International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

The Second Additional Protocol-2022: Relevance and Significance in Contemporary World

Namrata Mishra

Email: *namrata.mishra1506[at]gmail.com*

Abstract: ***The 2nd Additional Protocol of 2022 to the Convention on Cybercrime (Budapest Convention, 2001) for Enhanced Cooperation and Disclosure of Electronic Evidence represents a rapid advancement in international platform to deal with cybercrime. Recognizing the growth of complexity of transnational cyber offenses, the protocol deals with mechanisms to facilitate expedited cooperation among state parties along with balancing fundamental rights, including privacy and data protection. This project critically evaluates the protocol's key provisions, including direct cooperation with the service providers, emergency mutual legal assistance (MLA), and the need for new frameworks for data disclosure. It analyzes how the protocol seeks to address jurisdictional challenges and regulate trans-border access to e-evidence, crucial for cybercrime investigations. It concludes with recommendations for policy enhancements to provide balanced implementation, reinforcing cyber resilience without compromising individual liberties.***

Keywords: cybercrime cooperation, electronic evidence sharing, data protection and privacy, cross-border data access, Budapest Convention protocol

1. Introduction

In a rapidly digitalized world, cybercrime has evolved as one of the most pressing challenges to global security, governance, and individual rights. The rapid growth of technology has outpaced traditional legal frameworks, leading to gaps in the ability of states to effectively deal cyber threats. Recognizing this, the 2022 protocol represents a landmark step to modernize international legal frameworks and address the complexities of cybercrime in the 21st century. This protocol, building on the foundational Budapest Convention, aims to increase cross-border cooperation, streamline the disclosure of electronic evidence, and ensure that law enforcement agencies can deal with cyber threats along with safeguarding fundamental rights.

This project examines the key provisions of the 2nd additional protocol, its implications for international law enforcement, and its role in addressing contemporary cybercrime challenges. By evaluating its relevance and significance, the research aims to provide a comprehensive knowledge of how this protocol contributes to a safer and more cooperative digital world.

2. Review of Literature

1) "Aradhya Sethia, Rethinking Admissibility of Electronic Evidence, 24 Int'l J.L. & Info. Tech. 229 (2016)"

This article examines the complex procedural issues with respect to admissibility of electronic evidence, which forms foundation for enforcing legal rights and obligations. It focuses on key challenges such as whether a specialized or general legal framework is more effective, the specific criteria for determining admissibility, etc. Using India's legal framework as a central case study, this article also draws comparisons with other jurisdictions such as the USA, South Africa to explore how these issues have been dealt with.

2) "M. Gercke, Understanding Cybercrime: A Guide for Developing Countries (2d ed., ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, Draft Mar. 2011)".

The guide offers a comprehensive overview of important legal aspects of cybercrime, with a sole focus on the requirements of other countries. Given the "transnational aspect of cybercrime", the legal frameworks applicable to both developing and developed nations remain largely the same. However, the references provide benefit to the developing countries. It provides a wide range of resources to facilitate a deeper understanding of several issues.

3) "Christopher Kuner, The Internet and the Global Reach of EU Law, in EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law 112 (Marise Cremona & Joanne Scott eds., Oxford Univ. Press 2019) (originally published as LSE Legal Studies Working Paper No. 4/2017, Univ. of Cambridge Faculty of Law Research Paper No. 24/2017, Feb. 1, 2017)".

This article discusses about EU's action in exercising its global reach by several key mechanisms, including regulation, coercion, conditionality, and the blocking of recognition of 3rd country legal measures. These actions raise significant questions such as distinguishing between promoting core EU legal thoughts and increasing EU's political interests. This article discusses about EU's influence carrying responsibilities towards third countries, particularly the developing countries.

Research Objectives

1) To examine the specific provisions of the Protocol, particularly those related to enhanced co-operation and the disclosure of e-evidence.
2) To Evaluate the Relevance of the Protocol in addressing contemporary cybercrime challenges
3) To Propose Recommendations for Strengthening the Protocol's Impact

Research Questions

1) How effective is the 2nd additional protocol, 2022 in enhancing international co-operation and the disclosure of e-evidence?
2) How does the 2022 protocol and other international frameworks address contemporary cybercrime challenges?
3) What reforms can enhance its effectiveness in cross-jurisdictional electronic evidence disclosure?

Research Methodology

In this study, the doctrinal technique of research is used. The research used in the publication is descriptive in nature. For the primary data, the research explores international treaties and legislation. It gathers information from a variety of secondary sources, including research papers, journals, and articles. It talks about the type of exhaustion principle that is used in both national and international systems. For a country, it weighs the benefits and drawbacks of international exhaustion principles.

Abbreviations

- Additional Protocol – AP
- Second Additional Protocol (2022) – SAP-2022
- Convention on Cybercrime – CCC
- Budapest Convention (2001) – BC
- Council of Europe – CoE
- Mutual Legal Assistance – MLA
- Mutual Legal Assistance Treaty – MLAT
- Electronic Evidence – E-Evidence / E-Evidence
- Subscriber Information – SI
- Traffic Data – TD
- Stored Computer Data – SCD
- Domain Name Registration Information – DNRI
- Direct Cooperation – DC
- Emergency Cooperation – EC
- Emergency Mutual Assistance – EMA
- 24/7 Network of Contact Points – 24/7 Network
- Service Providers – SPs
- Joint Investigation Teams – JITs
- Video Conferencing – VC
- Cross-Border Data Access – CBDA
- Trans-Border Access to Data – TBAD
- International Cooperation – IC
- Jurisdictional Challenges – JC
- Data Disclosure – DD
- Personal Data Protection – PDP
- Privacy and Data Protection Safeguards – PDPS
- Human Rights Safeguards – HRS
- Information and Communication Technology – ICT
- Internet of Things – IoT
- Digital Forensics – DF
- Computer Forensics – CF
- Cybercrime Investigations – CI
- International Human Rights Law – IHRL
- General Data Protection Regulation – GDPR
- European Union – EU
- Court of Justice of the European Union – CJEU
- United States of America – USA
- United Nations – UN
- Information Technology Act, 2000 (India) – IT Act
- Digital Personal Data Protection Act, 2023 (India) – DPDP Act
- Bharatiya Sakshya Adhiniyam, 2023 – BSA
- Bharatiya Nagarik Suraksha Sanhita, 2023 – BNSS
- Supreme Court of India – SC

3. Analysis

Chapter 1: Legal Framework of the Protocol

1.1 Overview of the Protocol's Provisions

Analysing the pro-liferation of cybercrime and the growth of complexity of obtaining e-evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement agencies are limited by territorial jurisdictions. As a result, only a little share of cyber-crime that is reported to criminal justice adjudicating authorities is leading to court decisions.

As a response, 2022 protocol[1] gives a "legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective way to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards".

Preamble

"The protocol is signed by member states of the Council of Europe (CoE) and other states parties to the convention on cybercrime (ETS No. 185).[2] The Budapest Convention is known for its global impact. The convention is supplemented by the First Additional Protocol (ETS No. 189, 2003) on criminalizing racist and xenophobic acts committed via computer systems".[3]

However, the challenges posed by the cybercrime investigations relate to the storing of electronic evidence in foreign, multiple or unknown jurisdictions making access complex. The existing measures for cross-border cooperation are insufficient, requiring additional measures.

The protocol aims to:

a) Enhancing international cooperation on cybercrime and electronic evidence collection.
b) Bringing more efficient mutual assistance and new cooperation mechanisms, including:
   - Emergency cooperation.
   - Direct cooperation between competent authorities and service providers.
c) Giving legal clarity for service providers regarding data disclosure to foreign authorities.
d) Ensuring privacy and data protection safeguards in compliance with international human rights standards.

Any measures for cybercrime investigations must be subject to conditions and safeguards to protect individual rights. There should be compliance with constitutional and international obligations concerning privacy personal information.

[1] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

[2] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[3] https://www.coe.int/en/web/cybercrime/first-additional-protocol

Chapter I: Common Provisions
Chapter I of the protocol runs from Article 1 to Article 4.

Article 1 talks about the purpose of the protocol i.e. it supplements the Convention for parties to this protocol and also the 1st additional protocol to the Convention on Cybercrime.
"Article 2 specifies the scope of application of the protocol. It specifies that the measures in this protocol apply to-

a) Criminal investigations or proceedings related to computer systems and data, and the collection of electronic evidence, for Parties to the Convention and this Protocol; and
b) Criminal investigations or proceedings under the First Protocol for Parties to both the First Protocol and this Protocol. And each party must adopt necessary laws and measures to fulfil the obligations under this protocol".

1.2. Procedural Aspects of 2022 Protocol

Chapter II – Measures for Improved Cooperation[4]
Section 1 deals with the "General Principles" applicable to Chapter II.

Section 2: Direct Co-operation with Service Providers.
It runs from Article 6 to Article 7.

Article 6 talks about Domain Name Registration Information. Acc. To Article 6, Parties must empower their authorities to request domain name registration information from entities in other countries for criminal investigations.

"Article 7 deals with Subscriber Information. Acc. To Article 7, Parties must empower their authorities to order service providers in other countries to disclose subscriber information for criminal investigations. And Service providers must be allowed to disclose such information".

Section 3: International Cooperation for Stored Data.
It's comprised of Article 8 and 9.

"Article 8 discusses about the Expedited Production of Subscriber and Traffic Data. Acc. To Article 8, parties must empower their authorities to request subscriber and traffic data from service providers in emergencies".

Article 9 deals with expedited disclosure during Emergencies. To ensure the same parties must provide their 24/7 points of contact to request immediate assistance for disclosing stored data. The requested party must respond quickly and may also impose conditions.

Section 4: Emergency Mutual Assistance
"Article 10 deals with Emergency Mutual Assistance. Acc. To Article 10, Parties can request mutual assistance in emergencies. However, the requests must include a description of the emergency and relevance of the assistance".[5]

Section 5: Cooperation without Agreements
Section 5 covers Article 11 and Article 12.
Cooperation without agreements can be done through two means-

- Video Conferencing
- Joint Investigation Teams

"The parties can request for video conferencing for testimony or statements and the requested party must inform the requesting party of any delays/refusals".

The parties can also establish Joint Investigation Teams for enhanced coordination with approval of central authority. It can be conducted on a case-by-case basis without any formal agreements[6].

Chapter III: Conditions & Safeguards
Chapter III covers Article 13 & 14.

"Article 13 talks Conditions and Safeguards". Acc. to this article, Each Party must ensure that the powers and procedures under this Protocol comply with its domestic law. Such implementation must provide "adequate protection of human rights and liberties".

"Article 14 talks Protection of Personal Data". It provides that the personal data must follow specific measures unless alternative agreements ensure protection. Data use is restricted to specified purposes, requiring accuracy, relevance and protection for personal sensitive data. Security measures, oversight, retention period, individual rights and redress mechanisms must be ensured. Transfers require authorization, and breaches might justify suspension.

Chapter 2: The Protocol's Role in Addressing Contemporary Cybercrime Challenges

2.1. Emerging Cybercrime Trends and Challenges

2.3 Challenges

2.3.1 General Challenges:
Cybercrime investigations are inherently complicated due to the growth of evolving nature of technology and the global reach of digital activities. However, cybercrime investigations also face challenges, they are-

a) Reliance on ICTs ("Information and Communication Technologies")
The reliance on "ICT"s for cybercrime investigations is both a boon and a ban. Investigators depend on digital tools and platforms to collect, analyse and present evidence. However, reliance also brings out vulnerabilities. As cybercriminals often exploit weaknesses in these technologies. Additionally,

[4] Council of Europe Treaty Series – No. 224 (2022). Second Additional Protocol: Convention on Cyber-crime on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.05.2022.
[5] "Article 25 paragraph 3 of the Council of Europe Convention on Cybercrime, where requests for mutual assistance may be made by means of rapid communication in urgent circumstances which does not rise to the level of emergency as defined".
[6] This applies "whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned".

the rapid evolution of ICTs signifies that investigators must constantly update their skill and tools to keep pace with new threats.[7]

b) Amount of the Number of Users

The sheer volume of "internet users" worldwide (2 billion) brings complications in cybercrime investigations. With billions of users online, identifying suspects becomes a needle in a haystack problem. Also the anonymity provided to the users allow criminals to blend in with the legitimate users, making it difficult to trace their activities.[8]

c) Availability of Devices and Access

The introduction of devices such as smartphones, laptops, and IoT devices has enlarged the attack surface for cyber criminals. Investigators often face challenges in accessing these device due to encryption, lack of cooperation from device manufacturers or jurisdictional issues. Additionally, cybercrime criminals often use disposable or compromised devices, complicating investigations.

In the case of **Autronic v. Switzerland**, the European Court of Human Rights ruled that extensive interpretation of laws is the need when dealing with restrictions on communication. The court emphasized that any limitation on the means of communication (like technology or tools) inherently "interferes with the right to receive and impart information", which is protected under human rights law.[9]

d) Availability of Information

Cybercrime investigations needs access to vast amounts of data, including logs, metadata, and communication records[10]. The internet's success relies heavily on powerful search engines like Google, which allow users to search millions of webpages in seconds. However, this technology can be used for both good and bad purposes.

For example, "Google hacking" or "Googledorks" refers to using advanced search techniques to find sensitive information about computer security vulnerabilities. Criminals might use these methods to locate systems with weak password protections or other security flaws[11].

e) Missing Mechanisms of Control

The lack of standardized mechanisms for the purpose of monitoring and controlling online activities makes it complex to prevent and investigate cybercrimes. For example, the lack of universal protocols for data sharing between countries or industries obstructs coordinated efforts to combat cybercrime. All communication networks, whether phone systems for calls or "the internet", require management and "technical standards" to function properly. The internet is no exception. Discussions about internet governance highlight that, like national or even global communication systems, the internet also needs rules and coordination to ensure it works smoothly and fairly.[12]

f) International Dimensions

Cybercrime often crosses national borders, requiring international cooperation for effective investigations. However, differences in legal frameworks, extradition treaties, and political relationships can create critical obstacles. Jurisdictional disputes and delays in obtaining mutual legal assistance treaties (MLATs) additionally complicates the matters.

Important data needed to trace cybercrimes is often deleted quickly, making investigations harder. Traditional legal processes for international cooperation, like mutual legal assistance, are slow and time-consuming. Additionally, the principle of dual criminality creates problems if the crime isn't recognized in one of the countries involved. Criminals often exploit these gaps by targeting victims in other countries or operating from places with weak cybercrime laws, making investigations even more difficult.[13]

To address these issues, harmonizing cybercrime laws and improving international cooperation are crucial. Two key solutions are:

- The G8 24/7 Network, which enables faster communication between countries for cybercrime cases.
- CoE convention on Cybercrime, which includes provisions to streamline international cooperation.

g) Location and Physical Presence at the Crime Site

One of the biggest challenges in fighting cybercrime is preventing "safe havens"[14]—places where criminals can operate without fear of prosecution. Many "developing countries" lack proper cybercrime laws, making them easy targets for criminals who set up operations there to escape legal consequences. This becomes a global problem because serious cybercrimes affecting people worldwide can't be stopped if the country where the criminals are based doesn't have adequate laws.

For example, the "Love Bug"[15] computer worm, created in the Philippines in 2000, infected millions of computers globally. At the time, the Philippines lacked cybercrime laws, making

[7] "The Trans-national Dimension: Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[8] "Regarding the ne-cessary steps to improve cybersecurity, see: World-Information Society Report 2007, page 95", available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[9] "Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument."

[10] "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/

[11] Long, Johnny, Skoudis, David, & van E., Rik, "*Google Hacking for Penetration Testers* (2005)"; Dornfest, Rael, Bausch, Jesse, & Calishain, Tara, "*Google Hacks: Tips & Tools for Finding and Using the World's Information"* (2006) (accessed Feb. 25, 2025).

[12] *Sadowsky, Zambrano, Dandjinou*, "Internet-Governance: A Discussion Document", 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;

[13] *Beales*, "Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging", 2004, page 9, available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf

[14] "This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies".

[15] http://news.bbc.co.uk/1/hi/sci/tech/738537.stm.

it hard to prosecute the suspect. Such cases often pressure countries to pass stronger legislation.

h) Automation
While automation can narrow down certain aspects of cybercrime investigations, it also introduces challenges. Cybercriminals frequently use automated tools to launch attacks, such as botnets and malware. Investigators must introduce equally sophisticated automated tools to detect and respond to these virtual threats, which requires significant resources and expertise.[16]

i) Resources
Cybercrime investigations require substantial resources, including the requirement of skilled personnel, advanced technology, and financial support. Many law enforcement agencies, especially in developing countries, lack the necessary resources to conduct effective investigations. This resource gap frequently results in delayed or incomplete investigations.

j) Speed of Data Exchange Processes
The rapid exchange of data over the internet means that cybercriminals can swiftly move or delete evidence. Investigators should act swiftly to secure data before it is lost. However, the legal and technical measures requires to obtain and preserve data which results in lag behind the speed at which cybercrimes occur today.

For instance the exchange of "child pornography". Prior, physical copies of such material were handed over or transported, giving law enforcement opportunities to intercept and investigate. However, with the internet, this process has changed drastically. Offenders can now exchange videos instantly online, eliminating the need for physical transportation. This makes it much harder for law enforcement to track and stop these crimes.

Tools like "quick freeze procedures" and 24/7[17] network points help speed up cybercrime investigations.[18]

2.3.2 Legal Challenges

a) Challenges in Drafting National Criminal Laws
Updating national laws to address new forms of online cybercrime takes time, and many countries are still working on it. Existing laws need to be reviewed and revised to include modern crimes. For example, digital information (like electronic signatures) should be treated with the same legal weight as traditional documents (like handwritten signatures or printed papers).[19]

Updating laws to address these new crimes takes time, and many countries are still catching up. Key steps include:

- Recognizing new abuses of technology.
- Identifying gaps in existing laws.
- Drafting new legislation to address these gaps.

International cooperation is crucial because cybercrime often crosses borders. Without harmonized laws, fighting transnational cybercrime becomes difficult.

b) New Offences
Many cybercrimes are traditional crimes adapted to the digital world. For example- Fraud can happen via email instead of letters. If fraud is already illegal, existing laws may apply. However, some crimes, like manipulating computer systems, require new laws.

New types of cybercrime, such as theft of virtual currencies in online games, are emerging. These crimes may not be covered by existing laws, creating "safe havens" for offenders.

c) Need for New Investigative Tools
Cybercriminals use technology to commit crimes, so law enforcement needs advanced tools to investigate. However, some tools, like data retention, can infringe on the privacy of innocent users. Balancing effective investigation with protecting rights is a ongoing challenge.

d) Handling Digital Evidence
Digital evidence is crucial in cybercrime cases but comes with unique challenges. It is fragile and can be easily altered or deleted. [20]New technologies, like cloud computing, mean data may be stored abroad, making it harder to access. The process of handling digital evidence involves:

- Identifying relevant evidence.
- Collecting and preserving it carefully.
- Analysing the data.
- Presenting it in court.

Computer forensics plays a key role in analysing digital evidence[21]. Automated tools, like hash-value[22] searches for illegal images, help manage the growing volume of data.

4. India's Stand on the Second Additional Protocol to the Budapest Convention

4.1 Reasons for Denial

India has constantly refrained from becoming a party to the "Budapest Convention and its additional protocols". The main reasons for India's denial are the following[23]-

[16] "Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25."
[17] "The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country".
[18] The word "quick freeze" is used to describe: the immediate preservation of data on request of law-enforcement agencies.
[19] "Article 37 - Traffic and billing data 1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection"
[20] Moore, "To View or Not to View: Examining from Plain View Doctrine and Digital Evidences", *29 Am. J. Crim. Just. 58 (2004).*
[21] Frank G., *Electronic-Evidences and the Laws*, 6 Info. Sys. The Frontier 162 (2006).
[22] Anthony T. Vacca, "Computer based Forensics: Computer Crime Scenes Investigation", *48* (2d ed. 2004)
[23] D. Mohapatra, Cyber Security and Legal Frameworks in India, in Cross Industry Application of Cyber Security Framework 91, 91–

1) India has shown concerns over the potential infringement on its sovereignty by the cross-border flow of data without the explicit consent of the country irrespective of where the data is stored.
2) India argues that the protocol was drafted without the participation of many Non-European countries, including India which undermines the legitimacy of the treaty from India's perspective
3) India is concerned that the protocol could compromise the privacy and security of its citizen's data.
4) India believes that its own domestic legislative framework such as IT Act, 2000 and the proposed DPDP Act, 2023 can address cybercrime effectively without relying on international treaties.
5) India prefers a UN- based convention on cybercrime over the Budapest Convention

4.2 Admissibility of Electronic Records Under Indian Laws

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) governs the "admissibility of electronic records in legal proceedings". S. 63 of the BSA establishes that electronic records, including information printed on paper, stored in optical or magnetic media or recorded in semiconductor memory are deemed documents and are admissible as evidence withput requiring production of the original, provided that the device is regularly used, updated and properly functioning.

A certificate must accompany the electronic record, identifying record, describing its production process and it should be signed by a person in charge of the device or an expert.

The SC in the case of **Navjot Sandhu Case**[24] allowed secondary evidence of electronic records without strict compliance with S.65B of the IEA, provided the records were certified by a responsible official.

In the case of Anvar P.V. vs. P.K. Basheer[25] the Court held that electronic records as secondary evidence are inadmissible unless the conditions of Section 65B are satisfied.

S. 66 & 73 of the BSA talks about proof of electronic and digital signature respectively. S. 87 of the BSA creates a presumption that the information listed in an Electronic Signature Certificate is correct. S. 90 of the BSA provides that court has to presume that electrnic message's content is accurate as it was input for transmission. S. 93 of the BSA creates a presumption as to electronic records of 5 years old.

4.3 Investigation and Trial through electronic means under Bharatiya Nagarik Suraksha Sanhitha, 2023

S. 532 OF BNSS permits trials, inquiries, and proceedings, including summons, warrant, issuance, evidence recording and appellate proceedings, to be conducted electronically using audio-video communication.

S. 2 of BNSS defines "audio-video electronic" means as communication devices used for video conferencing, recording evidence and other legal proceeding.

S. 173 of BNSS permits cognizable offence reports via electronic means, requiring a signed record within 3 days.

S. 105 of BNSS provides that search and seizure processes must be recorded through audio-video means, preferably using cell-phones and the same shall be forwarded to judicial magistrate without delay.

5. Different Countries Stand on the 2nd Additional Protocol

5.1 European Union (EU)

The EU along with its member states has been a strong proponent of the "Budapest Convention and its additional protocols". It views the protocol as a strong tool for improving international cooperation in fighting cybercrime, particularly in accessing electronic evidence across borders. The protocol aligns with the EU's GDPR [26]and other cybersecurity directives ensuring privacy safeguards.

In the case of **Google Spain V. AEPD (2014)**[27] also known as the "Right to be forgotten" case, the CJEU examined the admissibility and reliability of digital records. The court held that electronic evidence must be handled in compliance with GDPR laws and must be reliable and verifiable.

5.2 United States

The US has been a big supporter of the Convention and its protocols. It views it as a tool to combat cybercrime and enhance international cooperation.[28] The UN Convention against cybercrime addresses technical and legal challenges by adapting traditional criminal investigation methods to the information and communication technology environment and enhancing international cooperation.

5.3 Russia and China

Like India, Russia and China have not signed the Convention or its protocols. Both countries have expressed concerns over state sovereignty and have opted for a UN- based framework for combating cybercrime.

6. Conclusion & Suggestions for Strengthening the Protocol

The 2nd additional protocol doesn't specify which authority should supervise the function of the contact point in each member state. If a contact point in one member state works by an authority with the power to order data retention, and another contact point in a different member state requests the same , the measures can be implemented immediately.

111 (I.G.I Global 2022), https://doi.org/10.4018/978-1-6684-3448-2.ch005.
[24] 2005 (11) SCC 600
[25] AIR 2015 SUPREME COURT 180
[26] General Data Protection Regulation (GDPR) – Legal Text
[27] https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN
[28] United Nations Convention against Cybercrime

However, the provisions of the 2nd additional protocol are not fully operational because of the pre-existing multilateral or bilateral treaties take precedence over the protocol. In order to make it fully functional it should be signed by many states as possible particularly non- European states.

Here are some recommendations for strengthening the protocol's impact-.

1) Creation of a standard digital protocol for streamlining communication between designated authorities
2) Alignment of domestic data retention laws with the protocol's provisions to ensure uniform application across jurisdictions
3) Encourage non-European states to ratify the protocol to improve its global applicability
4) Ensure that cross-border data access requests are accompanies with oversight mechanisms to prevent misuse of electronic evidence collection
5) Develop encrypted and real-time tracking mechanisms for evidence requests to ensure efficiency and transparency
6) Conduct regular training programs for law enforcement and cybercrime investigators on handling electronic evidence
7) Establish an independent monitoring authority to assess the protocol's implementation and address emerging challenges

References

[1] "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.
[2] Regarding the necessary steps to improve cybersecurity, see: World Information Society Report,http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.
[3] "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/
[4] Long, Johnny, Skoudis, David, & van Eijkelenborg, Rik, *Google Hacking for Penetration Testers* (2005); Dornfest, Rael, Bausch, Jesse, & Calishain, Tara, *Google Hacks: Tips & Tools for Finding and Using the World's Information* (2006) (accessed Feb. 25, 2025).
[5] Moore, To View or Not to View: Examining from Plain View Doctrine and Digital Evidences*, 29 Am. J. Crim. Just. 58 (2004).*
[6] Frank G., *Electronic Evidences and the Laws*, 6 Info. Sys. The Frontier 162 (2006).
[7] Anthony T. Vacca, "Computer based Forensics: Computer Crime Scenes Investigation*", 48* (2d ed. 2004)
[8] D. Mohapatra, Cyber Security and Legal Frameworks in India, in Cross Industry Application of Cyber Security Framework 91, 91–111 (I.G.I Global 2022), https://doi.org/10.4018/978-1-6684-3448-2.ch005.
[9] *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;
[10] *Beales*, "Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging", 2004, page 9, available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf
[11] Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47.
[12] "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/
[13] Long, Johnny, Skoudis, David, & van Eijkelenborg, Rik, *Google Hacking for Penetration Testers* (2005); Dornfest, Rael, Bausch, Jesse, & Calishain, Tara, *Google Hacks: Tips & Tools for Finding and Using the World's Information* (2006) (accessed Feb. 25, 2025).