UCP Journal *of* Law & Legal Education
Vol. 4, Issue 1 (January – June 2026)

Cybersecurity and Human Rights: Balancing Privacy with Law Enforcement Needs in Cross-Border Investigations

Muhammad Saleem Javed

Abstract

The increasing transnational nature of cybercrime and the widespread use of cloud-based technologies have made cross-border access to digital evidence essential for effective law enforcement. At the same time, such access raises significant concerns regarding privacy, due process, freedom of expression, state sovereignty, and other fundamental human rights. This study examines the legal and ethical challenges arising from the interaction between cybersecurity enforcement and human rights in cross-border investigations. It adopts doctrinal methodology, examining international and domestic legal frameworks, relevant judicial decisions, and scholarly literature. Particular attention is given to the Budapest Convention on Cybercrime, the Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence, the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act, and the European Union's General Data Protection Regulation (GDPR), together with developments in judicial jurisprudence concerning digital privacy, surveillance, and governmental access to electronic information. The study finds that existing frameworks have facilitated international cooperation but remain fragmented because of differences in jurisdiction, sovereignty, data-protection standards, and procedural safeguards. It further identifies risks associated with excessive or insufficiently supervised access to digital information, particularly in relation to necessity, proportionality, transparency, accountability, and effective remedies. The study argues for a human rights-based approach to cross-border cybersecurity enforcement, supported by clearer jurisdictional rules, stronger international cooperation, appropriate procedural safeguards, independent oversight, and accountable use of emerging technologies. Such an approach can facilitate legitimate law-enforcement access to digital evidence

* Lawyer, Junior Partner, Sukhera Law Chamber, Lahore, Pakistan email: m.saleemjaved001@gmail.com

Article History: Received: 05-05-2025; Received in revised form: 03-10-2026; Accepted: 05-10-2026.
Available online:26-10-2026
DOI: https://doi.org/10.24312/ucp-jlle.04.01.532

CC BY OPEN ACCESS — OPEN ACCESS

while protecting fundamental rights in an increasingly interconnected digital environment.

Keywords: Cybersecurity; Human Rights, Privacy, Cross-Border Investigations, Digital Evidence, Law Enforcement.

Introduction

Digital technology has revolutionised how we define crime and how law-enforcement communities investigate and prevent it (Rahman, 2021). Cybercrime is now a multi-jurisdictional activity, and perpetrators, victims, service providers and evidence of a crime may all be present in different States at the same time. This has been exacerbated by the rise of cloud computing, which allows data to be stored, processed and transferred to various servers and jurisdictions, despite the continued use of the traditional territorial concept of criminal investigation (Koops & Goodwin, 2014). Electronic evidence outside of law enforcement's control may therefore be needed, and the persons who are the subject of that evidence may have different rights to protection of privacy, due process and other fundamental rights (Laidlaw, 2021). This is where the basic conflict between effective cybersecurity enforcement and human-rights protection comes in. States have an interest in protecting against cybercrime, terrorism, fraud, and other serious crime, in which digital evidence could play a key role in investigation and prosecution (Rahman, 2021). But access to personal information across borders could impact privacy, freedom of expression, due process and effective legal remedy. The question before the States, therefore, is not just whether it is possible for them to obtain electronic evidence, but also the conditions under which this can take place, and the protections that have to be put in place to prevent any unjustified or disproportionate infringement on fundamental rights.

There is a patchwork of international and domestic laws, which show this competing interest. International cooperation is supported by the Budapest Convention on Cybercrime, and international challenges such as the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018 aim to overcome practical problems with accessing electronic data stored by service providers in different countries. Meanwhile, data protection policies

like the General Data Protection Regulation (GDPR) in the European Union impose substantive and procedural restrictions on processing and transferring personal data. The Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence adopted in 2022 builds upon the Budapest framework by outlining more efficient ways to access electronic evidence, such as direct cooperation with service providers, disclosure of evidence in an emergency, the registration information of domain names, and enhanced mutual-assistance procedures, as well as incorporating measures for data protection and human rights (Pangrazio & Sefton-Green, 2021). The developments suggest the ongoing attempts to balance the demands of cross-border investigations with privacy, due process and State sovereignty. This relationship is made more complex by the advances of technology. While encryption, the use of large-scale surveillance systems, AI, predictive policing, and biometric technologies have the potential to improve States' capacity to investigate and prevent cyber threats, there are also concerns about their necessity, proportionality, discrimination, transparency, and accountability (Laidlaw, 2021). In particular, increased State access to information in digital form may pose serious threats if surveillance takes place without proper authorisation and if those subject to it have no meaningful means to contest unlawful surveillance.

While scholarship in cybersecurity, privacy in the digital world, surveillance and international cooperation has grown significantly, these fields are often addressed individually. Research on what works in cybercrime tends to be more on the investigative side and more on the international side, whereas research on digital rights is more on the side of privacy and data-protection safeguards. This fragmentation has left the link between the mechanisms for the production of electronic evidence across borders and the principles of human rights that govern the exercise of such powers inadequately explored. The collection, processing and exchange of digital evidence is therefore in need of a more holistic analysis in accordance with common legal standards. This study therefore explores how the enforcement of cybersecurity law relates to human rights in the context of cross-border investigations by considering both the law and practice surrounding the cross-border access to electronic evidence and the ability of the current frameworks to support effective cooperation in cross-border investigations while

maintaining the protection of individuals' rights. The Budapest Convention and its Second Additional Protocol, the United States CLOUD Act and the GDPR are explored in conjunction with some judicial and contemporary developments on surveillance, digital privacy, and State access to information.

The study on cross-border investigative powers uses a rights-based analysis with the criteria of legality, legitimate aim, necessity, proportionality, independent oversight, transparency, accountability and effective remedy as a common ground for this assessment. These principles are not just general normative aspirations, but criteria for analysis (Laidlaw, 2021). The conditions of Legality are that interference with privacy and other protected rights is based on a clear and accessible legal basis, that there is a legitimate aim for the interference, and that it is actually necessary and that there are no less intrusive means available to achieve the legitimate aim (Laidlaw, 2021). The condition of Legitimate Aim is that the interference must serve a recognised law-enforcement, public-security or other lawful objective. The condition of Necessity is that the interference must be ‘genuinely required' and that there are no less intrusive measures available. The condition of Proportionality requires that the extent and intensity of the interference are proportionate to the objective pursued (Shany, 2022). Independent oversight, transparency, accountability and effective remedies are also explored to see if people have meaningful access to their information and protection from arbitrary or excessive access. This is a framework to facilitate comparison of the Budapest Convention, its Second Additional Protocol, the CLOUD Act, the GDPR, and existing judicial decisions. The study will address three research questions: What are the provisions of the Budapest Convention, its Second Additional Protocol, the US CLOUD Act and the GDPR on cross-border access to electronic evidence, and what human-rights safeguards do they offer? What jurisdictional, procedural, and human rights issues are created by cross-border access to electronic evidence, in the context of privacy, surveillance, due process, and State sovereignty? How to organise cross-border investigative mechanisms to ensure their effectiveness, in compliance with the principles of legality, necessity, proportionality, independent oversight and effective remedy?

Research Methodology

This study uses a qualitative, analytical and doctrinal legal research method to analyse the cross-border accessibility of electronic evidence for law enforcement purposes and the interplay with respect to the right to privacy and other fundamental rights. The research is mainly based on legal texts and judicial decisions, instead of empirical data. The primary sources are the Budapest Convention on Cybercrime, the Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence, the United States CLOUD Act 2018, the General Data Protection Regulation (GDPR), provisions of international human-rights law, and judicial rulings of the Court of Justice of the European Union (CJEU), the European Court of Human Rights (ECtHR), and the Supreme Court of the United States. Secondary sources include peer-reviewed academic journal articles, legal scholarship, institutional reports, and authoritative commentary on cybersecurity, electronic evidence, cross-border investigations, and digital privacy.

In this study, comparative legal synthesis is used to pinpoint the points of convergence and divergence between the legal frameworks selected. The methodology does not require that cybersecurity enforcement and human-rights protection be mutually exclusive, but looks at the circumstances in which cross-border access to electronic evidence may be made without impinging on privacy, due process, proportionality, accountability, and the sovereignty of other jurisdictions. This way, the study can evaluate not just the formal investigative powers at States' disposal, but also the procedural and substantive safeguards that would allow or bar States from exercising those powers in a manner consistent with fundamental rights. The methodology thus enables an overall evaluation of how investigative efficiency, cross-border cooperation, State sovereignty and rights protection interact in the current electronic-evidence regimes.

Literature Review

Because criminal investigations are multi-jurisdictional and electronic evidence is stored across multiple jurisdictions, scholarship has identified three issues facing law enforcement. These issues are related: jurisdictional uncertainty, the many faces

of electronic evidence, and the fragmentation of international and domestic regimes governing cross-border data access. Previous research indicates that there is no single solution to these concerns in the law. Instead, the success and legitimacy of cross-border investigations rely on the interplay of the various procedural cooperation tools, domestic investigative powers, data-protection frameworks and human rights protection. This is especially relevant when discussing cloud computing and data that could be stored, moved and processed in several jurisdictions at once. Koops & Goodwin (2014) draw attention to the fact that cloud technologies are undermining traditional concepts of territoriality and sovereignty, especially when the physical place of information is hard to pinpoint or when information is spread across multiple jurisdictions. These challenges are further complicated by the fact that cybercrime is a transnational phenomenon. According to Rahman (2021), jurisdictional issues, international legal disparities, and insufficient international cooperation are among the key challenges in cross-border investigations. Different procedures may be used for obtaining, producing and admitting electronic evidence and cooperation may be delayed or denied if the conduct in question is not criminalised in the requested State. These differences can hinder investigations and can even result in jurisdictional gaps that can be exploited by perpetrators. This distinction between the physicality of data and the legal rights to access it can be found in the literature as well: while the practical power of territorial location has been diminished by cloud computing, the legal weight of sovereignty remains (Shany, 2022). The question of whether electronic evidence is admissible or can be accessed across the border is not only whether it can be accessed across the border, but which jurisdiction should authorise it, what legal standards should be applied to the request, and what safeguards and remedies should be provided for those affected.

A second line of scholarly work is focused on the balancing of investigative needs of law enforcement with privacy and other fundamental rights. While access to digital information is vital to investigating cybercrime and other serious crimes, collecting, storing, transferring, and analysing personal data may also demean, infringe on, or disrupt privacy, due process, and freedom of expression. International data transfers can raise conflicts among rights and duties to respect privacy, the protection of data, and data

governance, especially when the information sought is stored at a service provider's site or in another State. The prevention and investigation of crime is a valid aim, while access to personal information, if unrestricted or inadequately monitored, might lead to an undue infringement upon the rights of the individual. Algorithmic systems can perpetuate existing biases or generate discriminatory results, and biometric and other surveillance through technological devices can provide levels of access to personal information that have never been thought of before. The literature thus continues to pose the question of how to enable the legal right to investigate while maintaining the wider security and rights-sustaining purpose of the digital environment (Pangrazio & Sefton-Green, 2021).

These issues have also influenced the evolution of international and domestic processes in relation to electronic evidence for cross-border access. The Budapest Convention on Cybercrime is a major contribution to the development of a set of shared values, processes and cooperation methods to fight cybercrime internationally. However, scholarship is still developing on issues of conflict between national laws, investigative jurisdiction over data located overseas, and the ongoing lack of certainty with regard to jurisdiction over electronically stored information. For instance, Ruohonen (2023) discusses the issue of cross-border access to data by law-enforcement authorities and the ongoing struggle between access to data, State sovereignty, privacy and international cooperation. Notably, these mechanisms are underpinned by human rights, the rule of law and data protection. It shows a step toward the evolution of the practice of mutual legal assistance from a limited to a more flexible approach to the cross-border collection of evidence.

Data protection systems are another aspect of this discussion. The GDPR is a rights-driven approach to the processing and sharing of personal data and emphasises safeguarding individuals from unfair or illegal interference with their personal information (Ruohonen, 2023). But national variations in data-protection frameworks and law-enforcement capabilities can create friction when personal data is sought or sent in cross-border investigations. This varied regulatory landscape takes on added importance when it comes to data flowing across jurisdictions that have different privacy-protection and investigative powers and

jurisdictions. The case law of the Court of Justice of the European Union (CJEU) has thus far been crucial to the construction of the bond between transfer of personal data, access by States and fundamental rights. In Schrems v. Data Protection Commissioner 2015, known as Schrems I, the CJEU addressed the transfer of personal data from the European Union and the protection offered in the destination country. It builds on this approach in Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18), also referred to as Schrems II, in which the Court discussed how EU fundamental rights are respected when data transfers are made internationally, and the impact of public authorities accessing transferred data in the receiving State.

The literature shows that cross-border cybercrime investigations are conducted in a disjointed mix of international cooperation mechanisms, domestic investigative tools, data protection regimes, and human rights protection frameworks. The scholarship on jurisdiction focuses on the challenges of applying the concept of territory to electronic evidence, and the scholarship on privacy and data protection underscores the dangers of a broad territorial reach by the State into personal information.

Legal Frameworks Governing Cross-Border Cybercrime Investigations

The legal systems governing cross-border investigations of cybercrime are the product of a tension between international cooperation, domestic investigative powers, data protection, and State sovereignty (Casino et al., 2022). The main problem is that the traditional territorial basis of criminal jurisdiction is becoming less stable as digital information is created, processed and stored within a single jurisdiction, but also across several countries at the same time. This creates some basic questions about the question: which State has a right to seek, to obtain, or to force disclosure of electronic evidence? There are three relevant frameworks to this debate: Budapest Convention; the United States (CLOUD) Act 2018; and the European Union's General Data Protection Regulation (GDPR). While these instruments have different goals, they show how these goals are still in constant tension with one another, particularly with respect to the need for efficient law enforcement, international co-operation, data protection and State sovereignty.

The Budapest Convention offers a valuable procedural framework for international cooperation on cybercrime investigations. It aims to align substantive and procedural cybercrime laws, as well as to promote cooperation among the States Parties, in securing the preservation of data, production orders, search and seizure of stored computer data, and other varieties of international assistance (Ruohonen, 2023). The importance of their role in cross-border investigations is that it acknowledges that international cooperation is necessary to respond to cybercrime, especially in the context of volatile electronic evidence and the limitations of standard mutual legal assistance agreements (Convention on Cybercrime, 2001). Accordingly, the exercise of personal rights within the scope of the Convention shall be subject to safeguards against arbitrary or disproportionate interference, such as the establishment of a clear legal basis, a legitimate purpose, necessity, proportionality, independent or judicial supervision and effective remedies. The Convention is thus a compromise between territorial sovereignty and the need to obtain digital evidence in a timely fashion.

The Second Additional Protocol to the Budapest Convention builds on this concept in the face of the ever-changing and diffuse or indeterminate location of electronic evidence. It provides new tools for cross-border cooperation, such as direct cooperation with service providers and registrars, improved tools for obtaining subscriber data and traffic data, emergency cooperation and other fast-track cooperation tools. It is important because of its ability to mitigate a major drawback of the traditional mutual legal assistance model: investigations involving electronic evidence that quickly disappears, shifts or may become inaccessible. The Protocol aims to enhance investigative efficiency while at the same time preserving human rights, rule-of-law and data-protection (Second Additional Protocol to the Convention on Cybercrime, 2022). But increased access does not automatically imply the lawfulness and proportionality of the investigative measure concerned The U.S. CLOUD Act, 2018 takes a different route, offering domestic legal tools to give the United States government the power to compel covered service providers (under its jurisdiction) to provide electronic information, including information located outside the United States. The Act also provides a framework for executive agreements concerning some types of transborder access to

electronic evidence. Its angle takes account of the reality of the physical separation of data from the user, which cloud computing has brought about, and explores the issue of authority and service providers. The CLOUD Act aims to minimise delays caused by conventional cross-border evidence requests by focusing not solely on the physical location of the relevant server, but rather on the provider's legal control over the data. Meanwhile, its extraterritorial nature poses questions about the sovereignty of the State where the data is being held and what rights individuals have if the disclosure happens. The tension between unilateral domestic measures to obtain electronic evidence and the principles of international comity, territorial sovereignty and human rights protection is, therefore, illustrated in the Act.

The constitutional framework of government access to provider-held information will also help clarify the analysis of the CLOUD Act. The third-party doctrine was established in the U.S. Supreme Court cases of United States v. Miller (1976), and Smith v. Maryland(1979), concerning the disclosure of information to financial and telecommunications companies. This old-fashioned method of understanding the Fourth Amendment was then revived in Carpenter v. United States(2018), in which the Court determined that the government's acquisition of historical cell-site location information constituted a Fourth Amendment search, and that the information was particularly revealing. Carpenter is relevant because information possessed by service providers can provide a great deal of information on the individual's movements, communications and private life. The legal aspects of access across borders should therefore be more than efficient; they should also be defined by clear and precise legal rules, effective control and protection against over-collection or indiscriminate use, especially when access is sought by individuals outside the country where the investigation takes place, and they may have fewer chances to contest such use by the State.

As for the GDPR, it offers a legal approach that prioritises data privacy and individual rights in data governance. It creates rules on how personal data can be processed and passed on, such as lawfulness, purpose limitation, data minimisation, transparency, security and accountability (Charter of Fundamental Rights of the European Union, 2012). While the GDPR is not a cybercrime treaty, it has a clear link to investigations involving cross-border requests

for data by Law Enforcement and data transfers. GDPR is not a cybercrime treaty but has a clear link with cross-border requests for data by Law Enforcement and data transfers where personal data is involved and protected under European data-protection law. The legal challenge is thus to enable legitimate access to information by law enforcement across the border, without the possibility of circumvention of the applicable data protection standards through cooperation between authorities (Directive (EU) 2016/680, 2016).

The Budapest Convention, Second Additional Protocol, CLOUD Act and GDPR are three separate, but related, attempts at regulating the transfer of electronic evidence across borders. The Budapest framework focuses on the importance of international cooperation and on harmonising procedures; the CLOUD Act focuses on how to get access to data held by providers across jurisdictions without relying on foreign law; the GDPR focuses on the protection of personal data and the rights of individuals. In this way, cybersecurity enforcement and human-rights protection do not have to be mutually exclusive goals; there should be a legal framework that defines the circumstances in which it is possible to have privacy, due process, proportionality, accountability,and respect for State sovereignty along with effective access to electronic evidence (United Nations, 2024).

CJEU Jurisprudence and Cross-Border Data Protection

The Court of Justice of the European Union (CJEU) offers a valuable judicial component to cross-border data transfers and State access to electronic information. Schrems v. Data Protection Commissioner (Case C-362/14) – commonly known as Schrems I – related to the transfer of personal data from the European Union to the United States and the level of protection provided in the receiving jurisdiction. The case established the link between international transfers and the fundamental rights guaranteed by Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and showed that the presence of a formal transfer mechanism is not sufficient to justify transferring personal data, where the legal system of the recipient does not offer an adequate level of protection. Thus, the relevance of Schrems I goes beyond the added value the Court could derive from a specific transfer mechanism: the assessment of the legitimacy of the transfer will still

be a matter of legal protection after the data has left the EU (*Schrems v. Data Protection Commissioner*, 2015).

This was further refined in *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (2020),* also referred to as Schrems II. It reviewed the consistency of mechanisms to transfer personal data to third countries with EU fundamental-rights needs, such as standard contractual clauses and the EU-US Privacy Shield, and the consequences of access by public authorities in the recipient country. It highlighted the importance of determining the degree of protection in the recipient jurisdiction, including whether any part of the government is likely to intervene for national security or other public reasons in the jurisdiction of the data recipient. Schrems II thus emphasises the need for robust safeguards and remedies in the event of the transfer of personal data from one jurisdiction to another. Schrems I and Schrems II, when taken together, prove that the efficiency or existence of international cooperation mechanisms cannot be considered as the basis for cross-border data governance. When assessing the legitimacy of cross-border data transfers, the level of protection in the receiving jurisdiction, possibility for public authorities' access, and effectiveness of remedies are key (*Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems,* 2020). This jurisprudence, therefore, offers a helpful judicial precedent for assessing four key principles across the borders: legality, necessity, proportionality, oversight and effective remedy.

The CJEU's reasoning in Tele2 Sverige AB v. Post-och telestyrelsen () continues to reinforce the role of necessity and proportionality when it comes to State access to communications data. The judgment addressed the retention and access to communications data, and made it clear that there is no justification for interfering with privacy or data-protection rights other than the general need to combat serious crime. Instead, the nature and extent of the data that is involved, the nature and duration of the interference, and the protections afforded to access should be considered in deciding on the justification for interference (*Tele2 Sverige AB v. Post- och telestyrelsen,* 2016).

All three cases (Schrems I, Schrems II and Tele2 Sverige) offer judicial support and substance to the rights-based principles that are analysed in this study. The value of their application is that they serve as evidence that cross-border access to digital

information is not subject to a single criterion: that is, whether or not authorities have a formal investigative power or whether the investigation is for a legitimate purpose. The jurisprudence thus supports an integrated approach, in which the authority of investigation is looked at together with the substantive and procedural safeguards and restraints for its exercise.

European Court of Human Rights Jurisprudence on Surveillance and Privacy

The jurisprudence of the European Court of Human Rights (ECtHR) offers valuable guidance on the conditions for the compatibility of State surveillance and interception of communications with the right to privacy, enshrined in Article 8 of the European Convention on Human Rights (ECHR). The jurisprudence is applicable to cross-border cyber investigations because investigative authorities might be able to access, analyse, and share communications and other personal data in other jurisdictions.

Roman Zakharov v. Russia (2015) was heard by the Grand Chamber, which considered a system of secret interception of mobile communications. The Court highlighted the need for safeguards that can prevent arbitrary or abusive surveillance. The case highlights the need for sufficient statutory provisions concerning the circumstances, scope and supervision of surveillance measures, in addition to the existence of statutory authority for surveillance. It is relevant to cross-border investigations because of the importance of establishing clear legal limits where it is possible for someone to have very limited awareness and opportunity to contest secret access to his communications (*Roman Zakharov v. Russia*, 2015).

In the case of Szabó and Vissy v. Hungary (2016), the Court examined a law which allows for secret surveillance for the national security of Hungary. The judgment emphasised the need for appropriate safeguards and for powers of intrusive surveillance to be subject to independent control. The case is also significant for cross-border investigations, as secret investigative techniques can have significant implications for privacy while curtailing the rights to contest the collection and use of information of those impacted. When surveillance is done without notice, independent

authorisation and supervision become more significant. (*Szabó and Vissy v. Hungary*, 2016).

The Grand Chamber in Big Brother Watch and Others v. the United Kingdom (2021) discussed bulk interception of communications and the sharing of intelligence. The Court reviewed protections that are in effect throughout the surveillance process, including authorisation, choosing the surveillance, examination and use of intercepted material. The case is of particular significance to digital investigations as it illustrates the need for a security mechanism to not just be implemented when data is first collected but also to be in place when accessing, examining, retaining and using information in the future (*Big Brother Watch and Others v. the United Kingdom*, 2021).

The Court in Centrum för Rättvisa v. Sweden considered a system of bulk signals intelligence and the protection of secret surveillance. The judgment highlights the need to look at the entire legal framework of surveillance, particularly the way it has been authorised, supervised and safeguarded against misuse. Its importance to cross-border cybersecurity investigations is due to the potential for digital communications to be collected or processed on intelligence or investigative systems across multiple jurisdictions (*Centrum för Rättvisa v. Sweden*, 2021).

All these cases illustrate that privacy protection during surveillance goes beyond a formal legal authorisation. Key elements in considering compatibility with fundamental rights of intrusive investigative powers are clear, well-defined legal rules, independent oversight, necessity, proportionality and safeguards against abuse. The ECHR jurisprudence thus offers a practical and clear judicial foundation for the application of the human rights approach used in this study to cross-border access to electronic evidence (European Parliament & Council of the European Union, 2016).

Comparative Legal Analysis Through the Human-Rights Framework

The comparative analysis shows that the Budapest Convention and its Second Additional Protocol have different institutional and legal approaches to cross-border electronic evidence compared to the CLOUD Act 2018 and the GDPR approach. The Budapest framework is mainly about international

cooperation for criminal-law purposes; the Second Additional Protocol introduces more direct and prompt procedures for the acquisition of electronic evidence; the CLOUD Act introduces obligations on data processing regarding data located in the possession of providers subject to the jurisdiction of the United States; and GDPR introduces conditions on the processing and transfer of personal data abroad. The various orientations offer opportunities for cooperation, as well as possible conflicts, between investigative authority and data protection and State sovereignty. The Second Additional Protocol acknowledges the practical challenge of finding electronic evidence in different, remote, evolving or unknown jurisdictions while maintaining human rights and data protection protections.

The first common requirement upon which this study evaluated the legality of cross-border access to electronic data/evidence by law-enforcement authorities is when measured in the scale of the analytical framework. Any access to foreign data for investigative purposes should be based on a clear and explicit legal basis and in a limited and defined procedure. Necessity constitutes the second requirement. Investigative authorities have to make a bona fide link between the information requested and the legitimate investigative purpose. Proportionality is another ground for considering the relation between investigative aims and the protection of individual rights (Ruohonen, 2023). Thus, CJEU and ECHR case law offers a significant counterweight to the "efficiency-based" goal of achieving rapid access to electronic evidence. Independent oversight and effective remedy are other safeguards. An investigation that crosses the border can lead to accountability gaps because the requesting State may have different laws than the State in which a provider is operating and the State where an affected individual is located.

The comparison thus indicates that the lack of international cooperation mechanisms is not the only challenge. Instead, the issue at hand is the simultaneous presence of different legal regimes which impose different procedural obligations and rights protection on the same digital information. A cooperative system for cross-border investigations must therefore be based on a sustainable cooperation system, which will enhance the accessibility of electronic evidence while continuing to guarantee minimum

standards in terms of lawfulness, necessity, proportionality, supervision, accountability and redress.

Challenges and Criticisms in Balancing Cybersecurity and Human Rights in Cross-Border Investigations

. Regulating cross-border cybercrime investigations is a legal puzzle because the success of cybersecurity enforcement often hinges on the availability of information, cross-border cooperation, and the application of new investigative tools (Casino et al., 2022). Meanwhile, the growth of government authority over these areas could also have a negative impact on privacy, due process, freedom of expression, and other basic rights. The key issue is thus how to create mechanisms to respond to transnational cybercrime while not allowing the exceptional nature of digital threats to be used as an excuse for disproportionate state action (Pangrazio & Sefton-Green, 2021).

A major obstacle is the ***lack of jurisdiction over electronic evidence***. The territorial location of electronic information may be undefined or undeterminable, as opposed to physical evidence (Casino et al., 2022). Data can be created in one country, managed by a company in another, and stored or processed via servers in multiple jurisdictions. As a result, multiple states may have a valid legal interest in the same information. This jurisdictional complexity may lead to confusion about which state's laws are applicable to the collection, disclosure, transfer, and use of digital evidence. Investigating authorities may want to access information as quickly as possible, especially when information is at risk of being deleted or altered; and the territorial state might consider the unilateral access as infringing on its sovereignty (Shany, 2022). Such disputes may stall investigations and introduce a degree of uncertainty into the legal landscape for service providers and impacted people (United Nations Office on Drugs and Crime, n.d.).

The ***Data Protection Standards (DPS)*** are divergent in nature. Another big hurdle is the gap between national and regional data protection systems. The level of privacy, personal data and procedural rights protection is highly variable across states. The information that is lawfully obtained by law enforcement in one jurisdiction may be more tightly regulated in another jurisdiction (Ruohonen, 2023). Such differences may lead to conflicts in the

transfer of personal data across borders for investigative purposes. There may be differences in legal requirements, political interests, national security concerns, or concerns about what will happen to the information after it is shared. This leads to states' reluctance to share information (Pangrazio & Sefton-Green, 2021).

The ***traditional mutual legal assistance arrangements have been criticised*** as being slow and cumbersome, especially in the context of investigations involving the rapid evolution of digital evidence. However, any attempts to speed up cooperation should be done in accordance with the basic principles of law. Access to data within another state's jurisdiction cannot be based on efficiency (Ruohonen, 2023). To achieve sustainability, there must be processes that facilitate timely cooperation with transparency and accountability. International mechanisms should therefore aim to minimise unwarranted delays without doing away with judicial safeguards or diminishing the capacity of individuals to contest unlawful interference with their rights (Wired, 2025).

The ***expansion of surveillance powers*** is accompanied by a loss of privacy. As surveillance powers increase, privacy decreases. Access to extensive electronic information is a key component of cybersecurity investigations. Digital data such as metadata, communications records, cloud storage, location data, and more can be important evidence in criminal investigations. But the information that is available also poses a danger of excessive investigatory capacity. One of the basic issues is the risk of over- or under-surveillance. Any measures that affect fundamental rights must be kept to a minimum for the purpose of the investigation, and the amount of information gathered should be commensurate with the severity of the suspected offence (UNODC, n.d.).

One of the key issues when it comes to ***cybersecurity and law enforcement is encryption.*** Strong encryption keeps individuals, businesses, governments and critical infrastructure safe from unauthorised access and threats. Meanwhile, law enforcement could find it challenging if the relevant evidence is stored in encrypted devices or communications. The issue of lawful access is especially sensitive, as any steps taken to enable the government to access information could also leave the public at large more vulnerable to cyber threats. Weakening encryption, whether done intentionally or by accident, could have consequences for not only for criminal suspects but also for ordinary citizens who rely on

secure communications for their personal and professional lives (Pangrazio & Sefton-Green, 2021). Accordingly, attempts to enable legal access to investigate should be carefully evaluated to prevent harm to the security of digital systems in general.

The ***use of Artificial Intelligence (AI), biometric identification, predictive analytical systems*** and other new technologies is growing, which adds to the problems in the field of cyber security from a cross-border perspective. The tools can enhance the capacity of authorities to detect threats and analyse large amounts of digital data. They can also expand the scope and invasiveness of surveillance. Automated systems have the potential to impact individuals in ways that are hard to understand and/or hard to challenge, especially when the operation of an algorithm is not made transparent. There are also concerns about false-positive results, inequitable results and over-reliance on automated decision-making (Casino et al., 2022). This multi-jurisdictional and multi-stakeholder nature of the collection, processing or analysis of information raises issues of jurisdiction and accountability, even more so due to the cross-border use of such technologies. Regulation, therefore, must make sure that technological innovation does not move faster than the laws needed to regulate it.

From a human-rights perspective, the central issue is therefore not the technological capability of AI itself, but the conditions under which automated investigative tools are deployed. The legality and proportionality of data collection, the quality and provenance of training data, human oversight of consequential decisions, transparency concerning automated processes and access to effective remedies should be considered when AI is used in cross-border investigations. Human decision-makers should remain accountable for investigative measures that significantly affect individuals rather than treating algorithmic outputs as independently determinative.

The Role of Emerging Technologies in Cybersecurity and Privacy

Yet at the same time, the evolution of digital technologies poses opportunities and challenges for cybersecurity and privacy protection. The more AI, blockchain, and quantum computing are developed and integrated into law enforcement agencies' operations,

the more ethical and legal issues arise with their use in cybersecurity investigations (Biasiotti, Turchi, & Quintarelli, 2022. Using predictive policing systems driven by AI, vast amounts of data are analysed to detect potential criminal behaviour. These systems may help boost law enforcement efficiency, but also bring concerns regarding bias, accuracy, and due process. Studies have shown that AI algorithms trained using biased data may foster continuing discriminatory practice in policing (Biasiotti, Turchi, & Quintarelli, 2022). For example, facial recognition systems have been criticised for disproportionate misidentification of ethnic minorities, leading to wrongful arrests (Hill et al., 2022). The European Parliament has proposed stringent regulations on AI in law enforcement to prevent their misuse, and still many countries have begun to implement these technologies in their law enforcement and investigations without sufficient oversight (Biasiotti, Turchi, & Quintarelli, 2022).

Blockchain has the promise of being decentralised and immutable, and it would have hundreds of solutions in cybersecurity. Law enforcement faces disadvantageous situations when it seeks to access digital evidence (Pangrazio & Sefton-Green, 2021). More and more organised criminal groups are beginning to use blockchain-based crime platforms due to the difficulty authorities have in tracing those who commit crimes (Koops & Goodwin, 2014). On the other hand, blockchain has the potential to empower individuals through increased sovereignty over their data. The ability to control personal data through decentralised identity systems would pave the way for challenging traditional state surveillance mechanisms and thus require reconsideration of law enforcement practices.

Artificial quantum computing will have an opposing effect on some existing encryption mechanisms. While encryption currently plays an indispensable role in safeguarding digital communication, quantum computing may jeopardise most used cryptographic methods (CISA, 2022). This poses a paradox in that quantum computing could help enhance some of the realms of cybersecurity, while in other instances, it could assist in orchestrating fresh cyber-attacks. Governments and private enterprises around the world are investing in quantum-resistant encryption; however, there is an absence of an international regulatory framework to supervise quantum computing in the enforcement of cybersecurity. This absence, in itself, raises the

prospect of state actors misusing quantum technologies for mass surveillance.

The proliferation of biometric surveillance, including facial recognition and fingerprint analysis, presents new challenges for privacy entitlements. The usage of biometric evidence to enhance crime investigation has become more prevalent, but this has also been linked to egregious violations of privacy (Shany, 2022). Cheap-level mass biometric surveillance in China has enabled the scrutiny of ethnic minorities, stirring international resentment (Ruohonen, 2023). While the erroneous use of biometric data in public domains is now proposed to be restrained within the European Union, diversity of attitude for current regulation implementation continues among its member states.

Emerging technologies thus represent a double-edged sword for the enforcement of cybersecurity. While AI, blockchain, and quantum computing offer unprecedented approaches for digital security, they come with ethical and legal quandaries. Balancing the advancement of technologies and protection of human rights needs to be a concerted effort between governments, technology companies, and civil society. There should be increased supervisory structures and ethical norms to guarantee that in this digital era, cybersecurity initiatives shall not diminish the fabric of basic human rights (Koops & Goodwin, 2014).

Actionable Legal and Institutional Recommendations

Given the difficulties posed in the areas of balance, cybersecurity, and human rights in the course of cross-border investigations, innovative and comprehensive solutions must be found. In a time when cybercrimes continue to grow exponentially and technology speeds ahead of legal development, a harmonisation of a framework to ensure effective law enforcement with respect for individual rights is due. Below are recommendations which could be put in place to address these pressing concerns.

(a) States should prioritise effective implementation of the Second Additional Protocol to the Budapest Convention as a practical mechanism for improving cross-border access to electronic evidence. Rather than creating entirely new global institutions, States should use the Protocol's existing cooperation mechanisms to improve direct cooperation with

service providers, access to subscriber and traffic data, emergency assistance and other forms of expedited cooperation. Implementation should remain subject to the Protocol's human-rights, rule-of-law and data-protection safeguards.

(b) At present, the existing *Mutual Legal Assistance Treaties* (MLATs) are such that they have not been very amenable and proactive in handling cyber-related cases. The world over, many inquiries are at a standstill because of the delay in data sharing between countries. Therefore, renewing the MLATs is to create a real collaboration system/platform to allow the real-time sharing of data by law enforcement agencies. Important Updates include: A centralised worldwide digital request platform that has the provision for fast, secure share for its citizens: transparency and accountability of operation between them. A system that fast-tracks emergency cases, so law enforcement can get critical evidence without delay. A legal requirement laid down for states receiving MLAT requests to do transparency reporting to ensure non-abuse of power and in accordance with human rights standards (Laidlaw, 2021).

(c) Personal data should be protected in cybercrime investigations. Most countries have not yet implemented strong data protection laws, hence the unauthorised collection of data and mass surveillance under the pretext of security. There should be a standardised global protocol for data protection, so that law enforcement agencies are guided on strict standards to follow while accessing digital data across borders. The following essential safeguards should be included: Policies of data minimisation, in which only the relevant and necessary information is gathered. Mandating end-to-end encryption to safeguard users from unapproved access. A global overseeing body that scrutinises cross-border data requests for potential human rights violations.

(d) Cross-border investigative mechanisms should incorporate minimum safeguards requiring a clear legal basis, legitimate investigative purpose, necessity and proportionality. Requests involving particularly sensitive information should be subject to stronger safeguards reflecting the intensity of

the interference with privacy and other fundamental rights (Shany, 2022).

(e) The fast emergence of artificial intelligence in cybersecurity investigation provides opportunities as well as hazards. AI-based tools can improve threat detection and automate digital forensics but, if unwisely regulated, might aggravate biases and privacy concerns. Hence, it becomes imperative to formulate an ethical AI framework to prescribe the use of AI in law enforcement. Some primary measures are: Algorithms for bias detection, to ensure that AI tools are not unfairly targeting certain communities. High standards of transparency, which would permit independent auditing of AI-based investigative tools. Mechanisms for user consent are necessary, so that people are aware that AI surveillance is being used in an investigation (Laidlaw, 2021).

(f) Where AI, biometric systems or other advanced technologies are used in cross-border investigations, legal frameworks should establish clear rules concerning human oversight, accuracy, transparency, data governance and accountability. Automated systems should support rather than displace legally accountable decision-making (Shany, 2022).

With these in place, the international community can effectively carry out the fight against cybercrime without undermining the core principles of human rights.

Conclusion

The shift towards cloud computing, distributed data storage and digitally mediated crime has changed the role of territorial jurisdiction in the investigations and prosecution of crime. Electronic evidence may be created in one jurisdiction, processed through infrastructure located in another and held by a service provider subject to the laws of a third. This division raises a continuing legal paradox regarding the effectiveness of law-enforcement action and the protection of privacy and data protection, due process and territorial sovereignty by the States.

An analysis of the comparative picture reveals that it is not a single uniform model that makes use of the existing legal framework. The Budapest Convention presents the basis of

international cooperation, and the Second Additional Protocol aims to overcome the practical shortcomings of the conventional mode of cooperation by establishing new methods to acquire electronic evidence. The CLOUD Act takes a different path, placing obligations on providers subject to the United States' jurisdiction, which can lead to entanglements with foreign sovereignty and data-protection regimes. The GDPR, on the other hand, has a greater focus on protecting and legally transferring personal data. These differences reflect the need for cross-border cooperation to rely on the interplay of several legal systems, not one uniform system.

This is a fragmented environment where judicial jurisprudence plays an important role in providing protections. Schrems I and Schrems II highlight the need to evaluate the degree of protection when personal data is transferred to another jurisdiction, especially when public authorities can access this data. Tele2 Sverige restates the need for and proportionality of communications data. Likewise, the case law of the ECHR, such as Roman Zakharov, Szabó and Vissy, Big Brother Watch and Centrum för Rättvisa, shows that legal clarity, supervision and prevention of arbitrary or disproportionate surveillance are important. Carpenter further highlights the challenge and limitations of adapting traditional privacy doctrines to the scope and sensitivity of contemporary digital information when interpreting the Constitution of the United States. When interpreting the Constitution of the U.S., Carpenter also provides an example of how difficult it is to apply traditional privacy doctrines to the scale and sensitivity of modern digital information.

The results thus indicate that the problem is not so much the lack of legal tools as the existence of different tools in disjointed form. For effective cross-border investigation, it is necessary to have mechanisms that enable access to lawful evidence in a timely fashion without enabling investigative powers to go round the hoops of the safeguards applicable in the jurisdiction in question. There is a common analytical foundation for reconciling these competing interests in the principles of legality, legitimate aim, necessity, proportionality, independent oversight, accountability and effective remedy.

The recommendations put forward in this study therefore focus on small and incremental changes and change processes, and on processes where new institutions are not to be invented, but rather

built on existing ones. There are more readily achievable avenues for reform, such as strengthening implementation of the Second Additional Protocol, modernising mutual legal assistance procedures, creating standardised electronic-evidence requests, increasing judicial and independent oversight and bolstering protections for international data transfers. These precautions also take into account the political and sovereignty limitations for cooperation on cybercrime at the international level. While there are advantages in a universal cybercrime regime on the conceptual level, there are significant differences between States regarding privacy, national security, investigative powers and data governance, which makes a smooth transition to a universal regime at a global level challenging.

Finally, it is not a question of balancing cybersecurity enforcement with the protection of human rights. A cross-border investigative system that is sustainable must be able to incorporate both. Whether international cybercrime cooperation processes are lawful, necessary, proportionate, accountable and respect the rights of persons across jurisdictions will become a key question in the future as to the legitimacy of international cooperation in the fight against cybercrime.

References

Big Brother Watch and Others v. The United Kingdom, [GC], nos. 58170/13, 62322/14 & 24960/15 (ECtHR 2021). https://hudoc.echr.coe.int/

Biasiotti, M. A., & Turchi, F. (Eds.). (2023). European investigation order: Where the law meets the technology. Springer. https://doi.org/10.1007/978-3-031-31686-9

Carpenter v. United States, 585 U.S. 296 (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8*(1), Article tyac014. https://doi.org/10.1093/cybsec/tyac014

Centrum för Rättvisa v. Sweden, [GC], no. 35252/08 (ECtHR 2021). https://hudoc.echr.coe.int/

Charter of Fundamental Rights of the European Union, 2012/C 326/02 (2012). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

Cybersecurity and Infrastructure Security Agency (CISA). (2022). Preparing critical infrastructure for post-quantum cryptography. https://www.cisa.gov/sites/default/files/2022-09/cisa_insight_post_quantum_cryptography_508.pdf

Convention on Cybercrime, ETS No. 185 (2001). Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Data Protection Commissioner v. Facebook Ireland Ltd., Case C-311/18, ECLI:EU:C:2020:559 (CJEU 2020). https://eur-lex.europa.eu/legal-content/EN/CASE/?uri=CELEX:62018CJ0311

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. Policing and Society, 33(2), 188–204. https://doi.org/10.1177/14613557221089558

Koops, B.-J., & Goodwin, M. (2014). *Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law*. Tilburg Institute for Law, Technology and Society. https://doi.org/10.2139/ssrn.2698263

Laidlaw, E. B. (2021). *Privacy and cybersecurity in digital trade: The challenge of cross-border data flows*. SSRN. https://ssrn.com/abstract=3790936

Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of New Approaches in Educational Research, 10*(1), 15–27. https://doi.org/10.7821/naer.2021.1.616

Rahman, M. H. (2021). *Practical challenges in cross-border cybercrimes: Prosecutors and investigators perspectives*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840435

Roman Zakharov v. Russia, [GC], no. 47143/06 (ECtHR 2015). https://hudoc.echr.coe.int/

Ruohonen, J. (2023). Recent trends in cross-border data access by law enforcement agencies. *arXiv*. https://arxiv.org/abs/2302.09942

Schrems v. Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650 (CJEU 2015). https://curia.europa.eu/juris/liste.jsf?num=C-362/14

Second Additional Protocol to the Convention on Cybercrime, CETS No. 224 (2022). Council of Europe. https://www.coe.int/en/web/cybercrime/second-additional-protocol

Shany, Y. (2022). *Digital rights and the outer limits of international human rights law*. Hebrew University of Jerusalem. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4270794

Smith v. Maryland, 442 U.S. 735 (1979). https://supreme.justia.com/cases/federal/us/442/735/

Szabó and Vissy v. Hungary, no. 37138/14 (ECtHR 2016). https://hudoc.echr.coe.int/

Tele2 Sverige AB v. Post- och telestyrelsen, Joined Cases C-203/15 & C-698/15, ECLI:EU:C:2016:970 (CJEU 2016). https://eur-lex.europa.eu/legal-content/EN/CASE/?uri=CELEX:62015CJ0203

United Nations. (2024). *United Nations Convention against Cybercrime*. UNODC. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

United Nations Office on Drugs and Crime (UNODC). (n.d.). *The use of cybercrime procedural tools and human rights implications*. https://www.unodc.org/documents/cybercrime/

United States v. Miller, 425 U.S. 435 (1976). https://supreme.justia.com/cases/federal/us/425/435/

Wired. (2025). *Dutch human rights advocate monitored using predictive surveillance technologies*. https://www.wired.com/story/dutch-activist-surveillance-case-2025/