

Mechanisms of Cooperation in the Investigation and Prosecution of AI-Related Crimes: An Analytical Study on Council of Europe Convention No. 108 Concerning Personal Data Protection and Automated Processing

MAZARI Nacereddine^{1,*}, HADI Ameer²

¹ University of Ziane Achour (Algeria), n.mazari@univ-djelfa.dz

¹ University of Ziane Achour (Algeria), ameur.hadi@univ-djelfa.dz

Received: 16 / 06 / 2025

Accepted: 12 / 10 / 2025

Published: 04 / 11 / 2025

Abstract:

This analytical study aimed to explore international cooperation mechanisms in the investigation and prosecution of AI-related crimes, with a focus on analyzing the Council of Europe Convention 108 and its impact on personal data protection in the context of automated processing. The study revealed that the rapid development of AI has created new challenges for international judicial cooperation, requiring the adaptation of existing legal frameworks, the enhancement of technical expertise exchange, and the harmonization of national legislation. It also emphasized the importance of striking a delicate balance between security requirements, crime prevention, and personal data protection, highlighting the pivotal roles of Convention 108 and the Budapest Convention in this context. The study concluded with the necessity of developing complementary international protocols, strengthening the role of supervisory authorities, encouraging public-private cooperation, and investing in specialized training to foster effective international cooperation in combating this emerging type of crime while respecting human rights.

Keywords: *AI-related Crimes; International Judicial Cooperation; Personal Data Protection; Convention 108; Digital Evidence; Cybercrimes*

* MAZARI Nacereddine

I. INTRODUCTION:

The world is undergoing a radical transformation across various aspects of life with the accelerating development of Artificial Intelligence (AI) technologies. AI systems have become an integral part of the global digital infrastructure, utilized in diverse fields including business, healthcare, education, security, and government. With this widespread adoption, new challenges have emerged concerning the potential misuse of these technologies for criminal acts.

"AI-related crimes" are defined as illegal acts that leverage AI technologies as a tool to execute a crime, or those that target AI systems themselves. This category of crimes encompasses a broad spectrum of activities, ranging from traditional cybercrimes enhanced by AI technologies, such as highly targeted phishing attacks or the dissemination of self-propagating malware (Caldwell & al, 2020), to novel crimes involving data manipulation or the development of self-learning AI systems for illicit purposes.

The transnational nature of many of these crimes, which often exploit global digital infrastructure, necessitates the activation of effective international cooperation mechanisms in investigation and prosecution. The ability to identify criminals, track digital evidence, and implement legal procedures requires close coordination and cooperation among different nations.

In this context, the significance of the international legal framework governing judicial cooperation in criminal matters becomes evident. International agreements and treaties play a crucial role in facilitating information exchange, mutual legal assistance, and extradition between states. Among these agreements, the Council of Europe's Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) holds particular importance, given its focus on protecting personal data in the context of automatic processing, an aspect highly relevant to AI-related crimes (Nadiya, Oksana, Viacheslav, & Yurii, 2023).

Convention 108 addresses fundamental principles related to the collection, storage, and processing of personal data and emphasizes the need to ensure individuals' rights to access and rectify their data. Given the increasing reliance on AI systems that heavily depend on analyzing vast amounts of personal data (Big Data), understanding the impact of this Convention on judicial cooperation mechanisms in combating AI-related crimes becomes paramount (Council of Europe, 2018).

The legal and technical challenges facing international cooperation in this domain are numerous and interconnected. On the legal front, national legislations concerning cybercrimes and personal data protection vary, which can impede the exchange of evidence and the implementation of cross-border legal procedures. Furthermore, the complex nature of AI technologies can make it difficult to determine criminal liability in cases involving the use of these systems to commit crimes.

On the technical front, challenges include the difficulty of collecting and analyzing cross-border digital evidence, which may be encrypted or stored in different jurisdictions. Moreover, understanding the operation of AI algorithms and identifying how they are used in criminal activities requires specialized technical expertise that may not be readily available to law enforcement agencies in all countries.

The issue of personal data protection raises additional challenges in the context of international judicial cooperation in combating AI-related crimes. While the exchange of personal information may be necessary to investigate and prosecute these crimes, a balance must be struck between security requirements and the protection of the right to privacy and other fundamental rights of individuals.

These challenges necessitate the development of more effective and adaptable international cooperation mechanisms aligned with the nature of AI-related crimes. This includes enhancing information exchange among law enforcement agencies and judicial authorities in various countries, developing unified standards and procedures for collecting and analyzing digital evidence, and fostering specialized training for judges and investigators in cybercrime and AI technologies.

Additionally, it may be necessary to consider updating and developing existing international legal frameworks, such as Council of Europe Convention No. 108, to ensure their effectiveness

in addressing the challenges posed by AI-related crimes. This could involve clarifying the scope of the Convention's application to data processed by AI systems and defining the necessary safeguards for personal data protection within the context of international judicial cooperation.

This analytical study aims to contribute to a deeper understanding of international cooperation mechanisms in the investigation and prosecution of AI-related crimes, with a specific focus on analyzing Council of Europe Convention No. 108 and its impact on personal data protection in the context of automated processing. By exploring the legal and technical challenges facing this cooperation, the study seeks to provide insights and recommendations that can contribute to strengthening international efforts to effectively combat this growing type of crime in a manner consistent with human rights principles.

1. Problem Statement:

The steady increase in the use of AI technologies across various aspects of life, including criminal activities, presents a new challenge to the international community's efforts in combating crime. The advanced capabilities of AI systems provide criminals with new tools to commit their crimes with unprecedented efficiency and speed, while simultaneously posing significant difficulties for law enforcement agencies in detecting, investigating, and prosecuting these crimes. These difficulties are particularly evident in the context of international judicial cooperation, where legal, technical, and cultural considerations intersect among different nations, complicating the process of exchanging information and evidence and extraditing criminals.

Therefore, the importance of the international legal framework governing personal data protection, foremost among them Council of Europe Convention No. 108, becomes prominent. While international judicial cooperation may sometimes require the exchange of personal data related to suspects or victims, this exchange must occur within a framework of safeguards that ensure the protection of such data and respect for the right to privacy. Consequently, the question arises as to the effectiveness of current international judicial cooperation mechanisms in addressing AI-related crimes given the limitations imposed by Convention 108 on personal data protection, and how to strike a balance between the requirements of security and crime fighting and the protection of individuals' fundamental rights in this evolving context.

How can international cooperation mechanisms for investigating and prosecuting AI-related crimes be effectively activated in a manner consistent with the principles of personal data protection stipulated in Council of Europe Convention No. 108?

2. Study Questions:

- What are the most prominent legal and technical challenges facing international cooperation in investigating and prosecuting AI-related crimes?
- How does the international legal framework for personal data protection, especially Council of Europe Convention No. 108, affect the mechanisms for exchanging information and evidence in the context of investigating AI-related crimes?
- What are the current mechanisms for international judicial cooperation and their suitability for dealing with the transnational nature of AI-related crimes?
- What are the best international practices and experiences in judicial cooperation to combat cybercrimes that can be leveraged to develop cooperation mechanisms to address AI-related crimes?
- What amendments or proposals can be made to existing international legal frameworks, including Council of Europe Convention No. 108, to enhance effective cooperation in investigating and prosecuting AI-related crimes while ensuring the protection of personal data and fundamental rights?

3. Significance of the Study:

This study holds significant importance in light of the notable increase in crimes that utilize AI technologies or target AI systems themselves. Understanding existing international cooperation mechanisms and identifying the challenges that hinder their effectiveness in this field is a fundamental step towards developing more effective international strategies and policies to combat this emerging type of crime. By analyzing Council of Europe Convention No. 108 and its impact on personal data protection in this context, the study can contribute to highlighting the need to strike a delicate balance between the requirements of security and crime fighting and the protection of individuals' fundamental rights in the digital space.

The results of this study are expected to enrich the ongoing debate about developing international legal frameworks to address the challenges posed by AI technologies to criminal justice. By providing practical recommendations based on in-depth analysis, the study can assist policymakers, international organizations, and law enforcement agencies in adopting more effective policies and procedures to enhance international judicial cooperation in combating AI-related crimes, while ensuring respect for international standards of personal data protection and human rights.

II. Study Methodology:

This study adopts a Comparative Analytical Methodology to achieve its objectives and answer its questions. This methodology involves two main stages:

1. First: Legal Analysis

In this stage, an in-depth analysis of legal texts relevant to the study's topic is conducted. The analysis specifically focuses on:

- Council of Europe Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108): A detailed analysis of the Convention's provisions is performed to understand the fundamental principles governing personal data protection in the context of automated processing and to determine the extent of these principles' impact on information exchange within international judicial cooperation.

- Other Relevant International Legal Instruments: Other international agreements and treaties related to judicial cooperation in criminal matters and combating cybercrime are reviewed and analyzed, such as the Budapest Convention on Cybercrime, and bilateral and multilateral agreements concerning mutual legal assistance and extradition. The focus is on provisions governing cross-border information and evidence exchange and their potential impact on AI-related crimes.

- Comparative National Legislations: Examples of legislations from different countries concerning cybercrimes, personal data protection, and international judicial cooperation are selected and studied. The focus is on how these legislations deal with crimes involving the use of AI technologies and how they regulate data and information exchange within international cooperation.

2. Second: Comparative Analysis

In this stage, a comparison is made between the legal texts analyzed in the first stage. The comparison focuses on:

- Comparison of Personal Data Protection Principles: A comparison of the principles and standards stipulated in Convention 108 with those contained in other international legal instruments and national legislations is conducted to identify similarities and differences and their impact on judicial cooperation in the context of AI-related crimes.

- Comparison of Judicial Cooperation Mechanisms: A comparison of the mechanisms and procedures stipulated in international agreements and national legislations is performed to determine their effectiveness in dealing with the special nature of AI-related crimes, including the technical and legal challenges related to collecting digital evidence and determining responsibility.

- Identification of Strengths and Weaknesses: Through the comparison, the strengths and weaknesses in current legal frameworks are identified with regard to facilitating international cooperation in the investigation and prosecution of AI-related crimes while ensuring personal data protection.

3. Study Sample:

The study sample includes the following legal texts and materials:

3.1. Primary Legal Text:

- Council of Europe Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data.

- Its Additional Protocol regarding supervisory authorities and transfers of data across borders.

3.2. Relevant International Legal Instruments:

- Budapest Convention on Cybercrime.

- United Nations Convention against Transnational Organized Crime.
- Bilateral and Multilateral Mutual Legal Assistance Treaties and Extradition Treaties (selected examples thereof).

3.3. Comparative Legislations:

- Laws and legislative texts from countries with different experiences in combating cybercrimes, personal data protection, and international judicial cooperation will be selected (to be determined based on their importance and impact in this field).

3.4. Secondary Legal Materials:

- Academic studies and research published in specialized journals and conferences on AI-related crimes, international judicial cooperation, and personal data protection.
- Reports from international and regional organizations (Council of Europe, United Nations, Interpol) related to these topics.
- Legal opinions and interpretations issued by judicial bodies and legal experts regarding the application of relevant legal texts.

By analyzing and comparing these legal texts and materials, the study seeks to provide a comprehensive understanding of international cooperation mechanisms in the investigation and prosecution of AI-related crimes in light of the personal data protection principles stipulated in Council of Europe Convention No. 108.

III. Conceptual Framework of the Study:

The conceptual framework of the study represents the fundamental pillar upon which its analysis and understanding of key concepts, terminology, and the relationships between them are based. This framework aims to clarify the basic concepts related to AI-related crimes, international judicial cooperation, and personal data protection, and to define the scope and theoretical boundaries of the study.

1. Basic Concepts of Artificial Intelligence and Crime:

- Artificial Intelligence (AI): AI is generally defined as the ability of machines and computer programs to simulate human mental capabilities, such as learning, reasoning, problem-solving, and decision-making. AI encompasses a wide range of technologies and algorithms (Christopher & al, 2021), including Machine Learning, Neural Networks, Natural Language Processing, and Computer Vision.

- AI-related Crimes: This concept is central to the study and includes two main categories of criminal acts:

- Crimes using AI technologies as a tool: In this type, AI systems are used to facilitate or execute traditional or cybercrimes. This can include using AI to develop sophisticated phishing attacks (Ratnawita, 2022), create misleading content (Deepfakes) for fraud or defamation, or utilize robots and smart systems to commit physical crimes.

- Crimes targeting AI systems themselves: In this type, the criminal act's objective is to manipulate, disrupt, or steal data or algorithms from AI systems. This can include poisoning attacks on machine learning models, theft of intellectual property related to AI systems, or disrupting AI-dependent infrastructure (Malatji & Alaa, 2024).

- Cybercrimes: Cybercrimes are defined as illegal acts committed using computers and the internet. Cybercrimes significantly overlap with AI-related crimes, as AI technologies can be used to enhance the capabilities of traditional cybercrimes or to commit new types thereof.

2. Concepts of International Judicial Cooperation and Personal Data Protection:

- International Judicial Cooperation: This concept refers to the set of mechanisms and procedures adopted by states to cooperate with each other in legal and judicial matters, especially in combating crime. International judicial cooperation mechanisms include the exchange of information and evidence, mutual legal assistance in investigations and judicial proceedings, extradition, and the enforcement of foreign judicial decisions (Godswill & Kiu, 2024).

- Information Exchange: Information exchange among judicial authorities and law enforcement agencies in different countries is a crucial element of international judicial cooperation. This includes exchanging data related to suspects, victims, evidence, and legal procedures (Dennis, 2022).

- Mutual Legal Assistance (MLA): Refers to cooperation between states in assisting each other in criminal proceedings, such as obtaining witness testimonies, searching premises, freezing and seizing assets (Office in Belgrade, 2013), and providing documents.
- Extradition: Is the procedure by which a person accused or convicted of a crime is surrendered from one country to another for trial or to serve a sentence.
- Personal Data Protection: This concept refers to the set of principles and legal rules aimed at ensuring individuals' rights to control their personal data and protect their privacy when such data is collected, processed, and circulated.
- Automated Processing of Personal Data: Refers to any operation or set of operations performed on personal data by automated means, including the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction. AI systems heavily rely on the automated processing of personal data (dataprotection, 2020).

3. Conceptual Linkages and Study Scope:

- **Relationship between AI-related crimes and International Judicial Cooperation:** The transnational nature of many AI-related crimes necessitates the activation of effective international judicial cooperation mechanisms. However, the unique characteristics of these crimes, such as the difficulty in determining jurisdiction, the nature of digital evidence, and technical challenges in investigation, pose specific challenges to traditional cooperation mechanisms.

- **Relationship between Personal Data Protection and International Judicial Cooperation in the context of AI-related crimes:** Investigating and prosecuting AI-related crimes often requires the collection, processing, and exchange of personal data. This exchange must take place within a legal framework that protects individuals' data privacy rights. Council of Europe Convention No 108 represents an important framework in this context, as it sets out personal data protection principles in the context of automated processing, which is highly relevant to AI systems.

- **Conceptual Dimension of the Study:** This study is based on a conceptual framework that links the three main concepts:

- **AI-related crimes:** As a new and evolving type of crime that poses special challenges to crime-fighting efforts.

- **International Judicial Cooperation:** As an essential tool to address the transnational nature of these crimes.

- **Personal Data Protection "Convention 108":** As a legal framework that regulates data exchange in the context of judicial cooperation and ensures individuals' rights.

- **Scope and Theoretical Boundaries of the Study:** The study primarily focuses on analyzing international cooperation mechanisms in the investigation and prosecution of AI-related crimes from the perspective of Council of Europe Convention No 108 concerning personal data protection and automated processing. The study does not aim to provide a comprehensive analysis of all aspects of AI or all types of cybercrimes, but rather specifically focuses on the interaction between the challenges posed by AI-related crimes and the requirements of international judicial cooperation in light of personal data protection principles.

Through this conceptual framework, the study seeks to provide a solid theoretical basis for analyzing legal texts and materials, interpreting findings, and generating recommendations that contribute to strengthening effective international cooperation in combating AI-related crimes while respecting individuals' rights to personal data protection.

IV. Comparative Analytical Study:

1. First: Analysis of International and National Legal Texts Related to Data Protection and Judicial Cooperation in the Context of AI Crimes

Table 01: Analysis of Council of Europe Convention No 108 - Fundamental Principles of Personal Data Protection and their Impact on Judicial Cooperation

Article/Principle	Explanation and Interpretation Related to Judicial Cooperation in AI Crimes
Article 4: Data	States that personal data must be accurate, complete, up-to-date, and relevant

Quality	for the purposes for which they were collected. In the context of judicial cooperation, the accuracy of exchanged data about suspects and digital evidence must be ensured, which is crucial in AI crimes where evidence may be complex and technical.
Article 5: Data Collection and Processing	Requires personal data to be collected for legitimate and specified purposes, and to be adequate, relevant, and not excessive in relation to these purposes. When exchanging data within judicial cooperation, the purpose must be clearly defined, and it must be ensured that the requested data is necessary for investigating or prosecuting a specific AI-related crime.
Article 6: Security	Obliges parties to take appropriate security measures to protect personal data from unauthorized access, alteration, disclosure, or accidental or unlawful destruction. This principle is vital when exchanging sensitive digital evidence related to AI crimes to ensure its integrity and confidentiality.
Article 8: Individuals' Fundamental Rights	Grants individuals rights such as the right to know of the existence of a personal data file, to obtain a copy of the data, and to have it rectified or erased if inaccurate or processed unlawfully. These rights must be considered when exchanging personal data in the context of judicial cooperation, especially concerning individuals suspected or witnesses in AI crimes.
Article 12: Transborder Data Flows	Places restrictions on the transfer of personal data to other countries unless those countries provide an adequate level of legal protection. This principle poses a significant challenge in the context of international judicial cooperation in AI crimes that often transcend national borders, requiring mechanisms to ensure the protection of transferred data.

Source: Prepared by the researchers

This table illustrates the fundamental principles of personal data protection stipulated in Council of Europe Convention No. 108 and their potential impact on international judicial cooperation in the investigation and prosecution of AI-related crimes. The Convention emphasizes the necessity of data quality, legitimacy of collection, security, and individuals' rights in processing their personal data. It also imposes restrictions on transborder data flows. These principles form an important framework that must be considered when exchanging information and evidence in the context of judicial cooperation to combat AI crimes, highlighting the need to balance security and justice requirements with the protection of the right to privacy.

Table 02: Analysis of the Budapest Convention on Cybercrime - Provisions Related to International Cooperation

Article/Provision	Explanation and Interpretation Related to AI Crimes
Article 23: General Mutual Legal Assistance	States the obligation of parties to afford the widest measure of mutual legal assistance in investigations and proceedings concerning cybercrimes. This can include the exchange of information and the provision of digital evidence related to AI crimes.
Article 27: Procedures concerning digital evidence	Addresses specific procedures for the collection, preservation, and disclosure of digital evidence in the context of international cooperation. This article is of particular importance in AI crimes, where crimes often rely on complex digital evidence.
Article 29: Spontaneous Information Exchange	Allows parties to spontaneously exchange information concerning cybercrimes without prior request in cases of necessity or urgency. This can be beneficial for the rapid detection of cross-border AI crimes.
Article 30: Communication Channels	Defines mechanisms and channels of communication between parties for exchanging requests for legal assistance and information related to cybercrimes. Facilitating effective communication channels is essential for swift cooperation in AI crimes.
Article 32: Extradition	Deals with the conditions and procedures for extraditing persons accused or convicted of cybercrimes. This can apply to perpetrators of AI-related crimes that fall within the scope of the Convention.

Source: Prepared by the researchers

The Budapest Convention on Cybercrime specifically focuses on international cooperation in combating cybercrimes, which increasingly include AI-related crimes. The Convention defines states' obligations to provide mutual legal assistance, exchange information, facilitate the collection of digital evidence, and extradite criminals. These provisions are of crucial

importance in addressing the transnational nature of AI crimes and are complementary to the personal data protection principles stipulated in Convention 108.

Table 03: Analysis of the Additional Protocol to Convention 108 - Supervisory Authorities and Transborder Data Flows

Article/Provision	Explanation and Interpretation Related to Judicial Cooperation in AI Crimes
Article 1: Supervisory Authorities (Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018)	Obliges parties to establish independent supervisory authorities responsible for ensuring compliance with personal data protection principles. These authorities can play a role in overseeing data exchange operations within judicial cooperation related to AI crimes.
Article 2: Mutual Assistance Between Supervisory Authorities	States the obligation of supervisory authorities to provide mutual assistance to each other in the performance of their duties, including the exchange of information and assistance in investigations. This cooperation can be beneficial in cases involving the unlawful processing of personal data using AI technologies.
Article 3: Transfer of Data to Another State	Defines additional conditions for the transfer of personal data to states not bound by the Convention, with a focus on ensuring adequate safeguards for the transferred data. This provision poses a challenge when cooperating with non-party states in investigations related to AI crimes.

Source: Prepared by the researchers

The Additional Protocol to Convention 108 adds provisions concerning independent supervisory authorities and their role in ensuring compliance with personal data protection principles, as well as regulating transborder data flows. Supervisory authorities can play a significant role in overseeing data exchange operations in the context of judicial cooperation to combat AI crimes and ensuring respect for individuals' data protection rights. Furthermore, the provisions concerning transborder data flows highlight the need for mechanisms that ensure an adequate level of protection when exchanging data with other countries in this context.

Table 04: Analysis of Examples of Comparative National Legislations (French Example) - Provisions Related to Cybercrimes and Data Protection

Law/Article	Explanation and Interpretation Related to AI Crimes and Judicial Cooperation
French Penal Code - Articles Related to Cybercrimes (e.g., hacking, computer fraud)	These articles define acts considered cybercrimes and their prescribed penalties. These provisions can apply to AI-related crimes that use digital technologies. In the context of judicial cooperation, these articles establish the legal basis for requesting legal assistance or extradition.
Law No. 78-17 of January 6, 1978, on Data Processing, Data Files, and Liberties, as amended (lafrenchtech, 2020)	Defines personal data protection principles in France, consistent with Convention 108 and the General Data Protection Regulation (GDPR). This law sets out the conditions for data collection, processing, and transfer, which must be considered when exchanging information with other countries within judicial cooperation.
French Code of Criminal Procedure - Articles Related to International Legal Assistance	These articles define the procedures and rules for providing and receiving mutual legal assistance in criminal matters with foreign states. These articles establish the legal framework for exchanging information and evidence in investigations related to AI crimes.

Source: Prepared by the researchers

This table provides an example of how national legislations deal with cybercrimes, personal data protection, and international judicial cooperation. It illustrates how national laws define criminal acts, establish rules for data protection, and regulate cooperation procedures with other countries. When dealing with cross-border AI crimes, it is essential to understand these national legislations and how they interact with international conventions such as Convention 108 and the Budapest Convention.

Table 05: Analysis of Mutual Legal Assistance and Extradition Treaties (General Models)

Provision/Procedure	Explanation and Interpretation Related to AI Crimes
Scope of Mutual Legal Assistance	Usually includes the exchange of information and evidence, searches of premises, hearing of witnesses, and provision of documents. These mechanisms can be used in investigations related to AI crimes to collect digital evidence and identify suspects.
Grounds for Refusal of Assistance	Typically include threats to national security, public order, or violation of fundamental principles of law or human rights in the requested state. It must be ensured that requests for assistance related to AI crimes comply with these principles, especially concerning personal data protection.
Extradition Procedures	Define the conditions and procedures for extraditing persons accused or convicted of crimes. These procedures can apply to perpetrators of AI-related crimes if the acts constitute offenses punishable by law in both states.
Principle of Dual Criminality	Usually requires for extradition that the act committed constitutes an offense punishable by law in both the requesting state and the requested state. This may pose a challenge in new AI crimes that may not be explicitly criminalized in all states.

Source: Prepared by the researchers

This table illustrates the general provisions and procedures stipulated in mutual legal assistance and extradition treaties. These treaties are important tools for international judicial cooperation in combating all types of crimes, including AI-related crimes. The specific nature of AI crimes, such as the difficulty in determining jurisdiction and the emergence of new criminal acts, may require adapting and interpreting these treaties to apply them effectively in this context. Additionally, principles such as dual criminality and human rights protection must be considered when activating these mechanisms in AI crime cases.

2. Second: Comparison Between the Legal Texts Discussed

Table 6: Analytical Comparison of the Contents of the Previous Tables

Point of Comparison	Council of Europe Convention No. 108	Budapest Convention on Cybercrime	Additional Protocol to Convention 108	Comparative National Legislations (French Example)	Mutual Legal Assistance and Extradition Treaties (General Models)
Main Focus	Protection of personal data in the context of automated processing.	International cooperation in combating cybercrimes. (Jonathan, 2014)	Enhancing data protection through supervisory authorities and regulating transborder data flows.	Criminalizing electronic acts, regulating data protection, and judicial cooperation procedures at the national level.	Mechanisms and procedures for international judicial cooperation in criminal matters.
Data Protection Principles and their Impact on Cooperation	Emphasizes data quality, legitimacy of collection, security, individuals' rights, and restricting transfer to countries with inadequate protection levels. Forms a framework that must be considered when exchanging information in	Does not directly address data protection principles in the same detail, but requires safeguards when exchanging information and digital evidence.	Enhances data protection through supervisory authorities and regulates data transfer in more detail, affecting cooperation conditions.	National laws include data protection principles (often consistent with Convention 108 and/or GDPR), affecting how information is exchanged with other countries.	Requires respect for human rights and fundamental legal principles, which implicitly include personal data protection when exchanged.

	judicial cooperation.				
International Cooperation Mechanisms	Does not directly stipulate judicial cooperation mechanisms, but influences how data is exchanged within these mechanisms.	Defines clear mechanisms for cooperation in cybercrimes, such as mutual legal assistance, information exchange, and extradition.	Focuses on cooperation between supervisory authorities for data protection, which can support judicial cooperation in data-related cases.	Stipulates national procedures for providing and receiving international legal assistance and defines extradition conditions.	Defines the scope of legal assistance, grounds for refusal, and extradition procedures and conditions (e.g., dual criminality principle).
Challenges Related to AI Crimes	Highlights challenges related to transferring personal data necessary for investigating cross-border crimes to countries with different protection levels.	Provides tools for dealing with the transnational nature of digital crimes, which include AI crimes, but may need adaptation to address the unique characteristics of these crimes.	Adds another layer of considerations when transferring data for judicial cooperation purposes, especially with countries not party to the Convention.	Definitions of cybercrimes, scope of data protection, and cooperation procedures may vary between countries, hindering effective cooperation in AI crimes.	The principle of dual criminality may pose a challenge in the case of new AI crimes that have not been uniformly criminalized. Dealing with complex digital evidence also requires specialized expertise.
Potential Points of Integration	The data protection principles in Convention 108 can form a framework for ensuring respect for fundamental rights when applying cooperation mechanisms stipulated in the Budapest Convention and legal assistance treaties.	The Budapest Convention can provide practical mechanisms for implementing judicial cooperation while respecting data transfer restrictions and individuals' rights stipulated in Convention 108.	Supervisory authorities can contribute to facilitating secure and lawful information exchange within judicial cooperation.	National legislations can implement international obligations and provide specific mechanisms for cooperation while respecting data protection principles.	Considered the general framework for cooperation, and must be applied while considering specific data protection rules in other conventions and national legislations.

Source: Prepared by the researchers

This table illustrates how various legal texts interact in the context of international cooperation to combat AI-related crimes and protect personal data:

- Convention 108 focuses on setting standards for personal data protection, which is crucial when exchanging information within judicial cooperation. The data transfer restrictions it imposes constitute a challenge that must be overcome with adequate safeguards.

- The Budapest Convention provides the practical framework for cooperation in cybercrimes, including the exchange of digital evidence and the provision of legal assistance.

However, it may require flexible interpretation and application to address the unique characteristics of AI crimes.

- The Additional Protocol to Convention 108 enhances data protection and adds an institutional dimension through the role of supervisory authorities, which can contribute to building trust in cross-border data exchange operations for judicial cooperation purposes.

- National legislations play a vital role in implementing international obligations and defining national cooperation procedures. Discrepancies among these legislations can create challenges for effective cooperation.

- Mutual Legal Assistance and Extradition Treaties represent traditional tools for cooperation, but their application to AI crimes requires considering the digital nature of these crimes and challenges related to jurisdiction, dual criminality, and digital evidence.

V. Results and discussion:

1. Results

- Council of Europe Convention No. 108 emerges as a primary source of principles related to personal data protection in the context of automated processing. These principles directly influence international judicial cooperation mechanisms in combating AI-related crimes, as the exchange of sensitive digital information and evidence must comply with these standards to ensure respect for the right to privacy.

- The Budapest Convention on Cybercrime provides a practical framework for international cooperation in combating cybercrimes, which increasingly include AI-related crimes. The Convention defines mechanisms for mutual legal assistance, exchange of information and digital evidence, and extradition, enhancing states' capacity to address these cross-border crimes.

- The Additional Protocol to Convention 108 strengthens the data protection regime by defining the role of independent supervisory authorities and regulating transborder personal data transfers in more detail. This Protocol adds an extra layer of legal consideration when exchanging data for judicial cooperation purposes in AI crime cases, especially with states not party to the Convention.

- An analysis of comparative national legislations reveals discrepancies in the definitions of cybercrimes, the scope of data protection, and judicial cooperation procedures among states. These discrepancies hinder effective cooperation in investigating and prosecuting AI-related crimes, necessitating greater legislative convergence.

- Mutual legal assistance and extradition treaties are essential tools for judicial cooperation, but their application to AI crimes faces challenges related to the digital nature of evidence, jurisdiction determination, and the principle of dual criminality in light of emerging AI-related criminal acts.

- The unique characteristics of AI crimes, such as the complexity of digital evidence and the difficulty in determining criminal liability, require flexible adaptation and interpretation of existing legal frameworks to ensure their effectiveness in combating these crimes.

- The analysis highlights the urgent need to enhance the exchange of expertise and technical knowledge among law enforcement agencies and judicial authorities in different countries to understand the nature of AI crimes and how to collect and analyze complex digital evidence associated with them.

- The absence of standardized criteria for collecting, preserving, and exchanging digital evidence poses a significant challenge to international judicial cooperation in AI crime cases, necessitating efforts to develop such standards to facilitate effective cooperation.

- The transnational nature of AI crimes raises challenges related to determining the competent jurisdiction for investigation and prosecution, requiring the search for legal solutions that ensure perpetrators of these crimes do not escape punishment.

- The private sector, possessing advanced expertise and technologies in AI, can play a crucial role in supporting efforts to combat AI-related crimes through cooperation with law enforcement agencies and judicial authorities.

- Effective handling of AI crimes requires the presence of specialized judges and investigators with a deep understanding of AI technologies and related legal aspects, necessitating the development of specialized training programs in this field.

- The analysis demonstrates that balancing security requirements, crime fighting, and personal data protection presents an ongoing challenge in the context of international judicial

cooperation in AI crime cases. It requires finding solutions that achieve security objectives while respecting individuals' fundamental rights.

- The analysis indicates that current international legal frameworks may not be sufficient to address all the challenges posed by AI crimes, necessitating consideration of developing new international agreements or protocols specifically addressing these crimes.

- Data protection supervisory authorities can play a pivotal role in facilitating the secure and lawful exchange of personal data between states for judicial cooperation purposes, by providing advice, guidance, and oversight of these operations.

- Effectively dealing with the rapid evolution of AI crimes and their legal and technical complexities requires continuous international dialogue and the exchange of views and best practices among states, international organizations, academics, and experts in this field.

2. Discussion:

The findings of this study represent an in-depth analysis of the challenges and opportunities related to activating international cooperation mechanisms in the investigation and prosecution of AI-related crimes, with a focus on the impact of Council of Europe Convention No. 108 on personal data protection. The rapid development of AI technologies and the accompanying potential for misuse in criminal activities necessitate a precise understanding of the existing international legal framework and how it interacts with these emerging challenges.

The first finding highlights the pivotal importance of Convention 108 in guiding personal data exchange operations in the context of judicial cooperation. The principles stipulated in the Convention concerning data quality, legitimate collection, security, and individuals' rights represent a fundamental standard that must be adhered to to ensure respect for the right to privacy when combating AI-related crimes. The fifth finding indicates that the restrictions imposed by the Convention on transborder data flows may pose a practical challenge to cooperation with countries that do not adhere to similar protection standards. This necessitates finding mechanisms to ensure adequate safeguards for transferred data, perhaps through complementary bilateral or multilateral agreements.

Conversely, the second finding sheds light on the vital role of the Budapest Convention in providing practical tools for international cooperation in the field of cybercrimes, which increasingly include AI-dependent crimes. The mechanisms for mutual legal assistance, information and digital evidence exchange, and extradition stipulated in the Convention form an important basis for cooperation. As the sixth finding indicates, the unique nature of AI crimes requires flexible adaptation and interpretation of these mechanisms, especially concerning complex digital evidence and determining criminal liability in cases where human actions intersect with the operation of AI systems.

The fourth finding emphasizes the disparity in national legislations as an obstacle to effective cooperation. Differences in cybercrime definitions, data protection scope, and judicial cooperation procedures among states that are parties and non-parties to Convention 108 and the Budapest Convention can hinder the process of evidence exchange and the implementation of cross-border legal procedures. This underscores the need for international efforts to harmonize legislations and unify fundamental concepts related to AI crimes and data protection.

The seventh and eighth findings point to the significant technical challenges facing judicial cooperation in the field of AI crimes. The exchange of specialized technical expertise and knowledge in understanding the operation of AI algorithms and analyzing complex digital evidence is essential for successful investigations. Furthermore, the absence of standardized criteria for collecting, preserving, and exchanging digital evidence significantly impedes states' ability to cooperate effectively. This calls for international investment in developing these standards and providing the necessary training for law enforcement agencies and judicial authorities.

The eleventh finding emphasizes the importance of building specialized capabilities for judges and investigators to deal with these emerging crimes. Understanding the basic technologies of AI and how they can be used in criminal activities, in addition to familiarity with legal aspects related to digital evidence and data protection, is an imperative necessity for effective investigations and fair prosecution.

From an institutional perspective, the third finding indicates the increasing importance of data protection supervisory authorities, as stipulated in the Additional Protocol to Convention 108. These authorities can play a pivotal role in facilitating the secure and lawful exchange of personal data for judicial cooperation purposes, through oversight, advice, and ensuring compliance with protection standards. The tenth finding also highlights the importance of cooperation with the private sector, which often possesses advanced technical knowledge of AI systems, in supporting efforts to combat these crimes.

The ninth finding underscores the ongoing challenges related to jurisdiction in cyberspace, where AI-related crimes easily transcend national borders. This necessitates continuous research for legal solutions that ensure perpetrators of these crimes do not escape punishment, perhaps through expanding the scope of jurisdictional principles or developing new mechanisms for joint cross-border investigations.

The twelfth finding points to the complex nature of the balance between security requirements, crime fighting, and personal data protection in this context. Any international cooperation mechanism must strive to achieve this delicate balance, ensuring that individuals' fundamental rights are not sacrificed in the name of security.

The thirteenth and fifteenth findings call for the necessity of considering the development of new international legal frameworks that specifically address the unique challenges posed by AI crimes, and for establishing continuous international dialogue and exchange of views and best practices among all concerned parties. The rapid development of AI technologies necessitates a flexible and adaptable international legal response that considers both the potential of these technologies to serve crime and the need to protect fundamental rights and freedoms of individuals in the digital age. Enhancing effective international cooperation in this field requires a shared commitment to overcoming legal, technical, and institutional challenges, and building an international criminal justice system capable of confronting these emerging threats.

VI. Study Recommendations:

Based on the study's findings and discussion, we can offer a set of recommendations to enhance international cooperation in investigating and prosecuting AI-related crimes while ensuring personal data protection:

- Develop supplementary international protocols or agreements to the Budapest Convention and Convention 108 that specifically address the legal and technical challenges posed by AI-related crimes, including standardized definitions of these crimes and procedures for collecting and analyzing digital evidence.

- Undertake international efforts to harmonize national legislations related to cybercrimes and personal data protection, especially concerning acts involving the use of AI technologies, to facilitate judicial cooperation and cross-border evidence exchange.

- Establish international platforms or mechanisms for exchanging specialized technical expertise and knowledge among law enforcement agencies and judicial authorities in the field of AI and digital evidence, including the development of shared tools and techniques for digital forensics.

- Work towards establishing unified international standards for the collection, preservation, and exchange of digital evidence in the context of criminal investigations related to AI crimes, to ensure their admissibility in judicial proceedings across different countries.

- Explore and develop innovative legal solutions for jurisdictional challenges in cyberspace facing the investigation of cross-border AI crimes, including expanding the scope of jurisdictional principles or creating mechanisms for joint investigations.

- Build effective mechanisms to enhance cooperation among law enforcement agencies, judicial authorities, and the private sector (such as technology companies and AI service providers) to exchange information and provide technical assistance in investigations related to AI crimes.

- Design and implement specialized training programs for judges, investigators, and prosecutors on the nature of AI crimes, advanced digital investigation techniques, and legal aspects related to data protection in the context of international cooperation.

- Develop secure and effective communication channels between states for exchanging information and requests for legal assistance related to AI crimes, while ensuring compliance with data protection standards.

- Empower and enhance the role of data protection supervisory authorities in facilitating the secure and lawful exchange of personal data for judicial cooperation purposes, and potentially establish mechanisms for direct cooperation between these authorities and their counterparts in other countries.

- Support and encourage continuous international dialogue and the exchange of views and best practices among states, international organizations, academics, and experts in the field of combating AI crimes and data protection, to ensure keeping pace with rapid developments in this area.

VII. Conclusion:

In conclusion, this analytical study has sought to clarify the challenges and opportunities related to enhancing international cooperation in the investigation and prosecution of AI-related crimes, with particular attention to the impact of Council of Europe Convention No. 108 on personal data protection. The analysis revealed that the accelerating development of AI technologies has created new forms of cross-border crimes, necessitating concerted international efforts to address them effectively. While existing international legal frameworks, such as the Budapest Convention and Convention 108, provide important foundations for cooperation, they face challenges in adapting to the unique nature of these crimes and their technical and legal complexities.

The study highlighted the need to strike a delicate balance between the requirements of security and crime fighting and the necessity of protecting personal data and fundamental rights of individuals in the context of international judicial cooperation. Activating cooperation mechanisms requires overcoming discrepancies in national legislations, developing unified standards for digital evidence, enhancing the exchange of technical expertise, and building specialized capacities among judges and investigators. Furthermore, the increasing role of data protection supervisory authorities and cooperation with the private sector are crucial elements in building an effective and reliable international cooperation system.

The study emphasizes the importance of adopting a comprehensive and integrated approach to enhancing international cooperation in combating AI-related crimes. This includes developing supplementary international legal frameworks, harmonizing national legislations, establishing mechanisms for information and expertise exchange, investing in specialized training, and fostering continuous international dialogue. Addressing this global challenge requires a shared commitment from all states, international organizations, and concerned parties to work together to ensure the safe and responsible use of AI technologies and to protect societies from the risks of their misuse in criminal activities.

VIII. References:

Caldwell, M., & al. (2020, August 5). AI-enabled future crime. *Crime Science*(14), pp. 1-13. doi:<https://doi.org/10.1186/s40163-020-00123-8>

Christopher, C., & al. (2021, October). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, p. 102383. Retrieved from <https://doi.org/10.1016/j.ijinfomgt.2021.102383>

Council of Europe. (2018). *Convention 108 + Convention for the protection of individuals with regard to the processing of personal data*. Council of Europe.

dataprotection. (2020). *Your rights in relation to automated decision making, including profiling (Article 22 of the GDPR)*. Retrieved 03 04, 2025, from dataprotection: <https://www.dataprotection.ie/en/individuals/know-your-rights/your-rights-relation-automated-decision-making-including-profiling>

Dennis, G. (2022, June). International Law Enforcement, Judicial Cooperation and Criminal Investigations under the New EU and UK Cooperation Agreement: What Are the

Implications for Data Sharing, Mutual Legal Assistance and Extradition? *SSRN Electronic Journal*, pp. 2-6. doi:<http://dx.doi.org/10.2139/ssrn.4265899>

(2018). *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. European Treaty Series - No. 108, Strasbourg. Retrieved from <https://rm.coe.int/16800ca434>

Godswill, O. A., & Kiu, P. E. (2024, May). Methods of Judicial Cooperation and the Procedure for Enforcement Under International Law; Identifying the Nexus between Theory and Practice. *NEWPORT INTERNATIONAL JOURNAL OF CURRENT RESEARCH IN HUMANITIES AND SOCIAL SCIENCES*(3), pp. 80-88. Retrieved from <http://dx.doi.org/10.59298/NIJCRHSS/2024/4.3.8088>

Jonathan, C. (2014, January). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University law review. Monash University. Faculty of Law*(3), p. 698.

lafrenchtech. (2020). *Personal Data*. Retrieved 03 06, 2025, from lafrenchtech: <https://lafrenchtech.gouv.fr/en/personal-data/>

Malatji, M., & Alaa, T. (2024, February). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI and Ethics*. Retrieved from <http://dx.doi.org/10.1007/s43681-024-00427-4>

Nadiya, I., Oksana, B., Viacheslav, K., & Yurii, M. (2023, August). International Legal Cooperation in the Field Of Criminal Justice: New Challenges and Ways to Overcome Them. *Journal of Law and Sustainable Development*(4), p. e767. Retrieved from <http://dx.doi.org/10.55908/sdgs.v11i4.767>

Office in Belgrade. (2013). *MUTUAL LEGAL ASSISTANCE MANUAL*. Belgrade: Council of Europe.

Ratnawita. (2022). Cybersecurity in the AI Era Measures Deepfake Threats and Artificial Intelligence-Based Attacks. *Journal of the American Institute*, pp. 180-185.