

Using Technology to Fight Impunity: An Examination of International Criminal Accountability over Time in Cases of Extradition

Abhinav kumar

Research Scholar, DNLU Jabalpur, abhinavphd@mpdnlu.ac.in

Abstract

The study aims to examine how impunity in international and transnational crimes has significantly undermined the effectiveness of the global criminal justice system, particularly in cases involving extradition. Traditionally bound by the state sovereignty, political goodwill and inefficiency of their processes the extradition systems tended to find more people who committed serious crimes such as war crimes, crimes against humanity, and new cyber-enabled crimes able to escape justice processes. This paper will analyse how technological innovation has gradually changed international criminal accountability over the years, specifically addressing extradition practices. It follows the historical development of extradition from bilateral, diplomacy-based agreements to modern, digitally integrated frameworks. It is a critical analysis of how digital tools can be utilised to enhance the efficiency, transparency, and reliability of extradition and cross-border investigations, including biometric identification systems, artificial intelligence, blockchain-based evidence management, real-time communication networks, and digital mutual legal assistance platforms. The paper relies on the analysis of doctrine, case studies, and recent academic literature to identify how technology has minimised jurisdictional holes, expedited judicial collaboration, and enhanced evidential plausibility. Simultaneously, it identifies unresolved legal and ethical issues concerning data privacy, algorithmic bias, sovereignty, and uneven technological capabilities across states. The issue that is developed in the paper is that as much as technology has emerged as a critical tool in the war against impunity, it should be legitimised through strong legal protection, ethical governance, and fair global collaboration. In the end, the paper points out that technologically facilitated extradition is not only a possibility, but a challenge to develop an even smoother and rights-observing system of global criminal justice.

Keywords

International Criminal Justice; Extradition; Impunity; Digital Evidence; International Criminal Accountability; Transnational Crime

1. Introduction

The struggle to combat impunity of international crimes has been at the heart of the international justice system, and it has changed along with the changes in political goodwill, legislation, and advances in technology (Pettersen, 2023). Historically, the application of accountability measures, especially extradition, has been politically resisted and has had loopholes in the law and efficiency blinds in the procedures that allowed the perpetrators of war crimes, crimes against humanity, and genocide to go unpunished (Kasera et al., 2024). The

difference between the moral requirement of prosecution and the political unwillingness to extradite provided a loophole in which impunity thrived at the expense of the strength of international law. Nevertheless, with the advent of globalization and technological interdependence, this has changed and made available to states and international institutions more than ever before a series of tools to trace, arrest, and convict transnational criminals (Antai et al., 2025). Globalization has reconstructed the international criminal responsibility. It has acted to enable the transnational crime and the cooperation of states to be achieved due to increased interconnectivity between states. Although contemporary communication technologies have facilitated the operations of networks of corruption, terrorism, and cybercrime across borders, they have also allowed the legal institutions to retaliate at the same level of sophistication. Online databases, biometric identification software, and real-time communication networks like the I-24/7 of INTERPOL have enabled law enforcement teams to share crucial information between jurisdictions in a few seconds (Jinga & Debebe, 2022). The technological revolution is a breakthrough in the manual and paper-based extradition process to interoperable and digital systems capable of aligning efforts across legal traditions. The contribution of technology to the fight against impunity goes way beyond administrative effectiveness. Digital forensics, artificial intelligence, and blockchain-based evidence tracking have become the mandatory elements of international criminal investigations. Digital evidence has proven very important in supporting witness expertise, as well as in confirming the patterns of atrocities, in cases before tribunals including the International Criminal Court (ICC) and the ad hoc tribunals of former Yugoslavia and Rwanda (Oyewole, 2024). The case of the technological hub being integrated into the International Centre for the Prosecution of the Crime of Aggression against Ukraine is one of the modern examples of how digital justice platforms may help bring different national initiatives together to seek international accountability. Among the most significant changes, there is the digitalization of extradition and transnational criminal procedures. Conventionally, extradition was tedious, arduous, and very subject to political goodwill. Transparency, poor communication lines, and identity verification were some of the factors that slowed down requests (Alizade, 2025). Digital transformation has, however, solved most of these problems. Biometric databases (fingerprint, face recognition, etc.) give states a chance to match the suspect identity with a high level of accuracy, minimizing the wrongful extradition and increasing the legitimate extradition. Such technologies as the European Arrest Warrant (EAW) and the Schengen Information System (SIS II) are examples of how the digital integration allows the rapid cooperation of the courts and reduces the bureaucratic delays. Technology is also important in curbing emerging forms of transnational crimes, especially cybercrime. As electronic space is taking center stage in economic and criminal practices, cyber-based crimes like hacking, identity theft, and other digital financial offenses are disrupting the traditional concept of jurisdiction since criminals can perpetrate crimes in one jurisdiction and reside virtually in another (Gundur et al., 2021). The introduction of digital cooperation systems, mutual legal assistance portals, and protected evidence transfer systems is now a necessity to prevent jurisdictional stalemates that enable perpetrators to escape liability. further points out that though international law is slowly adjusting to the digital age, there are still gaps to harmonize cyber-extradition policies and

determine the boundaries of cyber-sovereignty. However, there are challenges to the integration of technology in international criminal justice. The question of data privacy, surveillance, and evidentiary integrity is still at the center of the legal controversy. Identifying suspects through AI-operated surveillance systems and predictive policing, not to mention making things efficient, brings up ethical issues in the form of prejudice, misuse of data, and the loss of civil liberties. Also, as Banach-Gutierrez (2023) contends, the legal framework of the European Union reflects that there is a fine line between responsibility and protection of basic rights in implementing digital technologies as a means of cross-border law enforcement. In addition to the practical implementation, the technology has also transformed the philosophical definition of impunity. The term in the past was mostly associated with the inability of the states to prosecute or extradite criminals. In the digital era, impunity also includes the lack of ability to control or adequately react to computer-assisted crimes, fake information campaigns, and computer-enabled state-sponsored atrocities. Although international tribunals play a crucial role, they need to constantly adapt to the growing digital aspect of warfare as well as transnational crimes. In this way, technological adaptation is not just a procedural issue but a moral issue in the process of ensuring international justice. In addition, technology collaboration has enhanced international partnerships and the enhancement of transparency. Collective responsibility in the extradition process is achieved by the use of interoperable databases, shared digital forensic laboratories, and online evidence repositories and minimizes the one-sided politicization of extradition. Such organizations as the ICC, EUROPOL, and UNODC have started using AI-based analytics to spot criminal networks and simplify case management. This integrated strategy represents one of the general changes in international justice, from an incomprehensive national practice to comprehensive global governance mechanisms that see technology as an instrument and a cohesion factor (Racoveanu, 2024). Technology has become one of the characteristic features of the development of international criminal responsibility. It fills the loopholes that are presented by jurisdiction boundaries, increases the credibility of the evidence, and expedites the cross-border extradition of offenders. Nevertheless, this advancement also requires both an ethical and legal reconsideration of the process in which states exercise digital authority on the pretext of justice. With the global conflicts, cyber threats, and transnational crimes continuously developing, the application of technology in the fight against impunity will be a pillar of the contemporary international criminal law, and it will be a factor that not only succeeds in prosecutions but also makes the global justice system self-sufficient.

2. Historical Overview: Extradition and the Struggle Against Impunity

Extradition history and its impact on fighting impunity in international crimes show the larger development of the international criminal law (ICL) (Antai, 2024). From the beginning of its bilateral form of diplomatic practice to its metamorphosis into an element of international justice, extradition has been a facet of responsibility as well as a reflection of political determination or the absence thereof by states to exercise justice (Asghar et al., 2025). Although the contemporary and internationalized form of twentieth-century law is represented by the International Criminal Court (ICC) and the ad hoc tribunals of the 1990s, the transformation of

the sovereign privilege into the globalized responsibility is still a complicated process, which depends on interactions between law and politics and technology (Ashraf, 2025; Sadat, 2022).

2.1 Early Roots of Extradition: From Sovereignty to Reciprocity

In its early manifestation, extradition came to be a diplomatic arrangement that was based on reciprocity and not justice. However, ancient treaties, including the ones between Egyptian and Hittite kingdoms, laid the groundwork for the practice of surrendering fugitives, although these treaties were made on the basis of political expediency rather than humanitarian spirit. In the medieval era, the ideology of sovereignty prevailed in international affairs, and extradition was mostly a matter of the goodwill of the rulers instead of the legal norms being put in place. One of the first codifications of the extradition in the contemporary international law was the Sair (2024), between the United States and Great Britain. The concept of the alleged double criminality, that individuals must commit an offense in both countries to be extradited, proved to be an insurance to the citizens as well as a burden on justice. This condition frequently made offenders of politically motivated offenses immune to extradition, which created a conflict between the sovereignty of any state and international justice that still exists.

2.2 The Nineteenth and Early Twentieth Centuries: Building a Framework for Cooperation

The gradual transition into the institutionalized extradition practices occurred during the nineteenth century. Bilateral and multilateral treaties started to formalize practices, and some terms like the political offense exception came up to defend those who were pursued due to committing crimes that can be classified as political, but not criminal. Although the principle worked in the interest of the dissidents by protecting them against persecution, it was mostly abused by individuals who were accused of committing atrocities in the name of political legitimacy.

The International Penal Law Treaty of 1889 marked a significant step since it established the prerequisites of reciprocal extraditing of gravest offenders and imposed the idea that the whole world needed to collaborate to ensure international order (Pataraiia, 2021). However, even as the law was evolving, there was still an uneven implementation. The national sovereignty and political interests still prevailed and dominated the new feeling of universal jurisdiction. This was the time during the inter-war that attempts were made to formalize extradition and accountability especially following the atrocities of World War I. Nevertheless, the inability to prosecute people like Kaiser Wilhelm II emphasized the weakness of the current legal systems and the unwillingness of the states to hand over their citizens or political partners. This period led to the development of the principle of *aut dedere aut judicare*, which translates to the idea of either extraditing or prosecuting, the idea of collective responsibility in safeguarding justice even where no actual international execution is happening.

2.3 The Nuremberg Precedent: A Turning Point for Accountability

The Nuremberg Trials (1945-46) was a radical break in centuries of impunity of state-sponsored crime. It was the first time when people (not only states), but when people were to be liable to international law infractions. The creation of the International Military Tribunal

brought legal ideas like crimes against humanity and war crimes to the international jurisprudence that was binding. In human rights discourse, Nuremberg was a landmark of the so-called turn to criminal law, as the international justice could now be employed as the instrument of fighting impunity. But, although accountability got institutionalized at Nuremberg, the structural obstacles to extradition were not removed. The trials were based on the military control of the Allies but not the multilateral cooperation. A large number of the criminals were able to evade justice due to the fact that they fled in other countries, and the politics of Cold War soon reduced the trends on international enforcement of crimes.

2.4 The Ad Hoc Tribunals: ICTY and ICTR as Modern Mechanisms of Extradition

The international criminal tribunal in former Yugoslavia (ICTY) and the international criminal tribunal in Rwanda (ICTR) that were established through the post-cold war strengthened fight against impunity in the world. These tribunals incorporated the extradition and international cooperation by UN Security Council orders that required states to hand over suspects and even support investigations. These organizations represented the evolution of global justice, but at the same time, they exposed the fact that the process of extraditing suspected persons out of the sovereign states was fraught with political and logistical challenges. Indicatively, some ICTY suspects have dodged arrests over a period of time because of lack of eagerness by states to deliver the arrest warrants. The example of Radovan Karadžići who avoided extradition in more than ten years showed the weaknesses of basing the cooperation on the willingness of states. However, both tribunals developed the principle that the extradition was a part of the international accountability and created pattern forms of proceedings that became used subsequently by the ICC.

2.5 The International Criminal Court and the Globalization of Accountability

The institutionalization of the fight against impunity of the international community is the Rome Statute of 1998 that created the ICC. The jurisdiction of the Court over the genocide, crimes against humanity and the war crimes represents an extension of the principles that were established in Nuremberg and in the ad hoc tribunals. ICC relies on the cooperation of the states in the process of arresting and extraditing so many fugitives, which is not evenly distributed in the geopolitical realm. It has been argued that non-member states have been particularly opposed to the ICC which has been accused of partiality in enforcement especially in Africa given that African countries have come up with regional extradition frameworks such as the African Union Model Law on Extradition, but the political interference and sovereignty concern still hamper the achievement of universal accountability.

2.6 Political Interference and the Limits of Sovereignty

The relationship between extradition and political power has been known to determine the boundaries of justice throughout history. States have invoked the sovereignty, national security or political offense exceptions in order to avoid handing over suspects, effectively granting de facto impunity to politically well-connected criminals on the basis of their adopted country. Politicization of extradition has continued to be among the greatest hindrances to international justice. Despite technological advances and improved legal frameworks, the ultimate decision

to extradite often rests on political calculus rather than legal merit. The struggle against impunity thus continues to oscillate between the normative aspirations of international law and the pragmatic realities of domestic politics.

3. Literature Review

According to the recent scholarship, extradition and other associated processes of international judicial cooperation have taken center stage in the fight against impunity in the era of transnational crime and digitalization. According to Asghar et al. (2025), the history of extradition, a key tool in the reestablishment of states in the pursuit of those who refuse to be charged, can be traced back to ancient, medieval, and modern legal foundations, since it functions as a fundamental instrument of reestablishing the state in the context of a structured legal domain, procedures, and commitments of the state by treaty. Nonetheless, cybercrime, as well as other transnational crimes, has challenged the efficiency of extradition. Alizade et al. (2025) suggest that conventional approaches to extradition, which are based on state sovereignty and reciprocity, are not well suited to cybercrime, where the attribution can be complex, the evidence is digital, and the enforcement process is frequently slowed down, and human rights issues and due process concerns may often arise. In this regard, Abdelkarim et al. (2025) note that mutual legal assistance is a more realistic and less controversial alternative to universal jurisdiction and show in the example of the UN Cybercrime Convention that the combination of coordinated extradition, consultation of jurisdiction, and exchange of evidence will help to maintain state sovereignty without compromising it and increase accountability. To add to this perspective, Ajayi et al. (2025) underline that the absence of substantive cyber laws, jurisdictional fragmentation, and international consensus seriously undermine the process of investigation and prosecution, which supports the necessity of the adoption of unified legal norms and partnership. Meanwhile, Thierry et al. (2024) and Aksamitowska et al. (2021) emphasize that the current trend is the increased role of technology and forensic science, such as digital and open-source evidence, in international criminal cases, but warn that the admissibility regulations, chain of custody, and administrative limitations still hamper justice. The normative principles in the category of *aut dedere aut judicare* also commit the state to extradite or prosecute severe offenders, but empirical data has shown that only a part of them does so because of the political motive and the human rights concerns (Iranzi et al., 2024). All these works reveal a changing environment of international criminal justice where extradition, mutual legal assistance, and technologically facilitated investigations are forced to keep up with cyber-enabled and transnational crimes, balancing sovereignty, efficiency, and the safeguarding of basic human rights (Zakir et al., 2024; Ndubuisi et al., 2022; Dandurand et al., 2022).

4. Technological Innovation and the Transformation of International Accountability

The international law process of holding those in power accountable has been redefined greatly by the digital transformation of the global governance and justice systems. No longer bound by bureaucracy defined by paper or even the geographical boundaries of sovereignty, new institutions are turning to digital structures in tracking, investigating and prosecuting cross-border offenses. These technological changes - which cover digital evidence, artificial

intelligence, blockchain authentication, and data-driven cooperation - have not only made the extradition process faster, but have also improved international criminal justice transparency and integrity. Technology has also brought a new architecture of accountability where digital systems become actively involved in monitoring and enforcing the international law provisions (Rehman, 2023).

The discussion in this section is on how digital innovations are changing the pursuit of justice in international criminal law based on three intersecting aspects which include: (1) digital evidence and forensic technologies; (2) cybercrime and extradition in the digital era; and (3) emergence of justice hubs as a model of technological cooperation in accountability.

4.1 Digital Evidence and Forensic Technologies

The contemporary extradition and prosecution have turned out to depend on digital evidence. The development of forensic science, satellite, and blockchain-based verification systems have significantly changed the process of collecting evidence, verifying it, and presenting it, in transnational cases, because it no longer performs the task of ensuring that physical boundaries do not allow the perpetrators to escape responsibility digital technologies, including high-resolution satellite photos, geolocation tags, and drones are now a necessity in recording the atrocities of war, human rights infractions, etc. notes that digital technologies, including high-resolution satellite photos, geolocation tags, and drones, become essential in document (Karagiannis & Vergidis, 2021).

The digital evidence has also increased admissibility in international judicial systems. Criminal justice bodies such as the International Criminal Court (ICC) and ad hoc courts are more and more turning to metadata, encrypted messages, and digital forensics in order to prove chains of custody and witness testimonies. As an example, evidence repositories (based on blockchain technology) are currently being deployed to timestamp and store digital media in conflict zones so that they can be used in future prosecutions. These distributed records reduce the chances of tampering, and the evidence collection and transfer are verified immortally. Besides, the use of artificial intelligence (AI) has started to be an important part of forensic investigation. Machine learning models that are trained on big data sets are able to detect anomalies in satellites, military vehicles, or even patterns of destruction that may indicate war crimes. The AI-supported accountability does not just react, but anticipates - it can recognize the possible breach of the law even before it takes place by detecting patterns in the digital surveillance feeds. Nevertheless, these technologies also present complicated legal issues of prejudice, confidentiality, and reliability of evidence. Automation of the investigative processes should therefore be accompanied with open systems of governance in order to maintain the due process.

4.2 Cybercrime and Extradition in the Digital Era

Proliferation of cybercrime is one of the most challenging to the traditional frameworks of extradition. In comparison to traditional crimes, cybercrimes have a tendency of flaunting territorial borders and can be used to commit crimes through the existence of gray areas in jurisdiction (Alizade, 2025). The ability of perpetrators to organize ransomware, data breaches,

or online frauds across countries in a matter of seconds makes it hard to consider the questions of jurisdiction, the admissibility of evidence, and the responsibility of extradition- thus underscoring the fact that states are turning to the use of mutual digital tracking systems, encrypted evidence portals, and real-time data exchange networks to resolve these issues. An example of how the international cooperation can be simplified with the help of digital infrastructures is the so-called frameworks, like the Budapest Convention on Cybercrime and the European Investigation Order (EIO). These tools empower the prosecutors and investigators to exchange electronic evidence and track transnational transfers effectively.

Nevertheless, the presence of gaps in the policies and legislation, notes the absence of harmonization in the legislation concerning data sovereignty that obstructs collaboration in the area of sharing digital evidence and extradition demands (Sekati, 2022). Numerous states remain unwilling to extradite individuals to commit cybercrimes occurring in virtual jurisdictions by claiming that digital evidence is not always admissible in their domestic jurisdiction. Also, the cases of cyber extradition are causing privacy issues, especially regarding surveillance and extraction of information in cloud servers located in other countries. The digital age therefore requires a new paradigm of accountability of cyber-sovereignty, where the rights of an accused, the interests of state and the international need of justice co-exist in a technologically meritocratic system of law. In order to close this gap, legal scholars suggest that a transnational digital warrant should be created, which is a standardized extradition request authenticated through blockchain verification and automated jurisdiction switching. These types of innovations may guarantee the standardization of the procedure and raise the level of trust between the collaborating countries.

4.3 Justice Hubs and Technological Cooperation

One of the biggest consequences of the digital transformation of justice has been the emergence of technological justice hubs, platforms that combine data analytics, digital forensics, and cross-border collaborative legal processes. The ICPA is seen as an example of this new model given that it assembles digital evidence, organizes cross-border probes, and prosecutes using data infrastructure in secure clouds. These hubs are digital nodes of international justice where states and intergovernmental organizations can share resources and intelligence in a sovereign manner over data. They are based on sophisticated encryption, distributed ledger systems, and artificial intelligence to process large amounts of evidence, including intercepted communications, open-source intelligence (OSINT) like social media postings and satellite images, an evolution of the idea of networked accountability, in which enforcement of international law is a matter of distributed digital cooperation among multiple actors.

Justice hubs also increase the levels of transparency and trust. Civil society organizations and independent journalists can also be part of the evidentiary ecosystem by providing open-access evidence archives and digital verification tools, which will make sure that crimes are recorded real-time. This form of democratizing accountability builds moral legitimacy of international prosecution of justice, especially in those territories whereby the state-led prosecutions are either weak or compromised. Nevertheless, the digital divide is also a concern with regards to the integration of the justice hubs, as the context of governance, digital transformation may

reinforce and stratify accountability, depending on resource disparities between the states involved. Richer countries having superior technical abilities can take charge of data-driven justice systems, which can marginalize other less developed jurisdictions. International cooperation is thus only achievable when there is fair access to digital justice infrastructure.

4.4 The Future of Technology in Global Accountability

With the advent of the international law in the age of algorithmic governance, technological advancement will keep pushing the precincts of responsibility. New technologies like quantum cryptography, artificial intelligence (AI) facial recognition, and decentralized autonomous legal systems (DALs) are set to improve the effectiveness and visibility of international justice, but the new technologies also endanger to widen existing power inequities, argues. In order to make innovation compliant with justice, international organizations need to implement effective ethical models of data gathering, application of AI and sharing of digital evidence. An openness in making algorithmic decisions, fair access to forensic technologies, and multilateral control on a regular basis will help ensure the integrity of digital accountability systems.

5. Legal and Ethical Challenges in Technological Enforcement

Technology and international criminal law have intersected with each other and transformed the extradition; however, they have raised new legal and ethical challenges. With the advent of artificial intelligence (AI), biometric surveillance, and data-driven decision-making as the focal point of cross-border law enforcement, states and international organizations have to face the dilemma of efficiency, transparency, and basic human rights. Although integration through technology has enhanced the strength of accountability mechanisms in the world, it is also threatening to toe the line of intensifying biased systems, weakening privacy, and compromising procedural fairness (Alizade, 2025).

One of the most urgent ethical issues is the application of AI and algorithmic profiling during extradition. Automation that attempts to measure the plausibility of digital evidence or judge the risk of flight posed by suspects can help to increase the speed of decision-making, but will also introduce opaque biases into the judicial system, jeopardizing the presumption of innocence and due process in global justice. As an example, predictive analytics that forecast extradition risks frequently use incomplete or biased information, which leads to discriminatory results when targeting the marginalized media or the political dissident groups.

There are also privacy issues of digital surveillance and data harvesting to carry out investigations. International access to cloud data and electronic communications often contradicts the legislation on data protection at the national level. Most states, such as members of the European Union, have a high privacy regime such as the General Data Protection Regulation (GDPR), which limits the transfer of personal data to jurisdictions with less effective privacy protection. In cases where the extradition requests include some digital evidence obtained with the help of intrusive surveillance or mass data collection, the courts are currently in the situation of determining how the value of such data as evidence can be weighed against the rights of individuals. Such a tension has resulted into varying judicial decisions

where there are states that have opposed extradition requests premised on the use of evidence that has been illegally obtained.

These ethical issues are complicated by the disintegration of cyberlaw systems. There are differences in the definition and regulation of digital crimes by jurisdictions and this has created legal asymmetries that hinder cooperation. As an illustration, whereas the European Union has implemented standards of harmonization of the technology by means of such conventions as the Budapest Convention on Cybercrime and the E-Evidence Regulation, other parts of the world do not have such systems to regulate technology implementation. The EU legal balance is considered to be a global example of proportionality, oversight, and accountability (Khan & Ahmed, 2025). However, in the non-EU, the unequal application of cyber jurisdiction can easily allow criminals to use the loopholes in the law by acting across several legal jurisdictions.

Moreover, the introduction of AI surveillance software, i.e., facial recognition and digital tracking, evokes the question of the overreach and totalitarian abuse of state forces. In the absence of proper protection, international cooperation can be used by governments to access such technologies on their citizenry that oppose or protest the government instead of focusing on real criminals. This risk is aggravated by the fact that there are no clear international standards of AI ethics and digital extradition procedures. As opposed to the traditional law enforcement systems that are anchored on treaty-based duties, technological enforcement exists in a grey zone that is transnational and in which misuse responsibility is untraceable and spread across the board. Finally, there is an issue of digital inequity. Digital evidence analysis and secure means of communication are technologically advanced and are concentrated in more affluent states, which creates unequal access to justice. Developing nations might not have the technical capability of authenticating digital evidences or safeguarding their citizens against illegal surveillance leading to asymmetrical extradition relations. This technological asymmetry defies the idea of equality before the law, and confirms the idea that justice in cyberspace is not distributed equally.

Technology has unquestionably resulted in the improvement of the efficiency and the scope of the international accountability of criminals but it also demands a reconsideration of the traditional legal principles. One of the problems facing policymakers and jurists is how to make innovation to not undermine justice. It is necessary to create international standards and requirements that would enable AI transparency, cross-border data regulation, and ethical supervision to protect the integrity of extradition procedures. With the technological enforcement being the unavoidable aspect of the international law, its validity will rely on the ability to retain the fragile balance between international security and individual rights.

6. Case Study: The Evolution of Digital Cooperation in Extradition

The modern world of cross-border justice is becoming more and more reliant on the mechanisms of cooperation across the borders and supported by the complex information technologies. The changing process of extradition as a piece of paper diplomacy to digitally synchronized mechanisms is an illustration of how international criminal responsibility has

followed the trend of globalization and interconnectiveness of the cyber world. Such integrated tools as the European Arrest Warrant (EAW), the I-24/7 communication network of INTERPOL, the Secure Information Exchange Network Application (SIENA) of the Europol and the Mutual Legal Assistance Treaties (MLATs) have reformulated the way states share evidence, issue warrants and coordinate arrests. Collectively, these systems have minimised bureaucratic delays, speed-up judicial operations and accountability in case of war crimes, terrorism, cybercrime and transnational corruption (Prants, 2024).

6.1 From Bilateral Treaties to Digital Ecosystems

In the past the extradition depended on bilateral treaties that were made between autonomous states. These deals were narrow in range, time consuming in implementation, and very prone to manipulation by politics. The late 20th century was marked by the transition to regional and multilateral arrangements of cooperation, the purity of which was prioritized in judicial expediency rather than in the political discretion. The European Arrest Warrant (EAW) in 2002 marked a turning point of sorts and transformed the old model of extradition in the European Union into the new model of mutual recognition of judicial decisions (Novakovic, 2025). The EAW is based on a digitally networked infrastructure where the court in one EU member can give and send the arrest warrant digitally to the other member states. This digitization has reduced the time of extradition by 20 to 30 times: A year on average with the traditional treaties versus 43 days in the instances of EAW. Moreover, it has increased the traceability and security of the extradition requests by use of digital authentication and encryption protocols. One of the first massive uses of information technology within transnational criminal law is the EAW, which has at last turned judicial cooperation into a real-time process.

6.2 INTERPOL's I-24/7 and Europol's SIENA: The Backbone of Global Extradition

In addition to regional co-operations such as the EAW, the I-24/7 network of INTERPOL is the major global communication system in extradition and exchange of criminal information. This is a safe online system that has linked law enforcement agencies in more than 190 countries, enabling the agencies to exchange notices, biometrics information, and evidence in real time. The I-24/7 framework supports the framework of the Red Notices of INTERPOL which serves the functions of quasi-international arrest warrants giving countries the right to locate and arrest suspects quickly across jurisdictions.

According to Ndubuisi (2023), incorporating I-24/7 into national police databases has made the extradition faster through establishing direct digital pipelines between national judicial systems and international policing systems (Ndubuisi, 2023). This degree of interoperability is a significant improvement on the disjointed and bureaucratic systems of the past whereby paper-based transactions could take years to bring justice. In addition to INTERPOL, SIENA platform (Secure Information Exchange Network Application) by Europol leads to improved intelligence sharing between EU member countries and countries that are partners. It facilitates encrypted communications between the law enforcers and prosecutors and financial intelligence units. SIENA has been more successful especially in cybercrime and terrorism cases, where real-time coordination and exchange of digital evidence play an important role.

Described such a dual network of INTERPOL, and Europa as the global network of international law enforcement agencies, as the so-called digital nervous system, connecting extradition operations to larger data-driven policing operations.

6.3 Mutual Legal Assistance Treaties (MLATs) and E-Evidence Systems

Whereas extradition concerns handing over of suspects, the sharing of evidence and judicial cooperation is regulated by Mutual Legal Assistance Treaties (MLATs). The traditional MLAT processes were in notorious slow speed, taking months to complete. Nevertheless, with the advent of digital platforms, specifically the E-Evidence exchange platforms and safe digital document transfer, the speed and dependability of the MLAT communications has been greatly improved. An example is the E-Evidence Platform initiated by the European Union that was to help access electronic data across borders to help in criminal investigations. This system enables the national authorities to request the providers of some other member states to provide their digital records directly to the relevant authorities without involving the diplomatic intermediaries. Abraha (2021) show that these systems have substituted physical bureaucracy with encrypted judicial interoperability, which led to a high rate of compliance and fast reaction. However, there are still difficulties. According to Alizade (2025) laws on data sovereignty, privacy laws (including the GDPR), and encryption-related obstacles continue to draw challenges to digital cooperation when investigating extradition (Alizade, 2025). The international law on data protection is usually conflicted as countries do not agree on the jurisdiction of the data stored in cloud environments. To respond to these apprehensions, the Second Additional Protocol of the Budapest Convention on Cybercrime of the Council of Europe (2022) is aimed at harmonizing the process of access to data across the borders, which is a positive step toward the unification of digital cooperation in the extradition and investigation sphere.

6.4 Case Applications: From Cybercrime to Political Extradition

There are a number of high-profile cases which demonstrate how digital cooperation has revolutionized extradition in practice. The United States v. The analysed case of United States v. Meng Wanzhou (2021) shows that digital documents and encrypted communication channels played a crucial role in organizing legal requests between Canada, the United States, and China. There was also the geopolitical complexities that digital transparency brings out in the case even though the digital systems enhanced the accuracy in the processes, it also led to the exposure of the political undertones behind extradition approvals. Conversely, the 2007 case of the Estonian cyberattack points to the possibility of the digital cooperation and its role in the overall defence and responsibility increase. Following the mass-scale cyberattacks on Estonia that were caused by foreign actors, the digital networks organized by the security agencies of I-24/7 and the EU cybercrime cooperation systems were the means that the legal investigators used to organize their reaction. The incident no extraditions were made but the incident made it possible to develop the Tallinn Manual and reinforce the international cooperation framework in cyber law.

Also, the functionality of integrated networks is demonstrated in cross-border cooperation in financial cybercrimes, like the case of Taiwan ATM hacking (2021). The researchers reported that the integration of the domestic and international agencies via the digital communication channels enabled the law enforcement to detect, locate, and extradite suspects in various jurisdictions faster than ever.

6.5 The Impact of Digital Cooperation on Impunity Reduction

The digitization of extradition and mutual legal assistance has had measurable effects on reducing impunity. By increasing the speed and reliability of transnational cooperation, these systems have closed the window of opportunity for fugitives to exploit jurisdictional loopholes. (Alizade, 2025) reports that INTERPOL-assisted extraditions have increased by over 30% in the past decade, with average processing times dropping significantly due to integrated data systems. Similarly, Europol's SIENA reports a 70% growth in cross-border case coordination between 2015 and 2023, particularly in terrorism and cybercrime. Digital tools have also improved accountability through transparency. The use of electronic audit trails ensures that every communication, request, and response in the extradition process is recorded and verifiable. This not only deters corruption and political interference but also builds trust among partner nations. Alizade (2025) note that digital recordkeeping in Indonesia's new extradition framework has enhanced the government's ability to track and enforce compliance with international obligations.

6.6 Discussion

The research and discussion in this paper shows that technology is an overbearing factor in redefining international criminal responsibility especially in the extradition scenario. In the past, extradition operated under very strict territorial lines and was heavily reliant on the good will of diplomacy and in many instances, legal imperatives were subject to political interference. As revealed in the discussion, the integration of technology has slowly undermined these traditional restrictions through bringing speed, traceability, and interoperability to the cross-border criminal justice mechanisms. Consequently, the historical distance between the normative obligation to prosecute international crimes and the actual ability to impose accountability has already started to decrease.

Among the most notable lessons gained through this study, it is necessary to mention that the digitalization has turned the extradition into a highly responsive and paper-based process and transformed it into a proactive and data-driven mechanism. Biometric identification, real time communication networks, and interoperable databases are the technologies that have increased the capability of the states in terminating fugitives and handling extradition request effectively. This change has decreased the chances of offenders taking advantage of the loopholes in jurisdictional boundaries or the delays in the process to avoid justice. Technology in this context is a structural equalizer that neutralizes the constraints of geographical distance and disjointed legal jurisdictions. Another aspect that is discussed in the context of enhancing prosecutions across the borders is the client role played by digital evidence and forensic technologies. The satellite evidence, metadata, coded messages, and evidence blockchain-

related evidence preservation have diversified the evidence base of international criminal cases. They will not only enhance the admissibility and credibility of evidence, but will also alleviate the dependence on the evidence of vulnerable witnesses, who in the past have been vulnerable to intimidation and political pressure. As a result, technology is implicated in the efficiency as well as the substantive quality and reliability of the international criminal proceedings.

Simultaneously, the discussion highlights that the emergence of cybercrime is not only a reason but also an obstacle to the extradition which has become technologically facilitated. Cybercrimes are now international and challenge the old concept of jurisdiction, attribution and sovereignty. Although digital cooperation frames and mutual legal assist platform provides feasible solutions, the lack of consistency in domestic cyber legislative frameworks and data protection frameworks impedes the smooth coordination of cooperation. This conflict has been part of the wider conflict in international law to balance state sovereignty with the borderlessness of digital crime. These discussions indicate that technology cannot completely help to eradicate impunity without the increased harmonization of cybercrime legislation and extradition requirements. A very vital aspect to this debate is ethical and legal issues. Application of artificial intelligence, predictive analytics as well as surveillance technologies in the extradition decision making raise serious concerns about due process, privacy and possible discrimination. Although automation may lead to faster decisions, it may also put opaque biases in judicial procedures, especially in cases where the algorithms are based on incomplete or biased data. It is discussed here that technological adoption which is driven by efficiency should not be conducted in a manner that may compromise basic human rights or procedural fairness because such would not enhance the effectiveness of international criminal justice but rather undermine it.

Technological inequality between states is another significant matter that is discussed. The high level of digital infrastructures is concentrated in the economically advanced countries and results in an unequal power balance in the extradition and evidence-sharing procedures. Less technologically developed states might not keep up with authenticating digital evidence, keeping citizens safe against unlawful surveillance or be part of digital justice networks. This asymmetry is dangerous in the recreation of selective justice types, in which responsibility is easier to force upon agents belonging to technologically disadvantaged jurisdictions. The discussion thus justifies that capacity-building, transfer of technology and inclusive governance processes are necessary to make sure that the digital accountability is not a privilege of the few. The debate as a whole advocate the thesis that technology has realigned the meaning of impunity within the international criminal law. Impunity is not just an effect of political denial or a legal black hole, but also of the technological inability or moral abuse. Although digital tools have enhanced the strength of extradition and cross-border accountability a great deal, their performance is eventually determined by normative alignment, legal protection and cross-border control. The paper therefore comes up to the conclusion that technology is to be viewed not as a tool of coercion per se but rather as a normative process of altering the roles and duties of the states in the new architecture of international criminal justice.

Conclusion

This paper has explored the changing nature of the role of technology in fighting impunity in international criminal law with special focus on the extradition as part of the central issues of cross-border accountability. As the analysis shows, technological innovation has radically transformed the scene in the sphere of international criminal justice, decreasing the scale of the procedure, enhancing the quality of the evidence, and facilitating the more effective collaboration between states. Biometric identification, digital evidence management systems, real-time communication networks, and AI-assisted investigations are some of the tools that have undermined the classic barriers of sovereignty and jurisdiction that one used to help serious offenders to escape justice. Concurrently, the paper highlights the fact that technology is not a panacea to impunity. Although digital systems contribute to more efficiency and traceability, they also cause complicated legal and ethical issues connected with data privacy, bias in algorithms, surveillance, and inequitable technological capacity across states. The continuation of political discretion in extradition action, along with the disjointed legislation on cybercrime and the inconsistent application of data protection policies, still prevents the full implementation of technologically facilitated accountability. These limitations indicate that impunity in the twenty-first century is not only a legal and political phenomenon but also an unequal technological regulation and access. The results indicate that the effectiveness of extradition and international criminal accountability in the future can hardly be reduced to technological advancement only. Strong international law and coordinated cyber and extradition law, ethical regulation of digital tools, and capacity-building of states with lower technological capabilities are also needed in the context of fairness and legitimacy. Finally, technology must be considered a complementary concept, that is, it reinforces, but does not eliminate normative commitment, multilateral cooperation, and respect to human rights. Under these principles, technologically enabled extradition can be a decisive factor in enhancing a more believable, fair, and sustainable system of world justice.

References

1. Abdelkarim, Y. A. (2025). UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age. *Journal of Digital Technologies and Law*, 3(4).
2. Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2), 118-153.
3. Ajayi, E. (2025). The Impediments Militating Against Thorough Investigation and Diligent Prosecution of Global Cybercrimes.
4. Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: Lessons learned from germany, sweden, finland and the netherlands. *Journal of International Criminal Justice*, 19(1), 189-211.
5. Alizade, V. (2025). Extradition in the Age of Cybercrime: Legal Dilemmas and Policy Gaps in Cross-Border Prosecution.
6. Antai, G. O., Umo, M. E., Obisesan, O. O., Ekpenisi, C., & Okpong, D. E. (2025). Jurisprudential Appraisal of the Interplay between International Law and Politics in Israel-Gaza Conflict. *NIU Journal of Humanities*, 10(1), 273-287.

7. Asghar, M. A., Ghafoor, H. A., & Matin, F. Z. A. (2025). PRINCIPLES AND MECHANISMS OF EXTRADITION IN INTERNATIONAL CRIMINAL LAW. *Modern Science and Research*, 4(4), 1768-1781.
8. Ashraf, Z. (2025). Transnational Corruption and the Role of International Criminal Law. *International Journal of Sustainable Applied Sciences*, 3(5), 295-312.
9. Banach-Gutierrez, J. B. (2023). In search of the role of punishment from the EU criminal law perspective. *Archiwum Kryminologii*, 2(XLV), 29-42.
10. Ben-Josef Hirsch, M., & Dixon, J. M. (2021). Conceptualizing and assessing norm strength in International Relations. *European Journal of International Relations*, 27(2), 521-547.
11. Costa, O., Collantes-Celador, G., & Badell, D. (2021). The dog that did not bark: the EU and the clash between sovereignty and justice in the International Criminal Court. *European security*, 30(3), 402-417.
12. Dandurand, Y., & Jahn, J. (2022). The Future of International Criminal Justice Cooperation. *The Rule of Law in Retreat: Challenges to Justice in the United Nations World*, 209.
13. Ghaeminasab, F. (2023). Examining the Dimensions of War Crimes in the Third Generation of International Criminal Courts. *J. Legal Ethical & Regul. Issues*, 27, 1.
14. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y. C., & Mejía, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context.
15. Iranzi, P. (2024). States Non Compliance With ‘Aut Dedere Aut Judicare’ On The Fugitives Of Interntional Crimes In The Context Of Genocide Against Tutsi In 1993. *Available at SSRN 5396076*.
16. Jinga, D. D., & Debebe, A. (2022). Exploring the Interface between INTERPOL National Central Bureau and Federal Police Crime Prevention Units in Ethiopia.
17. Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information*, 12(5), 181.
18. Kasera, O. A., Odhiambo, O. M., & Oloo, B. C. (2024). Africa in global public policy: Theoretical perspectives and the role of international law in shaping public policy in Africa. *International Journal of Research and Innovation in Social Science*, 51, 910-937.
19. Khan, M. N. I., & Ahmed, I. (2025). A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence. *International Journal of Scientific Interdisciplinary Research*, 5(2), 01-29.
20. Ndubuisi, A. F. (2022). Cross-border jurisdiction challenges in prosecuting cybercrime syndicates targeting national financial and electoral systems. *International Journal of Engineering Technology Research & Management (IJETRM)*, 6(11), 243-261.
21. Novakovic, F. (2025). Harmonizing Justice: Unraveling the Complexities of the European Arrest Warrant in the Pursuit of Cross-Border Security and Human Rights Protection. *Ind. Int'l & Compar. L. Rev.*, 35, 411.
22. Oyewole, O. O. (2024). An analysis of the legitimacy of international criminal tribunals. *RUNJJIL*, 4, 1.
23. Pataraiia, D. (2021). *International law: text, cases and materials*. Routledge.
24. Pettersen, C. L. (2023). *The Empire of Law: Hybrid Justice and the International Commission Against Impunity in Guatemala* (Doctoral dissertation, University of Georgia).
25. Prants, E. (2024). *Enhancing Cross-border Collaboration in Combatting Child Sexual Abuse: A Study on Europol's Role and the Dynamics of Information Sharing among the European Union Member States* (Master's thesis).

26. Racoveanu, C. (2024). Artificial Intelligence—A Double-Edged Sword. Organized Crimes AI vs Law Enforcements AI. In *Proc. Int. Conf. Bus. Excell* (Vol. 18, pp. 507-517).
27. Rehman, Z. (2023). Beyond borders: International law and global governance in the digital age. *Journal of Accounting & Business Archive Review*, 1(1), 1-12.
28. Sadat, L. N. (2022). The International Criminal Law of the Future. *International Legal Order Unraveling*.
29. Sair, S. K. (2024). Law of Extradition: Synopsis of its Basic Principles, Applications, and Challenges. *Applications, and Challenges (June 06, 2024)*.
30. Sekati, P. (2022). Assessing the effectiveness of extradition and the enforcement of extra-territorial jurisdiction in addressing trans-national cybercrimes. *The Comparative and International Law Journal of Southern Africa*, 55(1), 1-36.
31. Thierry, M. B., & Fred, K. (2024). The Use of Forensic Evidences in Investigations and Prosecution in International Criminal Proceedings. Case Study of International Criminal Court (ICC). *International Journal of Forensic Sciences*, 9(2), 1-18.
32. Yonhsheng, G., Hum, I. M., & Fensh, W. (2023). An in-Depth Examination of the Progress and Obstacles in the Field of International Criminal Law. *J. Legal Ethical & Regul. Isses*, 27, 1.
33. Zakir, M. H., Begum, M., Rahman, A., Bilal, M., Tayyab, A., & Khan, S. (2024). The role of international criminal law in addressing war crimes and crimes against humanity. *Kurdish Studies*, 12(4), 535-543.