.

Continuous Learning

Implementing systems that update AI models dynamically as new data becomes available, ensuring adaptability to emerging crime patterns.

Public-Private Collaboration

Encouraging partnerships between regulators, financial institutions, and AI developers to share expertise, resources, and best practices.

4.2.4. Case Studies and Applications

Transaction Monitoring

Financial institutions use AI models to flag unusual transaction patterns in real time, reducing false positives and improving efficiency.

Asset Tracing

AI systems analyze financial flows and ownership records to identify and locate assets tied to criminal activities.

Suspicious Activity Report (SAR) Analysis

NLP models process large volumes of SARs to extract insights and identify trends in money laundering techniques.

4.2.5. Future Directions

Research and innovation in AI models for financial crime detection are expected to focus on:

- Developing domain-specific models tailored to AML and asset recovery contexts.
- Enhancing model robustness against adversarial attacks and biases.
- Integrating AI with blockchain and other emerging technologies for secure, transparent transaction monitoring.

By advancing AI models and addressing deployment challenges, stakeholders can enhance their ability to detect and combat financial crimes, safeguarding the integrity of financial systems and promoting global security.

4.3 Insights on AI-Assisted Security Challenges

The adoption of AI in AML, asset recovery, and crime prevention offers transformative potential but also introduces significant security challenges. These challenges stem from both the vulnerabilities of AI systems and the ways malicious actors exploit AI technologies. This section explores key insights into AI-assisted security challenges and offers strategies for addressing them.

4.3.1. Key AI-Assisted Security Challenges

Adversarial Attacks on AI Systems

- **Description**: Adversarial attacks involve malicious inputs designed to deceive AI models, leading to incorrect outputs.
- **Examples**: In AML systems, attackers may alter transaction data to avoid detection.In asset recovery, adversarial attacks can distort image recognition systems used to identify valuable assets.
- **Impact**: These attacks compromise the reliability and effectiveness of AI systems, undermining trust in their deployment.

Exploitation of AI for Criminal Activities

- **Description**: Criminals leverage AI technologies to enhance the efficiency and scale of illicit operations.
- **Examples**: Deepfake Technology generating synthetic identities or deceptive media to facilitate fraud and laundering. AI-Driven Cyberattacks using AI to automate phishing campaigns, identify system vulnerabilities, or execute denial-of-service attacks.
- **Impact**: The use of AI by malicious actors intensifies the sophistication and reach of financial crimes, making them harder to detect and mitigate.

Cybersecurity Vulnerabilities in AI Systems

- **Description**: AI systems, like other digital technologies, are susceptible to hacking, data breaches, and malware attacks.
- **Examples**: AI training datasets can be poisoned to introduce biases or vulnerabilities. Model inference attacks can extract sensitive information from deployed AI systems.
- **Impact**: Breaches of AI systems can expose sensitive financial data, disrupt operations, and erode stakeholder trust.

Weaponization of AI

- **Description**: Rogue states, terrorist groups, or organized crime networks exploit AI to advance their objectives.
- **Examples**: AI tools for coordinating transnational crimes, such as trafficking or money laundering. Disruption of financial systems through AI-enabled cyberwarfare.
- **Impact**: The weaponization of AI poses significant threats to global financial stability and security.

4.3.2. Strategies to Address AI-Assisted Security Challenges

Strengthening AI Security

- **Robust Development Practices**: Employ secure coding practices and conduct regular vulnerability assessments; use adversarial testing to identify weaknesses and improve system resilience.
- **Data Integrity and Privacy**: Protect training data with encryption and access controls.; implement privacy-preserving techniques such as differential privacy and federated learning.

Enhancing Threat Detection

- **AI-Driven Cybersecurity Tools**: Deploy AI systems for real-time monitoring and detection of cyber threats (Kalodanis, Rizomiliotis, and Anagnostopoulos, 2024). Use anomaly detection models to identify unusual patterns in network traffic or transactions.
- **Collaboration with Stakeholders**: Establish partnerships with financial institutions and law enforcement to share intelligence on emerging threats.

Regulatory and Policy Measures

- **Mandatory Security Standards**: Enforce requirements for secure AI system development and deployment, including regular audits and compliance checks.
- **Reporting Obligations**: Introduce policies for mandatory reporting of AI-related breaches and security incidents.
- **Global Collaboration**: Harmonize international regulations and best practices to address the transnational nature of AI-related threats.

Education and Awareness

- **Training for Professionals**: Provide training to developers, policymakers, and financial professionals on AI security risks and mitigation strategies.
- **Public Awareness Campaigns**: Educate stakeholders and the public about the risks associated with AI-assisted financial crimes.

4.3.3. Emerging Opportunities

While AI presents challenges, it also offers opportunities for enhancing security:

1. **AI-Augmented Defense Mechanisms**: Use AI to predict and prevent attacks by analyzing threat patterns and vulnerabilities proactively (Kaur and Saini, 2024).
2. **Collaboration Platforms**: Develop platforms for sharing threat intelligence and best practices across industries and jurisdictions.
3. **Innovation in AI Governance**: Establish ethics-driven frameworks to guide the development and use of AI technologies in sensitive applications.

4.3.4. Future Directions

Addressing AI-assisted security challenges requires continuous innovation and adaptation. Key areas for future research and action include:

- Developing resilient AI systems capable of withstanding adversarial attacks.
- Promoting the integration of AI with blockchain and other emerging technologies for secure, transparent financial operations.
- Strengthening international cooperation to tackle global security risks associated with AI exploitation.

By understanding and addressing these challenges, stakeholders can ensure that AI technologies are deployed responsibly and effectively, minimizing risks while maximizing their potential to combat financial crimes and enhance security.

5. Collaboration and Stakeholder Engagement in Research Activities

5.1 Role of Advisory and Steering Committees

The Advisory and Steering Committees play a pivotal role in ensuring the strategic direction, quality, and relevance of the AI-2-TRACE-CRIME project's research outputs. These committees are composed of interdisciplinary experts, including academics, legal practitioners, policymakers, and industry representatives, who bring diverse perspectives and expertise to the project.

The Advisory Committee provides high-level guidance and oversight to ensure that the project's objectives align with broader academic, professional, and societal goals. Its members contribute to shaping the research agenda, identifying emerging trends, and addressing potential gaps in the project's focus areas. By offering critical feedback on methodologies, deliverables, and overall progress, the Advisory Committee ensures that the project's outputs meet rigorous academic and professional standards.

The Steering Committee, on the other hand, is responsible for the operational and strategic management of the project. It oversees the implementation of research activities, coordinates with work package leaders, and ensures that milestones are achieved in a timely manner. The committee also facilitates communication and collaboration among project partners, fostering a cohesive approach to addressing the project's thematic streams.

Together, these committees act as key enablers of the project's success, providing both strategic vision and practical guidance. Their involvement enhances the credibility and impact of the project by ensuring that its outputs are informed by expertise, grounded in real-world relevance, and aligned with stakeholder needs.

5.2 Integration of Stakeholder Feedback

The integration of stakeholder feedback is central to the AI-2-TRACE-CRIME project's commitment to producing research that is both impactful and practical. Stakeholders, including financial institutions, regulatory bodies, law enforcement agencies, and civil society organizations, provide invaluable insights that inform the project's research and ensure its relevance to real-world challenges.

Feedback is systematically collected through various channels, including structured consultations, surveys, and stakeholder workshops. These interactions allow the project team to understand the practical challenges faced by stakeholders, such as the limitations of existing regulatory frameworks or the technical difficulties in implementing AI tools for AML and asset recovery.

Stakeholder input is integrated into the project's research at multiple stages. During the design phase, feedback helps refine research questions and methodologies to ensure they address pressing needs. During the analysis phase, stakeholders provide contextual insights that enhance the interpretation and applicability of findings. Finally, during the dissemination phase, stakeholder involvement ensures that outputs are presented in accessible formats and tailored to the specific needs of different audiences.

This collaborative approach not only enhances the relevance and utility of the project's outputs but also builds trust and engagement with the broader community. By prioritizing stakeholder feedback, the AI-2-TRACE-CRIME project ensures that its research contributes meaningfully to the development of effective policies, technologies, and practices for combating financial crime.

5.3 Partnerships with Industry and Academia

The AI-2-TRACE-CRIME project places significant emphasis on fostering partnerships with both industry and academia to enhance the depth, relevance, and practical application of its research. These collaborations ensure a robust exchange of knowledge, expertise, and resources, enabling the project to address the challenges of AI applications in AML, asset recovery, and crime prevention.

Partnerships with industry are particularly valuable in bridging the gap between theoretical research and real-world practice. Financial institutions, technology developers, and compliance professionals provide critical insights into the practical challenges and opportunities associated with deploying AI tools in AML and crime prevention. By engaging with these stakeholders, the project gains access to empirical data, operational expertise, and emerging technologies that enrich its research. These partnerships also create opportunities for piloting AI solutions in real-world settings, allowing for iterative testing and refinement.

Collaborations with academia ensure that the project is grounded in cutting-edge research and aligned with broader scholarly discourses. The involvement of leading academic institutions and researchers brings a wealth of theoretical and methodological expertise to the project. Academic partnerships also facilitate interdisciplinary approaches, integrating perspectives from law, computer science, and social sciences to address the complexities of AI governance and application in financial crime prevention.

Moreover, the project actively encourages collaborative initiatives, such as joint research papers, co-hosted events, and shared training programs, which further strengthen the synergy between academic and industry partners. These initiatives not only enhance the quality and visibility of the project's outputs but also contribute to building a community of practice that is committed to responsible and effective use of AI technologies.

Through strategic partnerships with industry and academia, the AI-2-TRACE-CRIME project ensures that its research is both theoretically rigorous and practically impactful. These collaborations play a crucial role in advancing the project's objectives, fostering innovation, and promoting the adoption of effective policies and technologies in combating financial crime.

6. Research Quality and Compliance

6.1 Ethical Considerations in AI Research

Ethical considerations are foundational to the responsible development and deployment of AI in AML, asset recovery, and crime prevention. The AI-2-TRACE-CRIME project acknowledges the profound societal implications of AI technologies and incorporates a robust ethical framework into its research activities to ensure alignment with human rights, fairness, and transparency.

Central to the ethical approach is the principle of human-centric AI, which emphasizes that AI systems must be designed and used to enhance human well-being without undermining fundamental rights. The project carefully considers the risks of bias, discrimination, and loss of privacy, which are particularly significant in AML contexts due to the sensitive nature of the data and the potential for adverse impacts on individuals and communities. To address these risks, the project integrates fairness and accountability mechanisms into its AI models, including thorough bias audits and the implementation of privacy-preserving technologies.

Transparency is another critical ethical consideration. AI systems often operate as "black boxes," making their decision-making processes difficult to understand or scrutinize. This lack of transparency can erode trust and accountability, particularly in high-stakes applications such as financial crime detection. To counteract this, the project prioritizes explainable AI, ensuring that the outputs of its systems can be interpreted and justified to regulators, stakeholders, and affected parties.

Collaboration with a diverse group of stakeholders, including regulators, civil society, and technical experts, further strengthens the ethical foundation of the project. These collaborations help ensure that the project's research is informed by a wide range of perspectives and responsive to the needs and concerns of different communities. Additionally, adherence to ethical guidelines and frameworks, such as those outlined by the European Commission and international AI ethics bodies, provides a standardized basis for evaluating and guiding the project's research.

By embedding ethical considerations into all stages of its activities, the AI-2-TRACE-CRIME project not only mitigates risks but also enhances the legitimacy and societal acceptance of its findings. This ethical commitment underscores the importance of balancing technological advancement with respect for human dignity and societal values.

6.2 Quality Assurance Procedures

Ensuring the quality and integrity of research outputs is a priority for the AI-2-TRACE-CRIME project. Rigorous quality assurance procedures are implemented throughout the research process to maintain high academic and professional standards, reinforce stakeholder trust, and maximize the impact of the project's findings.

The project adopts a systematic approach to quality assurance, beginning with the development of clearly defined objectives and methodologies for each work package. These objectives are aligned with the project's broader goals, ensuring coherence and consistency across all activities. Methodological rigor is further reinforced through detailed protocols for data collection, analysis, and interpretation, which are documented and subject to internal and external review.

Peer review plays a central role in the quality assurance process. Draft outputs, including research reports, policy briefs, and the Research Handbook, are reviewed by members of the project's Advisory Board as well as external experts in the fields of law, technology, and financial crime prevention. This multidisciplinary review ensures that the findings are accurate, relevant, and applicable to diverse contexts. Feedback from these reviews is systematically incorporated into the final outputs, reflecting the project's commitment to continuous improvement.

Regular monitoring and evaluation of progress against defined milestones also contribute to quality assurance. The PI, assisted by the Steering Committee, oversees this process, identifying potential issues early and implementing corrective actions where necessary. This proactive approach helps maintain the integrity and reliability of the research process.

Transparency and accountability are integral to the quality assurance framework. All research activities and outputs are documented in detail, enabling traceability and reproducibility. Ethical compliance and adherence to legal and regulatory standards, such as data protection laws, further enhance the credibility of the project's findings. By embedding these robust quality assurance procedures into its operations, the AI-2-TRACE-CRIME project ensures that its research outputs are not only scientifically rigorous but also trustworthy and impactful.

6.3 Risk Management in Research Activities

The AI-2-TRACE-CRIME project recognizes that research activities, particularly those involving emerging technologies such as AI, entail various risks that must be proactively managed. A comprehensive risk management framework is integral to the project's governance structure, ensuring that potential challenges are identified, assessed, and mitigated effectively.

One key area of risk management pertains to ethical and legal compliance. The sensitive nature of AML and asset recovery research necessitates strict adherence to data protection laws, such as the GDPR, and ethical guidelines for handling sensitive financial and personal data. The project employs robust data governance protocols, including secure data storage, encryption, and access controls, to mitigate risks associated with data breaches or misuse.

Technical risks are also a significant focus, given the experimental nature of AI research. Issues such as bias in AI models, adversarial attacks, and inaccuracies in predictive systems can undermine the reliability and fairness of research outputs. To address these risks, the project incorporates regular testing and validation of AI systems, employing adversarial testing and fairness audits to identify and rectify vulnerabilities. Collaboration with technical experts and stakeholders ensures that these measures remain effective and up-to-date.

Operational risks, such as delays in deliverables or misalignment between partners, are managed through clear project governance structures and regular coordination meetings. The PI and the Steering Committee monitor progress against timelines and milestones, addressing any deviations promptly to minimize their impact. Contingency plans are also in place to address unexpected challenges, such as changes in regulatory environments or technological limitations.

Stakeholder engagement is an additional layer of risk management. By involving diverse stakeholders in the research process, the project ensures that its outputs are relevant, practical, and responsive to real-world needs. This engagement helps preempt potential criticisms or gaps in the research, further strengthening its impact.

Ultimately, the risk management framework adopted by the AI-2-TRACE-CRIME project not only safeguards the integrity and credibility of its research but also enhances its ability to deliver meaningful and actionable findings. This proactive and systematic approach ensures that risks are effectively mitigated, enabling the project to achieve its objectives while maintaining high standards of accountability and resilience.

7. Dissemination and Impact

7.1 Strategy for Open Access Publication

The dissemination of research findings and outputs is a core objective of the AI-2-TRACE-CRIME project. To maximize the impact and accessibility of the project’s work, the Research Handbook prioritizes a comprehensive open access (OA) publication strategy. This approach aligns with the principles of transparency, inclusivity, and knowledge sharing, ensuring that the Handbook reaches a diverse and global audience.

The OA strategy for the Research Handbook is designed to facilitate unrestricted access to the project's insights and recommendations, promoting their use by academics, policymakers, practitioners, and the general public. By removing barriers to access, the Handbook can support ongoing research, inform policymaking, and contribute to the development of best practices in the fields of AI, AML, and crime prevention. The OA model not only broadens the reach of the Handbook but also enhances its credibility and relevance by fostering engagement with a wider range of stakeholders.

To achieve this, the Handbook will be published as an e-book, hosted on the official website of the Jean Monnet Center of Excellence at Neapolis University Pafos. It will also be made available on prominent academic and professional platforms such as ResearchGate, SSRN, and Academia.edu. These platforms are widely recognized for their ability to disseminate research outputs to targeted academic and professional audiences. Additionally, the Handbook will be shared through institutional repositories, ensuring its long-term preservation and accessibility.

The Handbook’s open access model adheres to the FAIR principles (Findable, Accessible, Interoperable, and Reusable), which emphasize the importance of making research outputs easily discoverable and usable by both humans and machines. Metadata for the Handbook will be optimized to ensure high visibility in academic search engines and indexing services, further increasing its accessibility to global audiences.

To maintain the highest standards of quality, the Handbook will undergo rigorous peer review by members of the project’s Advisory Board and external experts. This process ensures that the content is accurate, relevant, and aligned with the project’s objectives. All feedback will be incorporated into the final version, ensuring that the Handbook serves as a reliable resource for its intended audience.

The dissemination strategy also incorporates targeted outreach to stakeholders, including tailored communication to key groups such as financial institutions, regulatory bodies, legal professionals, and AI practitioners. Through webinars, workshops, and conferences, the Handbook will be presented as a central resource for discussions and collaborations on AI applications in AML and crime prevention. This dissemination effort ensures that the Handbook not only reaches its intended audience but also becomes a catalyst for further dialogue and innovation in the field.

The open access publication strategy for the Research Handbook reflects the project’s commitment to transparency, inclusivity, and the democratization of knowledge. By making its findings freely available, the Handbook serves as both a resource and a foundation for advancing global efforts to address the challenges and opportunities presented by AI in combating financial crime.

7.2 Tools for Research Dissemination (e.g., website, ResearchGate)

The dissemination of research findings is a critical component of the AI-2-TRACE-CRIME project, aimed at maximizing the visibility and impact of its outputs. A variety of tools have been selected to ensure that the project's research reaches diverse audiences, from academics and practitioners to policymakers and the general public. These tools have been strategically chosen to facilitate engagement, foster collaboration, and promote the uptake of research findings.

A central element of the dissemination strategy is the project's dedicated website, which serves as the primary platform for sharing resources, updates, and outputs. The website will host the Research Handbook as an open access publication, alongside supplementary materials such as policy briefs, working papers, and recorded webinars. Designed with user accessibility in mind, the website will include a repository of resources categorized by thematic streams, allowing visitors to easily navigate and locate materials relevant to their interests. Regular updates and an integrated blog will further ensure that the website remains a dynamic and engaging hub for project activities.

To extend the reach of the project's outputs, the Research Handbook and other deliverables will also be disseminated through widely recognized academic platforms such as ResearchGate, SSRN, and Academia.edu. These platforms enable direct engagement with the academic community, facilitating the sharing of research with scholars and professionals working in related fields. By utilizing these networks, the project ensures that its findings are integrated into ongoing global discussions on AI, AML, and crime prevention.

Social media plays a vital role in broadening the audience for the project's outputs. Dedicated social media posts on specialized platforms such as LinkedIn will be used to share updates, highlight key findings, and promote events. These platforms enable targeted outreach to specific professional and academic communities, creating opportunities for dialogue and feedback. Posts will be crafted to align with the communication styles of each platform, ensuring maximum engagement with users.

In addition to digital tools, the project will leverage traditional media channels, such as press releases and media partnerships, to announce major milestones and disseminate findings to a broader audience. Press releases will highlight significant developments, such as the publication of the Research Handbook, and will be shared with relevant outlets to ensure wide coverage. Partnerships with media organizations will further amplify the project's visibility and establish its outputs as credible and influential resources.

Dissemination efforts will also extend to in-person and virtual events, including conferences, workshops, and webinars. These events provide platforms for presenting the project's findings, engaging with stakeholders, and fostering collaboration. Participants will be encouraged to access and share the Research Handbook and related materials, ensuring that the project's outputs contribute to broader knowledge-sharing initiatives. Follow-up activities, such as feedback surveys and report sharing, will maintain engagement with participants and encourage the continued use of the project's findings.

Overall, the combination of digital platforms, social media, traditional media, and events ensures a robust dissemination strategy for the AI-2-TRACE-CRIME project. By employing these tools in a coordinated manner, the project aims to enhance the visibility and accessibility of its research, fostering meaningful impact across academic, professional, and public domains. The dissemination tools not only share knowledge but also create pathways for collaboration, dialogue, and innovation in the field of AI-driven crime prevention.

7.3 Enhancing Policy and Practice through Research

The AI-2-TRACE-CRIME project is committed to bridging the gap between academic research and its practical application in shaping policies and practices for combating financial crime. By aligning its research outputs with the needs of policymakers, practitioners, and other stakeholders, the project ensures that its findings have a tangible impact on real-world challenges.

Central to this effort is the integration of actionable insights derived from the project's interdisciplinary research. The Research Handbook synthesizes legal, technical, and operational analyses to offer concrete recommendations for improving the effectiveness of AML measures and asset recovery practices. These recommendations are designed to address gaps in existing frameworks, propose innovative solutions, and support the development of coherent, adaptable, and enforceable policies.

The project emphasizes the importance of evidence-based policymaking, where research findings directly inform the design and implementation of legislative and regulatory measures. For instance, insights into the limitations of current AI governance frameworks or the identification of biases in AI systems are translated into proposals for more robust oversight mechanisms and clearer compliance guidelines. This approach not only enhances the effectiveness of AML strategies but also builds trust among stakeholders by demonstrating the accountability and fairness of the systems in place.

In addition to influencing policy, the project actively seeks to enhance professional practice. Through collaboration with financial institutions, law enforcement agencies, and regulatory bodies, the project's outputs are tailored to address operational challenges faced by these entities. Practical tools, such as case studies, training modules, and best practice guidelines, are developed to equip professionals with the knowledge and skills needed to effectively utilize AI in their efforts to combat financial crime. This focus on capacity building ensures that research findings are not confined to theoretical discussions but are instead actively applied to improve workflows, decision-making, and overall outcomes.

Stakeholder engagement is a key element of this endeavor. By involving policymakers, industry experts, and civil society representatives in the research process, the project ensures that its outputs are both relevant and practical. Consultative workshops provide opportunities for stakeholders to share their perspectives, validate findings, and co-develop solutions. This inclusive approach not only strengthens the applicability of the research but also fosters a sense of ownership among stakeholders, increasing the likelihood of successful implementation.

The dissemination strategy further supports the translation of research into policy and practice. By leveraging open access publication models, academic platforms, and professional networks, the project ensures that its findings reach a broad audience. Targeted outreach efforts, such as policy briefs and tailored presentations, are used to engage decision-makers and practitioners directly, facilitating the uptake of the project's recommendations.

In summary, the AI-2-TRACE-CRIME project aims to deliver actionable insights, foster stakeholder collaboration, and prioritize capacity building. The project bridges the gap between theory and application, ensuring that its research contributes meaningfully to the development of more effective and equitable solutions in AML and asset recovery.

8. Sustainable Research

8.1 Ensuring Continued Impact of Research Findings

The long-term impact of the AI-2-TRACE-CRIME project's research findings is a central priority, requiring deliberate strategies to ensure that its contributions to AML, asset recovery, and crime prevention remain relevant and actionable. This commitment involves both the sustained dissemination of the project's outputs and their integration into ongoing policy, practice, and academic discourse.

A critical element in ensuring continued impact is the accessibility and durability of the Research Handbook and other key deliverables. By adopting open access publication models and hosting outputs on institutional and academic platforms, the project guarantees that its findings remain publicly available and easy to reference for years to come. Efforts to index the Handbook in major academic databases and repositories further ensure its visibility and discoverability among researchers and practitioners.

In addition to ensuring accessibility, the project focuses on embedding its findings within existing systems and frameworks. Policy recommendations and best practices generated by the research are shared online and could be used by relevant national and international bodies, such as the Financial Action Task Force (FATF) and the European Commission. Our ambition is that the project's insights inform ongoing policy discussions and legislative updates, contributing to the evolution of AML and AI governance frameworks.

To maintain the relevance of its research in a rapidly evolving field, the project emphasizes capacity building and professional development. Training programs, webinars, and workshops are designed to equip practitioners, regulators, and stakeholders with the tools and knowledge to apply the project's findings in their respective domains. These initiatives not only amplify the project's immediate impact but also create pathways for its insights to be adapted and expanded over time.

Stakeholder networks established during the project's lifecycle play a crucial role in sustaining its impact. By fostering relationships with academic institutions, industry leaders, and regulatory bodies, the project ensures that its findings continue to inform collaborative efforts and interdisciplinary research. Regular updates, follow-up studies, and ongoing stakeholder engagement maintain the momentum generated by the project and encourage the integration of its findings into new initiatives.

Ultimately, ensuring the continued impact of the project's research requires a multi-faceted approach that combines accessibility, integration, capacity building, and stakeholder collaboration. By implementing these strategies, the AI-2-TRACE-CRIME project positions its findings as enduring contributions to the fight against financial crime and the responsible use of AI technologies.

8.2 Opportunities for Future Funding and Collaboration

The AI-2-TRACE-CRIME project's research activities and findings provide a solid foundation for future funding opportunities and collaborative endeavors. Building on its interdisciplinary approach and established networks, the project is well-positioned to expand its work and explore new frontiers in the governance and application of AI in AML and asset recovery.

One significant opportunity for future funding lies in the extension of the project's thematic focus to emerging challenges in AI and financial crime prevention. For example, the increasing use of decentralized finance (DeFi) platforms and cryptocurrencies presents new risks and regulatory complexities that warrant in-depth research. Grant programs from organizations such as the European Research Council (ERC), Horizon Europe, or private foundations focused on AI ethics and governance provide potential avenues for securing support to address these evolving issues.

Collaboration with international partners offers another promising opportunity. Expanding the project's reach to include non-EU jurisdictions, such as the United States, the United Kingdom, and regions in Asia, would enable comparative studies that enhance the global relevance of its findings.

Industry partnerships also represent a key avenue for future collaboration. By working closely with financial institutions, technology providers, and regulatory bodies, the project can pilot and refine AI tools and frameworks developed during its lifecycle. These partnerships can also provide access to proprietary data and operational expertise, enabling more targeted and practical research. Joint funding applications with industry partners to innovation-focused programs, such as the EU's Digital Europe Programme, can further support such initiatives.

Additionally, the project's academic networks present opportunities for joint research applications and multi-institutional studies. Engaging with universities and research centers specializing in AI, cybersecurity, and financial crime can foster interdisciplinary projects that push the boundaries of existing knowledge. Collaborative workshops and conferences can also serve as catalysts for identifying shared research priorities and developing joint proposals.

Finally, the project's established stakeholder relationships provide a springboard for exploring public-private partnerships and co-creation initiatives. These collaborations can bridge the gap between research and implementation, ensuring that future projects are informed by real-world needs and challenges. This approach not only enhances the practical relevance of future work but also strengthens the case for sustained funding by demonstrating tangible outcomes.

In summary, the AI-2-TRACE-CRIME project's comprehensive research and extensive networks create significant opportunities for future funding and collaboration. By leveraging these strengths, the project can continue to innovate and contribute to the development of effective, ethical, and globally relevant solutions for combating financial crime in the era of AI.

Further Reading and References

Barabas, Chelsea. "Beyond bias: re-imagining the terms of" ethical ai" in criminal law." Geo. JL & Mod. Critical Race Persp. 12 (2020): 83.

Blauth, Tais Fernanda, Oskar Josef Gstrein, and Andrej Zwitter. "Artificial intelligence crime: An overview of malicious use and abuse of AI." Ieee Access 10 (2022): 77110-77122.

Blount, Kelly. "Using artificial intelligence to prevent crime: implications for due process and criminal justice." AI & SOCIETY 39.1 (2024): 359-368.

Bomhard, David, and Marieke Merkle. "Regulation of Artificial Intelligence: The EU Commission's Proposal of an AI Act." J. Eur. Consumer & Mkt. L. 10 (2021): 257.

Buocz, Thomas, Sebastian Pfotenhauer, and Iris Eisenberger. "Regulatory sandboxes in the AI Act: reconciling innovation and safety?." Law, Innovation and Technology 15.2 (2023): 357-389.

Busuioc, Madalina, Deirdre Curtin, and Marco Almada. "Reclaiming transparency: contesting the logics of secrecy within the AI Act." European Law Open 2.1 (2023): 79-105.

Caldwell, Matthew, et al. "AI-enabled future crime." Crime Science 9.1 (2020): 1-13.

Cancela-Outeda, Celso. "The EU's AI act: A framework for collaborative governance." Internet of Things 27 (2024): 101291.

Cantero Gamito, Marta, and Christopher T. Marsden. "Artificial intelligence co-regulation? The role of standards in the EU AI Act." International journal of law and information technology 32 (2024): eaae011.

Chiappetta, Allessia. "Navigating the AI frontier: European parliamentary insights on bias and regulation, preceding the AI Act." Internet Policy Review 12.4 (2023): 1-26.

Ebers, Martin. "Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act." European Journal of Risk Regulation 16.2 (2025): 684-703.

Hacker, Philipp. "A legal framework for AI training data—from first principles to the Artificial Intelligence Act." Law, innovation and technology 13.2 (2021): 257-301.

Hallevy, Gabriel. Liability for crimes involving artificial intelligence systems. Vol. 257. New York, NY, USA: Springer International Publishing, 2015.

Hayward, Keith J., and Matthijs M. Maas. "Artificial intelligence and crime: A primer for criminologists." Crime, Media, Culture 17.2 (2021): 209-233.

Helm, Paula, and Thilo Hagendorff. "Beyond the prediction paradigm: Challenges for AI in the struggle against organized crime." Law & Contemp. Probs. 84 (2021): 1.

Joseph, Jeena. "Predicting crime or perpetuating bias? The AI dilemma." AI & SOCIETY 40.4 (2025): 2319-2321.

Kalodanis, Konstantinos, Panagiotis Rizomiliotis, and Dimosthenis Anagnostopoulos. "European artificial intelligence act: an AI security approach." Information & Computer Security 32.3 (2024): 265-281.

Kaur, Manpreet, and Munish Saini. "Role of Artificial Intelligence in the crime prediction and pattern analysis studies published over the last decade: a scientometric analysis." Artificial Intelligence Review 57.8 (2024): 202.

King, Thomas C., et al. "Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions." Science and engineering ethics 26.1 (2020): 89-120.

Kusche, Isabel. "Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk." Journal of Risk Research (2024): 1-14.

Lagioia, Francesca, and Giovanni Sartor. "AI systems under criminal law: a legal analysis and a regulatory perspective." Philosophy & Technology 33.3 (2020): 433-465.

Nerantzi, Elina, and Giovanni Sartor. "'Hard AI Crime': The Deterrence Turn." Oxford journal of legal studies 44.3 (2024): 673-701.

Neuwirth, Rostam J. "Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)." Computer Law & Security Review 48 (2023): 105798.

Novelli, Claudio, et al. "A robust governance for the AI act: AI office, AI Board, scientific panel, and national authorities." European Journal of Risk Regulation 16.2 (2025): 566-590.

Novelli, Claudio, et al. "AI risk assessment: a scenario-based, proportional methodology for the AI act." Digital Society 3.1 (2024): 13.

Novelli, Claudio, et al. "Taking AI risks seriously: a new assessment model for the AI Act." Ai & Society 39.5 (2024): 2493-2497.

Pagallo, Ugo, and Serena Quattrocolo. "The impact of AI on criminal law, and its two fold procedures." Research handbook on the law of artificial intelligence. Edward Elgar Publishing, 2018. 385-409.

Pavlidis, Georgios. "Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era." Journal of Money Laundering Control 26.7 (2023): 155-166.

Pavlidis, Georgios. "Europe in the digital age: regulating digital finance without suffocating innovation." Law, Innovation and Technology 13.2 (2021): 464-477.

Pavlidis, Georgios. "Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI." Law, Innovation and Technology 16.1 (2024): 293-308.

Pehlivan, Ceyhun Necati. "Report: The EU AI Act: An Introduction." Global Privacy Law Review 5.1 (2024).

Perrot, Patrick. "What about AI in criminal intelligence: From predictive policing to AI perspectives." Eur. Police Sci. & Rsch. Bull. 16 (2017): 65.

Quintais, João Pedro. "Generative AI, copyright and the AI Act." Computer Law & Security Review 56 (2025): 106107.

Raja, R. Arshath, N. Yuvaraj, and N. V. Kousik. "Analyses on artificial intelligence framework to detect crime pattern." Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications (2021): 119-132.

Ruschemeier, Hannah. "AI as a challenge for legal regulation–the scope of application of the artificial intelligence act proposal." Era Forum. Vol. 23. No. 3. Berlin/Heidelberg: Springer Berlin Heidelberg, 2023.

Shoeibi, Niloufar, et al. "AI-crime hunter: An AI mixture of experts for crime discovery on twitter." Electronics 10.24 (2021): 3081.

Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." Computer Law Review International 22.4 (2021): 97-112.

Wachter, Sandra. "Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond." Yale JL & Tech. 26 (2023): 671.

Walters, Jacintha, et al. "Complying with the EU AI Act." European Conference on Artificial Intelligence. Cham: Springer Nature Switzerland, 2023.

Yeoh, Peter. "Artificial intelligence: accelerator or panacea for financial crime?." Journal of Financial Crime 26.2 (2019): 634-646.

Annexes

Annex A: Glossary of Terms

Adversarial Attack: A deliberate attempt to manipulate or deceive an AI system by introducing misleading inputs, often with the goal of causing the system to produce incorrect results.

Anti-Money Laundering (AML): Measures, laws, and regulations aimed at detecting and preventing the laundering of illicit funds through legitimate financial systems.

Artificial Intelligence (AI): A branch of computer science concerned with creating systems capable of performing tasks that typically require human intelligence, such as learning, reasoning, and decision-making.

Asset Recovery: The process of tracing, freezing, confiscating, and repatriating assets obtained through illicit means, typically related to corruption, organized crime, or financial fraud.

Bias (in AI): Systematic and unfair discrimination in AI outputs due to imbalances or flaws in training data, algorithms, or deployment contexts.

Compliance: Adherence to legal, regulatory, and ethical standards, particularly in contexts like financial transactions and corporate governance.

Differential Privacy: A technique for ensuring data privacy by introducing controlled noise into datasets, allowing for analysis while protecting individual data points.

Federated Learning: A machine learning technique that enables model training across multiple devices or institutions without sharing raw data, preserving privacy.

Explainable AI (XAI): AI systems designed to provide clear, understandable justifications for their decisions or outputs, enhancing transparency and accountability.

General Data Protection Regulation (GDPR): A comprehensive data protection regulation in the European Union that governs the collection, processing, and storage of personal data.

Risk-Based Approach: A framework for prioritizing actions based on the assessment of potential risks, often used in regulatory compliance and AI governance.

Annex B: Relevant Legislative and Policy Frameworks

1. **European Union AI Act**
   - Establishes a risk-based approach to regulating AI technologies, categorizing them as unacceptable, high-risk, or lower-risk. Key provisions include transparency requirements, human oversight, and specific rules for high-risk applications.
2. **Anti-Money Laundering Directives (AMLDs)**
   - A series of EU legislative acts aimed at strengthening the prevention of money laundering and terrorist financing. Key directives include AMLD4, AMLD5, and AMLD6, addressing issues such as beneficial ownership transparency and cross-border cooperation.
3. **Confiscation Directive**
   - Directive 2014/42/EU provides rules for the freezing and confiscation of proceeds and instrumentalities of crime in the European Union, supporting asset recovery efforts.
4. **General Data Protection Regulation (GDPR)**
   - EU regulation that governs the processing of personal data, emphasizing transparency, accountability, and data minimization.
5. **Financial Action Task Force (FATF) Recommendations**
   - International standards for combating money laundering and terrorist financing, adopted by FATF member states and providing guidance on regulatory frameworks.
6. **United Nations Convention Against Corruption (UNCAC)**
   - A global legal instrument that promotes measures to prevent and combat corruption, including provisions for asset recovery.
7. **NIS Directive (Directive on Security of Network and Information Systems)**
   - EU legislation aimed at improving cybersecurity resilience across member states, relevant for protecting AI systems used in financial crime prevention.
8. **Bank Secrecy Act (BSA) - United States**
   - U.S. legislation mandating financial institutions to maintain records and report suspicious activities, forming a key part of AML efforts.

Annex C: Research Guidelines for Team Members

The following guidelines outline the expectations and best practices for team members conducting research under the AI-2-TRACE-CRIME project, ensuring consistency, rigor, and compliance across all activities.

1. Ethical Conduct

- Adhere to the highest ethical standards in all research activities, ensuring respect for privacy, data protection, and human rights.
- Obtain necessary ethical approvals before initiating research involving human subjects or sensitive data.

2. Data Management

- Use secure systems for data collection, storage, and processing to protect confidentiality and integrity.
- Ensure compliance with data protection regulations, including GDPR, by minimizing data collection, anonymizing data when possible, and obtaining informed consent from relevant parties.

3. Collaboration and Communication

- Foster open and transparent communication among team members, sharing findings and updates regularly.
- Participate in scheduled meetings, workshops, and consultations to ensure alignment with project objectives and timelines.

4. Methodological Rigor

- Follow agreed-upon research methodologies, documenting all processes to ensure transparency and reproducibility.
- Regularly validate and test AI models to identify and mitigate biases, inaccuracies, or vulnerabilities.

5. Quality Assurance

- Submit draft outputs, including research papers and reports, for peer review by designated project members and external experts.
- Incorporate feedback from reviewers to improve the accuracy, relevance, and clarity of final outputs.

6. Risk Management

- Identify potential risks in research activities, including ethical, technical, and operational risks, and report them promptly to the Steering Committee.
- Implement mitigation strategies as outlined in the project's risk management framework.

7. Stakeholder Engagement

- Actively involve stakeholders in research processes where appropriate, ensuring that their input is valued and integrated into findings.
- Maintain professionalism and confidentiality in all stakeholder interactions.

8. Dissemination

- Ensure that research outputs are prepared for dissemination in formats suitable for diverse audiences, including policymakers, practitioners, and academics.
- Follow project guidelines for open access publication and share outputs on designated platforms.

These guidelines are designed to support team members in producing high-quality, impactful research while maintaining ethical integrity and operational efficiency throughout the AI-2-TRACE-CRIME project.