Paradigm Academic Press
Law and Economy
ISSN 2788-7049
SEP. 2024 VOL.3, NO.9

Cross-Border Data Sharing and Sovereignty: Reactions of Non-EU Countries to Article 32 of the Budapest Convention

Gabriela I. Matei[1]

[1] University of Bucharest, Romania

Correspondence: Gabriela I. Matei, University of Bucharest, Romania.

doi:10.56397/LE.2024.09.01

Abstract

This paper examines the concerns of non-EU countries regarding Article 32 of the Budapest Convention on Cybercrime, which allows cross-border access to stored computer data under certain conditions. While Article 32 aims to enhance international cooperation in combating cybercrime, it has been met with resistance from several non-EU countries due to perceived threats to national sovereignty, conflicts with domestic data protection laws, and concerns over fairness and equity in its application. The paper explores these concerns in detail, highlighting the potential impacts on data privacy, legal autonomy, and international cooperation. It discusses the broader implications of these reactions for global cybersecurity efforts, including the erosion of trust, fragmentation of international frameworks, and challenges to harmonizing cybercrime laws. The paper argues for a more balanced and inclusive approach to cross-border data sharing that respects diverse legal traditions and promotes greater transparency, dialogue, and mutual trust among nations. Addressing these concerns is crucial for ensuring that the Budapest Convention remains an effective tool for combating cybercrime in a way that is fair, equitable, and respectful of all countries' interests.

Keywords: Budapest Convention, Article 32, cybercrime, national sovereignty, data privacy, international cooperation

1. Introduction

In today's digital era, cross-border data sharing is crucial for global cooperation in cybersecurity, but it also raises complex challenges related to national sovereignty and data privacy. The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, is the primary international treaty addressing these issues. Article 32 of the Convention allows law enforcement agencies to access data stored in another country without prior approval, provided they have consent from the data holder or if the data is publicly available. While intended to enhance international collaboration against cybercrime, this provision has generated significant concern among non-EU countries. These countries argue that it undermines their sovereignty by permitting foreign entities to bypass local legal processes and access data within their jurisdictions. Additionally, they fear it may conflict with their domestic data protection laws and lead to potential misuse of their citizens' data by countries with different privacy standards. Moreover, many non-EU countries perceive the Convention as reflecting the interests of Western nations, raising concerns about fairness and equity in international cybersecurity cooperation. As a result, these reactions highlight the need for more balanced approaches to cross-border data sharing that respect diverse legal frameworks and promote mutual trust among nations.

2. Understanding Article 32 of the Budapest Convention

Article 32 of the Budapest Convention, formally known as the Convention on Cybercrime, deals with the sensitive issue of cross-border access to stored computer data. The article aims to address a fundamental challenge in the digital age: the need for rapid and effective cooperation across borders to combat cybercrime.

Given the global and borderless nature of cyber threats, traditional legal frameworks and jurisdictional boundaries often prove inadequate. Article 32 seeks to create a legal mechanism for law enforcement agencies to access data stored in foreign jurisdictions, which is essential for responding swiftly to cyber incidents and preventing the destruction or loss of critical digital evidence. However, the article's broad and somewhat ambiguous wording has generated significant debate about its potential implications for national sovereignty, data privacy, and international legal norms.

2.1 The Key Provisions of Article 32

Article 32, titled "Trans-border access to stored computer data with consent or where publicly available," is divided into two main parts:

Article 32(a): Access with Consent of the Person Concerned

This provision allows a law enforcement agency in one country to access or receive data stored in another country with the consent of the person who has lawful authority over that data. This could mean the owner of the data, such as an individual user or a business entity, granting permission to foreign law enforcement authorities to access their data directly from servers located abroad. The rationale behind this provision is to simplify cross-border investigations by bypassing the need for time-consuming formalities such as mutual legal assistance treaties (MLATs) when the data holder consents. While this can expedite investigations, it raises questions about whether such consent could be coerced or whether it circumvents established international protocols that respect national sovereignty.

Article 32(b): Access to Publicly Available Data

This part of Article 32 allows law enforcement authorities to access publicly available data, regardless of where it is geographically stored, without needing additional authorization from the country where the data resides. The provision is generally less contentious, as it pertains to data that is already accessible to anyone, such as information on public websites. However, complexities can arise when defining what constitutes "publicly available" data, especially in cases where data is partially restricted or exists in a grey area between private and public domains. The provision assumes that because the data is public, there should be no legal barriers to access, yet different countries have varying definitions and protections around the concept of publicly available information.

2.2 Purpose and Rationale Behind Article 32

The inclusion of Article 32 in the Budapest Convention reflects a pragmatic approach to cybercrime, acknowledging the challenges posed by the borderless nature of cyberspace. Cybercrime investigations often require immediate access to data stored in multiple jurisdictions, and the standard processes of international cooperation, such as MLATs, are frequently criticized for being slow and cumbersome. By allowing direct access to data with consent or when publicly available, Article 32 aims to remove procedural hurdles, enabling faster response times, which are critical in cases where data may be encrypted, deleted, or altered. The provision also recognizes the increasing role of private entities, such as internet service providers (ISPs) and cloud storage companies, in holding vast amounts of data crucial for criminal investigations. In many cases, these entities operate across borders and can provide quicker and more reliable data access than traditional state-to-state cooperation mechanisms. By allowing data access with the consent of these entities or individuals, Article 32 aims to streamline international cooperation and enhance the effectiveness of cybercrime investigations.

2.3 Ambiguities and Legal Challenges

Despite its intended benefits, Article 32 is often criticized for its vague language and lack of clarity, which can lead to multiple interpretations and legal uncertainties. For example, the provision does not define what constitutes "consent" or how it should be obtained, leaving it open to interpretation by individual countries or law enforcement agencies. This ambiguity raises concerns that consent could be obtained under duress or through other coercive means, undermining the voluntary nature implied by the article. Additionally, the lack of clear guidelines on what qualifies as "lawful and voluntary consent" can create inconsistencies in its application, potentially allowing for abuse by authorities seeking to bypass more stringent legal requirements. Another point of contention is the lack of a robust oversight mechanism within Article 32. While the provision facilitates rapid access to data, it does not include explicit safeguards or oversight procedures to prevent potential misuse or to protect the privacy and human rights of individuals whose data is accessed. This omission is particularly concerning for countries that prioritize data protection and privacy rights, as it suggests that foreign authorities could access data with minimal oversight from the country where the data is stored, raising alarms about potential breaches of national data protection laws and regulations.

2.4 Implications for Sovereignty and International Law

The most significant challenge posed by Article 32 is its potential impact on national sovereignty and the

established principles of international law. Sovereignty, the fundamental principle that grants states exclusive rights to govern their territory and enforce their laws without external interference, is directly challenged by any provision that allows foreign authorities to act unilaterally within another state's jurisdiction. Critics argue that Article 32 effectively bypasses this principle by permitting cross-border data access without requiring the consent or knowledge of the state where the data resides. This has led to concerns that Article 32 could set a precedent for extraterritorial enforcement actions, potentially undermining the authority of national governments to regulate and control activities within their own borders. The provision can lead to conflicts with domestic laws and legal frameworks, especially in countries with strict data protection regulations. For example, the European Union's General Data Protection Regulation (GDPR) mandates stringent controls on the transfer of personal data outside the EU, requiring that data protection standards are equivalent to those within the EU. Under Article 32, data accessed by foreign law enforcement agencies may not be subject to the same standards of protection, potentially violating domestic laws and international agreements aimed at safeguarding data privacy.

2.5 Broader Geopolitical and Strategic Concerns

Beyond the legal and procedural challenges, Article 32 has broader geopolitical and strategic implications. Many non-EU countries view the provision as reflecting Western-centric approaches to cybersecurity and international law enforcement, potentially sidelining the interests and legal norms of other regions. This perception is particularly strong among countries like Russia, China, and several members of the Global South, which have voiced concerns that the Convention's provisions, including Article 32, serve primarily the interests of Western states. These countries argue that the Budapest Convention lacks inclusivity and fails to adequately represent the perspectives of non-Western nations, creating an imbalance in the global governance of cyberspace. The emphasis on direct cooperation with private entities, which are often based in the United States or Europe, raises concerns about the influence of large technology companies and the potential for private-sector interests to shape public policy and international law enforcement practices. For countries with different regulatory philosophies or concerns about foreign interference in their digital ecosystems, this aspect of Article 32 is particularly troubling.

Article 32 of the Budapest Convention represents an ambitious attempt to address the complexities of cross-border data access in the fight against cybercrime. While its provisions are designed to facilitate faster and more effective cooperation, they also raise significant concerns regarding national sovereignty, legal clarity, data privacy, and international equity. The provision's ambiguous language and lack of oversight mechanisms create challenges that need to be addressed to foster broader acceptance and ensure that the Convention remains an effective tool for global cybersecurity cooperation. To achieve a more balanced approach, there is a pressing need for ongoing dialogue and refinement of the Convention's provisions to accommodate the diverse legal, cultural, and political contexts of all participating states.

3. Concerns of Non-EU Countries Regarding Article 32

The adoption and implementation of Article 32 of the Budapest Convention have generated substantial concerns among non-EU countries. These concerns revolve around three primary themes: the perceived infringement on sovereignty and jurisdictional integrity, conflicts with data privacy standards, and a lack of reciprocity and balance in the Convention's application. Each of these concerns reflects broader anxieties about international power dynamics, legal autonomy, and the protection of fundamental rights in an increasingly digital world.

3.1 Sovereignty and Jurisdictional Integrity

A core concern for non-EU countries regarding Article 32 is its perceived encroachment on national sovereignty and jurisdictional integrity. Sovereignty, a cornerstone of international law, denotes a state's right to exercise authority and control over its territory and legal matters without external interference. Article 32(b) appears to challenge this principle by allowing foreign law enforcement agencies to access data stored in another state's jurisdiction without prior consent from the government of that state. For many non-EU countries, this provision threatens to erode their ability to regulate activities within their own borders, setting a troubling precedent for unauthorized external interventions. Non-EU countries, particularly those like India, Brazil, and Russia, argue that Article 32 could facilitate conflicts of jurisdiction where multiple states claim legal authority over a particular cybercrime incident or data set. In practice, this means that foreign law enforcement could potentially operate on their soil, extracting or requesting data without oversight or cooperation from local authorities, thereby undermining their national legal frameworks. These countries fear that such scenarios could lead to a loss of control over their digital sovereignty, weaken their jurisdictional integrity, and generate significant diplomatic tensions, especially in cases where data access is contested or considered politically sensitive. The Budapest Convention lacks explicit mechanisms for resolving these jurisdictional disputes or addressing concerns about extraterritorial enforcement actions. The absence of a robust dispute resolution process creates uncertainties and anxieties about how conflicts over data access would be managed. This perceived gap in the Convention may deter non-EU countries from fully committing to its provisions, undermining the effectiveness of international cooperation against cybercrime.

3.2 Data Privacy Concerns

Another significant concern for non-EU countries relates to data privacy and the potential conflicts between Article 32 and domestic data protection laws. Many non-EU countries have developed comprehensive data protection frameworks designed to safeguard their citizens' privacy and ensure that personal data is not accessed or used without proper authorization. These laws are often informed by a broader commitment to human rights and the ethical use of information, recognizing the fundamental importance of privacy in democratic governance and social trust. Article 32's allowance for cross-border data access, particularly without state consent, is seen as potentially undermining these national efforts. In countries like Brazil and India, which have recently enacted stringent data protection laws (the General Data Protection Law in Brazil and the Personal Data Protection Bill in India), there is concern that Article 32 might create loopholes through which foreign agencies could access data without adhering to local privacy standards. This could weaken regulatory enforcement and erode public confidence in the government's ability to protect citizens' data from foreign intrusion.

There is apprehension that data accessed under Article 32 might not be subjected to equivalent privacy protections in the foreign jurisdiction, potentially leading to misuse or exploitation of sensitive personal information. This concern is especially pronounced in countries where data protection is tied to broader social justice and human rights issues, such as in several Latin American and African states. The provision could inadvertently facilitate practices that are contrary to local values or legal norms, such as mass surveillance or profiling, thereby generating significant resistance to its adoption.

3.3 Lack of Reciprocity and Perceived Imbalance

A third major concern among non-EU countries involves the perceived lack of reciprocity and balance in the application of Article 32. The Budapest Convention, developed primarily within the context of the Council of Europe and with substantial input from EU member states, is often viewed as a reflection of Western priorities and legal standards. Non-EU countries argue that the Convention, and Article 32 in particular, does not adequately take into account their unique legal, cultural, and political contexts.

Countries like Russia have criticized Article 32 as disproportionately favoring states with advanced cyber capabilities, predominantly in Europe and North America, which have the resources and technical expertise to engage effectively in cross-border data access operations. This dynamic is perceived as putting other countries, particularly those in the Global South, at a disadvantage. Without equitable participation in the drafting and amendment processes of the Convention, non-EU states feel they are being asked to adhere to rules and standards that they had little influence in shaping.

This perception of imbalance can undermine the spirit of international cooperation that the Convention aims to foster. Countries that view the provisions as skewed or inequitable may be reluctant to engage fully with the Budapest Convention, opting instead for alternative regional frameworks or bilateral agreements that they perceive as more aligned with their interests. For example, Russia have pursued their own initiatives, such as promoting an alternative cybercrime convention through the United Nations, emphasizing state sovereignty and non-interference as key principles.

3.4 Concerns Over Legal Certainty and Human Rights

Non-EU countries also express concerns about the lack of legal certainty and potential human rights implications of Article 32. The provision's vague wording—such as the undefined nature of "consent"—raises questions about how the law will be interpreted and applied in practice. Without clear definitions and guidelines, there is a risk that the provision could be exploited or misused by powerful states to pursue their interests under the guise of legal enforcement, potentially violating fundamental human rights. This uncertainty can discourage cooperation and erode trust between countries, especially those that have historically experienced external interference. Countries with different legal traditions, such as those in Asia, Africa, and Latin America, worry that the broad scope of Article 32 could be used to justify actions that contravene their domestic laws and international human rights commitments. For instance, a request for data that is considered legal under one country's laws could be seen as a violation of privacy rights under another country's regulations. Such conflicts could result in legal battles and further complicate international cooperation on cybercrime, particularly where there is no clear framework for adjudicating these disputes.

3.5 Strategic and Geopolitical Concerns

Beyond the legal and regulatory issues, there are also broader strategic and geopolitical concerns. Many non-EU countries perceive Article 32 as an extension of Western influence in cyberspace, which can be seen as part of a broader geopolitical strategy to maintain control over global internet governance. In particular, countries like China, Russia, and others have long argued that international cyber norms should reflect a more multipolar world, where power and influence are more evenly distributed. The perception that the Budapest Convention reflects Western-centric values and priorities may therefore deter these countries from fully committing to its provisions.

For many non-EU countries, concerns over Article 32 also intersect with broader questions about digital sovereignty, technological independence, and the control of information flows. In an era of increasing geopolitical competition in cyberspace, these countries may be unwilling to accept provisions that they believe could compromise their strategic autonomy or subject them to the surveillance and monitoring activities of foreign powers.

The concerns of non-EU countries regarding Article 32 of the Budapest Convention reflect deep-seated anxieties about sovereignty, data privacy, legal equity, and international relations in the digital age. These countries fear that the provision could undermine their national sovereignty, conflict with domestic data protection laws, and perpetuate a perceived imbalance in international cyber norms. Addressing these concerns requires ongoing dialogue and negotiation to develop more inclusive and balanced frameworks for cross-border data sharing that respect diverse legal traditions, safeguard privacy rights, and promote mutual trust among nations. Such efforts are crucial for fostering effective global cooperation in the fight against cybercrime while ensuring that international legal frameworks remain fair and equitable for all.

4. Impacts on International Cooperation and Cybersecurity Efforts

The concerns raised by non-EU countries regarding Article 32 of the Budapest Convention have profound implications for international cooperation and global cybersecurity efforts. These impacts extend beyond the immediate legal and regulatory challenges and touch on broader issues of trust, fairness, and inclusivity in international relations. As countries navigate these complexities, the effectiveness of global efforts to combat cybercrime and enhance cybersecurity may be significantly influenced by how well these concerns are addressed.

4.1 Erosion of Trust and Reluctance to Cooperate

One of the most significant impacts of Article 32 is the potential erosion of trust between countries, particularly between EU member states and non-EU countries. Trust is a fundamental component of any international cooperation, especially in sensitive areas such as cybersecurity, where the stakes are high, and the potential for conflict is significant. The perception that Article 32 allows for unilateral actions by foreign law enforcement agencies, potentially bypassing local laws and authorities, creates a sense of mistrust and apprehension among non-EU countries. This erosion of trust can lead to a reluctance to engage in broader international cooperation under the Budapest Convention framework. Countries that perceive their sovereignty or privacy protections to be at risk may choose to limit their involvement or may be less willing to share crucial information, fearing that it could be accessed or misused by foreign entities without adequate oversight or accountability. As a result, the global fight against cybercrime could become fragmented, with countries opting to pursue regional or bilateral agreements that they perceive as more aligned with their interests, rather than participating in a unified international approach.

4.2 Fragmentation of International Cybersecurity Frameworks

The perceived imbalances and ambiguities in Article 32 could lead to the fragmentation of international cybersecurity frameworks, as non-EU countries seek alternative arrangements that better reflect their interests and legal standards. For instance, some countries, particularly those in Asia, Africa, and Latin America, might opt to strengthen regional cybersecurity cooperation through organizations such as the African Union or the Association of Southeast Asian Nations (ASEAN). These organizations have been working on their own cybersecurity initiatives, often emphasizing principles such as state sovereignty and non-interference, which they feel are inadequately addressed in the Budapest Convention. Some non-EU countries are pursuing alternative global frameworks through the United Nations (UN). Russia and China, for example, have advocated for a new UN-led cybercrime treaty that would replace or supplement the Budapest Convention. Such a treaty would likely emphasize state sovereignty and offer a more state-centric approach to international cybersecurity governance, potentially appealing to countries that view the Budapest Convention as Western-centric. However, the development of parallel frameworks could lead to a fragmented global landscape, where conflicting norms, standards, and practices complicate international cooperation and reduce the effectiveness of global efforts to combat cybercrime.

4.3 Challenges to Harmonization of Cybercrime Laws

Article 32's controversial provisions could also undermine efforts to harmonize cybercrime laws across different jurisdictions. The Budapest Convention was designed to promote legal harmonization by encouraging states to adopt common definitions, legal principles, and procedures for investigating and prosecuting cybercrime. However, the concerns raised by non-EU countries suggest that there is still significant divergence in national approaches to cybercrime, particularly regarding cross-border data access and privacy protection. Non-EU countries that view Article 32 as incompatible with their domestic legal frameworks may be reluctant to align their laws with the Convention's provisions, limiting the harmonization of cybercrime laws. This lack of

harmonization could create legal and procedural gaps that cybercriminals can exploit, taking advantage of discrepancies in national laws to evade detection and prosecution. Without a common framework for defining and addressing cybercrime, international efforts to combat these threats will likely face significant challenges, reducing their overall effectiveness.

4.4 Potential for Diplomatic Tensions and Conflicts

The application of Article 32 has the potential to generate diplomatic tensions and conflicts, particularly in cases where data access requests are perceived as overreaching or politically motivated. For instance, if a foreign law enforcement agency were to access data stored within a non-EU country without prior notification or approval from the host government, this could be seen as an infringement of national sovereignty and provoke a diplomatic response. Such incidents could lead to bilateral disputes, strained diplomatic relations, and a reduction in overall cooperation on cybersecurity and other issues. Diplomatic tensions could also arise if a country perceives that its citizens' data has been accessed or used in ways that violate its domestic laws or international human rights obligations. This is particularly likely in cases where there are significant differences in legal standards and protections, such as between countries with strong data privacy laws and those with more permissive approaches to data access and surveillance. The resulting conflicts could further erode trust and make it more difficult to build the consensus needed for effective international cooperation against cybercrime.

4.5 Implications for Human Rights and Privacy

Concerns about Article 32's impact on human rights and privacy have significant implications for international cooperation on cybersecurity. Non-EU countries, especially those with strong commitments to data protection and human rights, may be hesitant to engage fully with the Budapest Convention if they believe that its provisions could lead to violations of these rights. For example, countries like Brazil, which have enacted comprehensive data protection laws, may view Article 32 as undermining their efforts to safeguard citizens' privacy, particularly if data is accessed by foreign entities without adequate safeguards.

This apprehension could lead to increased resistance to international cooperation on cybercrime and reluctance to share data with countries perceived as having lower standards of privacy protection. In turn, this could impede efforts to build a comprehensive and cohesive global cybersecurity strategy, as countries prioritize their domestic legal frameworks and human rights obligations over international commitments. Additionally, concerns about privacy violations could result in increased public scrutiny and opposition to international agreements perceived as infringing on fundamental rights, making it politically challenging for governments to ratify or implement such treaties.

4.6 Hindering the Development of a Global Consensus on Cyber Norms

The controversy surrounding Article 32 also poses challenges for the development of a global consensus on cyber norms and standards. Cybersecurity is a complex and rapidly evolving field, requiring continuous adaptation and agreement on norms of state behavior in cyberspace. However, the concerns raised by non-EU countries regarding Article 32 suggest that there are deep-seated differences in how states view issues like data sovereignty, privacy, and law enforcement jurisdiction in the digital realm. These differences can make it difficult to achieve a global consensus on key cybersecurity principles, such as what constitutes acceptable state behavior in cyberspace or how to balance law enforcement needs with the protection of human rights and data privacy. Without a shared understanding of these principles, international efforts to establish a stable and secure cyberspace may be undermined, increasing the risk of misunderstandings, miscalculations, and conflicts in the digital domain.

4.7 Impact on Capacity Building and Technical Assistance

Article 32's controversial nature could also affect capacity-building efforts and technical assistance programs aimed at improving global cybersecurity resilience. Many non-EU countries, particularly in the Global South, require support and assistance to develop their cybersecurity capabilities, enhance their legal frameworks, and build their capacities to investigate and prosecute cybercrime. However, these countries may be reluctant to engage with capacity-building programs that are perceived as promoting or enforcing the provisions of Article 32, especially if they view these provisions as contrary to their national interests or legal traditions. This reluctance could limit the effectiveness of international capacity-building efforts and reduce opportunities for knowledge sharing, technical cooperation, and the development of best practices. In turn, this could slow the progress of building a more resilient global cybersecurity architecture and leave many countries vulnerable to cyber threats, ultimately undermining the collective ability to prevent and respond to cybercrime.

The concerns of non-EU countries regarding Article 32 of the Budapest Convention have far-reaching implications for international cooperation and cybersecurity efforts. These concerns, centered on issues of sovereignty, privacy, fairness, and inclusivity, could lead to reduced trust, fragmented frameworks, and increased diplomatic tensions, all of which threaten to undermine global efforts to combat cybercrime. Addressing these

concerns will be crucial for building a more cohesive and effective international approach to cybersecurity. This requires not only re-evaluating the provisions of Article 32 but also fostering greater dialogue, understanding, and cooperation among all countries to develop a balanced and inclusive framework that respects diverse legal traditions and promotes global cybersecurity resilience.

5. Conclusion

The reactions of non-EU countries to Article 32 of the Budapest Convention underscore the complex and often contentious relationship between cross-border data sharing, data privacy, and national sovereignty in the digital age. As cyberspace becomes increasingly integral to every aspect of global society—from economic transactions to national security—international legal frameworks must adapt to new challenges posed by cybercrime. Article 32, designed to streamline and expedite international cooperation in the fight against cybercrime, reveals the tensions between the need for rapid, effective law enforcement and the need to respect national sovereignty, legal autonomy, and diverse data protection regimes. While the intention behind Article 32 is to facilitate faster cross-border access to data, the provision has been met with considerable skepticism and resistance from non-EU countries. These countries view the article as a potential encroachment on their sovereignty, enabling foreign law enforcement agencies to bypass national jurisdictions and undermine local legal frameworks. Moreover, there is a prevailing concern that Article 32 could lead to conflicts with domestic data privacy laws, which are often designed to safeguard citizens' personal information against unauthorized access and misuse. The perceived imbalance in the Convention's application, with its roots in Western-centric legal traditions, further exacerbates these concerns and highlights a need for more inclusive and equitable approaches to international cybersecurity governance.

To ensure that the Budapest Convention remains a viable and effective tool for combating cybercrime, it is essential to address the concerns raised by non-EU countries. This will require a multifaceted approach that includes ongoing dialogue and negotiation to clarify and refine the provisions of Article 32. Such dialogue must focus on achieving a balance between the legitimate needs of law enforcement for timely data access and the equally valid concerns about sovereignty, privacy, and legal autonomy. This balance could be achieved through the development of clearer definitions, more robust oversight mechanisms, and enhanced safeguards that protect against potential abuses and ensure that all data access is conducted in a manner consistent with international human rights standards. Fostering greater transparency and cooperation among all countries will be critical in building the trust necessary for effective international collaboration. Transparency in how cross-border data access requests are made, handled, and overseen can help alleviate fears of overreach or misuse and provide assurance that such access is conducted lawfully and ethically. Engaging non-EU countries more actively in the decision-making processes related to amendments and interpretations of the Convention can also help create a sense of shared ownership and commitment to its principles. This inclusive approach would help to address the perceived inequities in the Convention's application and ensure that it better reflects the diverse legal, cultural, and political contexts of all participating states. In addition to promoting transparency and dialogue, there is a need for developing alternative frameworks or complementary agreements that respect the diverse regulatory environments and data protection standards of different countries. Such frameworks could provide tailored mechanisms for data access that align more closely with national laws while still facilitating international cooperation. This could involve regional agreements that supplement the Budapest Convention or new global treaties under the auspices of the United Nations or other international organizations that address specific concerns about sovereignty and privacy in cyberspace. There is a critical need to consider the broader geopolitical context in which these concerns are being raised. Cybersecurity is not just a technical issue but also a strategic one, with significant implications for national security, economic competitiveness, and global governance. As such, it is vital to recognize the strategic interests and perspectives of all countries and to work toward building a genuinely inclusive international cybersecurity order that fosters trust and cooperation rather than deepening divides. This approach requires a commitment from all stakeholders—EU and non-EU countries alike—to engage in constructive dialogue, compromise, and mutual respect.

The concerns of non-EU countries regarding Article 32 of the Budapest Convention reveal the complexities and nuances of navigating cross-border data sharing in an era of rapid technological change and shifting geopolitical dynamics. Addressing these concerns is not merely a matter of legal fine-tuning but a broader effort to build a more inclusive, balanced, and effective framework for international cooperation in cyberspace. By fostering dialogue, enhancing transparency, and developing equitable mechanisms that respect diverse legal standards, the international community can strengthen its collective response to cybercrime and ensure that all countries are confident and willing partners in this crucial global endeavor. Only through such inclusive and balanced approaches can the Budapest Convention and similar frameworks remain effective tools for promoting a secure and cooperative international digital environment.

References

Bellanova, R., Carrapico, H., & Duez, D., (2022). Digital/sovereignty and European security integration: an introduction. *European Security*, *31*(3), 337-355. https://doi.org/10.1080/09662839.2022.2101887

Council of Europe., (2001). *Convention on Cybercrime (Budapest Convention)*. Council of Europe Treaty Series No. 185. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Greenleaf, G., (2012). Global Data Privacy Laws: Forty Years of Acceleration. *Privacy Laws & Business International Report*, *115*(1), 1-17. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235095

Tzanou, M., (2013). Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right. *International Data Privacy Law*, *3*(2), 88-99. https://doi.org/10.1093/idpl/ipt004

United Nations Office on Drugs and Crime (UNODC)., (2021). *The Need for a New International Treaty on Cybercrime: Perspectives from Non-EU Countries*. UNODC Cybercrime and Anti-Money Laundering Section. Retrieved from https://www.unodc.org/