AN IN-DEPTH STUDY OF THE BUDAPEST CONVENTION ON CYBERCRIME

*By **Rakshita Mathur***

4th Year BALLB Student, Guru Gobind Singh Indraprastha University, Delhi, India

ABSTRACT

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty aimed at combating computer and Internet crime (cybercrime) through the improvement of investigative methods, harmonisation of national laws, and increased international cooperation.

"The Committee of Ministers of the Council of Europe accepted the Convention and its Explanatory Report" on November 8, 2001, at its 109th Session. It was made available for signature in Budapest on November 23, 2001, and it became operative on July 1, 2004. As of April 2023, 68 states had ratified the convention, with two (South Africa and Ireland) having signed it but not yet done so.

The preamble outlines its main goal, which is to pursue a common criminal strategy aimed at safeguarding society from cybercrime, particularly through the creation of appropriate legislation and promotion.

It has been more than 40 years since cybercrime first appeared. The Council of Europe has been tackling this issue from a criminal law perspective since the mid-1980s. Since then, information and communication technology, or ICT, has completely changed societies everywhere. Furthermore, they are now far more vulnerable to security risks like cybercrime.

India is thought to be in the process of considering whether or not to become a party to this convention. India has not yet joined the Agreement because it is an emerging power in the twenty-first century and believes that it should have autonomy over its own information

technology laws and regulations. We will learn in the next years the course of action India will choose, as well as the role this Convention will play in that decision.

INTRODUCTION

The first international treaty aimed at combating computer and Internet crime (cybercrime) through the improvement of investigative methods, harmonisation of national laws, and increased international cooperation is the Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention.

"With the active participation of Canada, Japan, the Philippines, South Africa, and the United States as observer states, it was drafted by the Council of Europe in Strasbourg, France."[i]

On November 8, 2001, during its 109th Session, "the Committee of Ministers of the Council of Europe accepted the Convention and its Explanatory Report. On November 23, 2001"[ii], it was made available for signing in Budapest, and on July 1, 2004, it came into effect. Two states (South Africa and Ireland) have signed the convention but not ratified it, leaving 68 states that have done so as of April 2023.

Due to their lack of involvement in the Convention's formulation, significant nations like India have refused to ratify it after it came into effect. Russia has consistently declined to assist in law enforcement investigations pertaining to cybercrime and "opposes the Convention, claiming that its acceptance would violate Russian sovereignty. It is the first legally-binding multilateral measure to control cybercrime.

Due to an increase in cybercrime, India has been reevaluating its position on the Convention since 2018"[iii], however worries about sharing data with foreign agencies still exist.

The Convention on Cybercrime's Additional Protocol went into effect on March 1, 2006.

States that have accepted the additional protocol must make it illegal to disseminate racist and xenophobic content online as well as to make threats or insults with racist or xenophobic intent.

An alternative cybercrime pact is being drafted by the UN.

OBJECTIVES

The Convention, which addresses copyright infringements, computer-related fraud, child pornography, hate crimes, and breaches of network security, is the first international pact covering crimes perpetrated via the Internet and other computer networks. It also includes a number of procedures and powers, like authorised interception and computer network searches.

Its fundamental objective, put out in the preamble, is to pursue a shared criminal strategy intended at the protection of society against cybercrime, especially by establishing suitable legislation and promoting.

AGREEMENT

Over 40 years have passed since the advent of cybercrime. Since the middle of the 1980s, the Council of Europe has been addressing this issue from a criminal law standpoint. The problem had grown significant enough by 2001 to require a legally enforceable international treaty. The Convention on Cybercrime, which was negotiated by the Council of Europe's member states as well as by Canada, Japan, South Africa, and the United States of America, was made available for signature in November 2001 in Budapest, Hungary.

Information and communication technology (ICT) have since revolutionised society all over the world. Additionally, they have greatly increased their susceptibility to security threats like cybercrime.

A COMMON STANDARD

All things "cyber" have become too significant, even while it is acknowledged that we need to improve security, confidence, and trust in ICT as well as uphold the rule of law and the protection of human rights in cyberspace. It is becoming harder to come to an international agreement on common solutions when they affect both national (security) interests of States and fundamental rights of persons.

The most logical strategy to resolve this conundrum is to concentrate on widely accepted methods, such capacity building, and on shared "standards that are already in place and operational, like the Budapest Convention on Cybercrime.The Budapest Convention is a treaty on criminal justice that gives states the following benefits: (i) criminalization of a list of computer-related attacks; (ii) procedural legal tools to improve the effectiveness of cybercrime investigations and the securing of electronic evidence related to any crime, while maintaining protections for the rule of law; and (iii) international police and judicial cooperation on cybercrime and e-evidence."[iv]

Any State willing to cooperate and put it into effect is welcome to join. Fifty States were Parties (European countries as well as Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the USA) by November 2016, which also happened to be the Convention's 15th anniversary. It had been signed by 17 more people from all around the world, or they had been invited to join.

IMPLEMENTATION

Together with ten international organisations (including the UN Office on Drugs and Crime, the European Union, INTERPOL, the Organisation of American States, the Commonwealth Secretariat, and the International Telecommunication Union), these 67 states currently take part in the Cybercrime Convention Committee as members or observers. This Committee updates the Convention and evaluates how well the Parties are implementing it. The current focus of efforts is on finding solutions for law enforcement's access to cloud-based electronic evidence.

CAPACITY BUILDING

It is no longer news that capacity building is important when it comes to cybersecurity and cybercrime. For many years, appeals have been made internationally for technology support to strengthen criminal justice systems' ability to combat cybercrime. After the Budapest Convention on Cybercrime was adopted in 2001, the Council of Europe started helping nations

implement the convention, initially in Europe and then, starting in 2006, in other parts of the world, frequently in collaboration with the European Union.

But 2013, that was a whole other level of difficulty. In February 2013, the European Union in its Cybersecurity Strategy and the United Nations Intergovernmental Expert Group on Cybercrime both emphasised the need for a comprehensive agreement on capacity building.

The Global Cyber Space Conference in Seoul, Korea, in October 2013 focused on it. Using this momentum as a springboard, the European Union and the Council of Europe swiftly signed an agreement to collaborate on the "Global Action on Cybercrime" (GLACY) project the same week. At the same time, the Council of Europe resolved to open a Cybercrime Programme Office (C-PROC) in Bucharest, Romania, to support global capacity building.

A further logical outcome was the establishment of the Global Forum on Cyber Expertise during the ensuing Global Cyber Space Conference (Netherlands, April 2015).

By August 2016, C-PROC was in charge of a number of projects, some of which were in collaboration with the European Union and covered the Eastern Partnership region, which includes Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine, as well as South-Eastern Europe and Turkey (the project "iPROCEEDS" focuses on online crime proceeds).

“More broadly, the "Global Action on Cybercrime" project (GLACY) supports Senegal, Mauritius, Morocco, the Philippines, South Africa, Sri Lanka, and Tonga. These nations are prioritised because of their political dedication to putting the Budapest Convention into effect. while part of the new joint EU-CoE initiative "Global Action on Cybercrime Extended" (GLACY+), which runs from 2016 to 2020, some of these nations will be able to share their experience within their respective regions, while GLACY ends in October 2016.”[v]

ACCESS TO EVIDENCE IN CLOUD

It goes without saying that clarifying what behaviour qualifies as cybercrime under criminal law is crucial. This is reflected in Articles 2 (illegal access to a computer system) through 12 (corporate liability) of the Budapest Convention. In order to demonstrate how these provisions address issues like botnets, distributed denial of service assaults, and identity theft that weren't

even a thing when the Cybercrime Convention was formed, the Cybercrime Convention Committee has recently issued a number of guidance notes. The Committee is presently evaluating the degree to which parties have implemented sanctions and other measures that are suitable, reasonable, and deterrent in accordance with Article 13. In terms of substantive criminal law, the Convention is still relevant.

Given the limitations of the MLA process, which is typically intended to protect both the rights of individuals and the interests of the states in which evidence is located, the question of procedural law powers to secure e-evidence and, by extension, efficient access to evidence in a transnational and cloud context is a difficult challenge.

JURISDICTION

"Section 3 – Jurisdiction Article 22 –

Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory;

or b on board a ship flying the flag of that Party;

or c on board an aircraft registered under the laws of that Party;

or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged

offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[vi]

INDIA AND THE BUDAPEST CONVENTION

India and the Council of Europe worked together to modify the Information Technology Act of India in 2007 and 2008. With these changes, India's legal system now mostly complies with the Budapest Convention.

India has not yet ratified the Budapest Convention, despite the fact that membership has more than doubled since then. The causes are not totally evident. Several stakeholders have expressed the following concerns:

1. Participation

The fact that India shouldn't sign the Convention because it wasn't involved in its negotiation. It goes without saying that India would have preferred to have been involved in the original treaty's negotiations. This is not an Indian-only issue. However, other states realised that joining it would be beneficial and would offset this worry. They can now actively take part in the treaty's further development, including any potential negotiations for new protocols. Similar decisions have been made by India on two other Council of Europe treaties that it did not negotiate: the one on the transfer of sentenced individuals (which it requested membership to in 2016) and the other on international cooperation in tax affairs, to which it became a party in 2012.

2. Infringement on Sovereignty of Nations

Article 32b of the Budapest Convention infringes on state sovereignty by enabling transborder data access. "A Guidance Note issued in 2014 by the Cybercrime Convention Committee confirmed, after careful examination, the narrow meaning of Article 32b."[vii] The Indian government was then criticised in certain sectors for believing that Article 32 was excessively restrictive and that further choices would be required.

3. Lack of Checks & Balances on the Convention

There are reasons to refuse to comply, the MLA regime of the Convention is ineffective, or "the promise of cooperation not firm enough." It's true that the Cybercrime Convention Committee has determined that, even though parties' MLA levels are constantly rising, the procedure as a whole need to be made more effective. The recommendations provided by the Cloud Evidence Group and a set of recommendations that were accepted in 2014 are being followed in order to address this issue. The standards, follow-up, and capacity-building triangle that makes up the Convention's "algorithm" enables it to remedy potential flaws. However, one should maintain realism and refrain from expecting a single treaty to address every potential issue. India is a party to other international treaties; therefore, it would not anticipate this from them.

4. Addressal of State-to-State Relations

Since it is a convention on criminal justice, it does not apply to state actors, and some of the states that account for the majority of attacks against India have not ratified it. "It is a criminal justice treaty, after all, and other forums, like the UN GGE, are more suited to discuss state-to-state relations."[viii]

5. International Treaty to be Resorted to

India ought to advocate for a UN treaty. The intended scope of this plan, which appears to be popular in the BRICS setting, is still unknown. Is it designed to address state-to-state interactions, international security issues, criminal justice, or all of these - Considering what has happened since 1990, it seems improbable that a legally binding UN treaty will be available anytime nearby. Cybercrime, meantime, is increasing daily.

CONCLUSION

Over the course of the 21st century, various laws have been made with regards to information technology. The Budapest Convention on Cybercrime has been one such Agreement. However, being one of the first such documents, it has provided a comprehensive framework for the formation of the laws in national legal rules and regulations of several countries.

Other than the original signatories, the Convention has grown leaps and bounds in the past few decades. It has influenced countries that originally signed and even those nation states which joined later. India, too has been influenced by the Budapest Convention. However, it has also been of vast significance in making, amending and following regulations in stark contrast to the Budapest Convention. In other words, the Indian legal system has learnt and implemented laws that are suited to India and learnt from the drawbacks of the Budapest Convention.

Currently, India is seen to be in a mode of contemplation so as to figure out if they would like to be a party to this Convention. Since India is a rising power of the 21st century, have autonomy over own information technological laws and changes is something that suits India due to which India has not yet signed the Agreement. In the next few years, we shall find out the course of action India will hoose and the position of this Convention in such a choice.

ENDNOTES

[i] Clough, Jonathan, A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. P. – 2, Monash University Law Review (2014).
[ii] Ibid
[iii] Juneidi, Salaheddin, P. – 1, Council of Europe Convention on Cyber Crime (2002).
[iv] Campina, Ana & Rodrigues, Carlos. 1. 112. Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation (2022).
[v] Wicki-Birchler, David. 1. 63-72. 10.1365/s43439-020-00012-5. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime. International Cybersecurity Law Review Vol. I. (2020)
vi Council of Europe, Convention on Cybercrime, 23 November 2001.

[vii] Tapia, Johan. 10.13140/RG.2.2.12758.32323.. The Budapest Convention on Cybercrime, ORCID. (2022)
[viii] Ibid