The **Convention on Cybercrime**, also known as the **Budapest Convention on Cybercrime** or the **Budapest Convention**, is the first international treaty seeking to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, the Philippines, South Africa and the United States.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004.

As of October 2022, 67 states have ratified the convention, while a further two states (Ireland and South Africa) have signed the convention but not ratified it.

Since it entered into force, important countries like Brazil and India have declined to adopt the Convention on the grounds that they did not participate in its drafting. Russia opposes the Convention, stating that adoption would violate Russian sovereignty, and has usually refused to cooperate in law enforcement investigations relating to cybercrime. It is the first multilateral legally binding instrument to regulate cybercrime.[5] Since 2018, India has been reconsidering its stand on the Convention after a surge in cybercrime, though concerns about sharing data with foreign agencies remain.[6]

The United Nations is developing an alternative treaty on cybercrime.[8]

Objectives

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security.[9] It also contains a series of powers and procedures such as the search of computer networks and lawful interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering.

The Convention aims principally at:

- Harmonizing the domestic criminal substantive law elements of offenses and connected provisions in the area of cyber-crime
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form
- Setting up a fast and effective regime of international cooperation

The following offenses are defined by the Convention:

illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighbouring rights.

It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans-border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and

provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties. Further, as conditions and safeguards, the Convention requires the provision for adequate protection of human rights and liberties, including rights arising pursuant to obligations under European Convention on Human Rights, International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and shall incorporate the principle of proportionality.[10]

The Convention is the product of four years of work by European and international experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offense, similar to Criminal Libel laws. Currently, cyber terrorism is also studied in the framework of the Convention.

Agreement by the United States

Its ratification by the United States Senate by unanimous consent in August 2006 was both praised and condemned.[11] The United States became the 16th nation to ratify the convention.[12][13] The Convention entered into force in the United States on 1 January 2007.

Senate Majority Leader Bill Frist said: "While balancing civil liberty and privacy concerns, this treaty encourages the sharing of critical electronic evidence among foreign countries so that law enforcement can more effectively investigate and combat these crimes".[14]

The Electronic Privacy Information Center said:

The Convention includes a list of crimes that each signatory state must transpose into their own law. It requires the criminalization of such activities as hacking (including the production, sale, or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also requires each signatory state to implement certain procedural mechanisms within their laws. For example, law enforcement authorities must be granted the power to compel an Internet service provider to monitor a person's activities online in real time. Finally, the Convention requires signatory states to provide international cooperation to the widest extent possible for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their mutual assistance requests.[15]

Although a common legal framework would eliminate jurisdictional hurdles to facilitate the law enforcement of borderless cybercrimes, a complete realization of a common legal framework may not be possible. Transposing Convention provisions into domestic law is difficult especially if it requires the incorporation of substantive expansions that run counter to constitutional principles. For instance, the United States may not be able to criminalize all the offenses relating to child pornography that are stated in the Convention, specifically the ban on virtual child pornography, because of its First Amendment's free speech principles. Under Article 9(2)(c) of the Convention, a ban on child pornography includes any "realistic images representing a minor engaged in sexually explicit conduct". According to the Convention, the United States would have to adopt this ban on virtual child pornography as well, however, the U.S. Supreme Court, in *Ashcroft v. Free Speech Coalition*, struck down as unconstitutional a provision of the CPPA that prohibited "any visual depiction" that "is, or appears to be, of a minor engaging in sexually explicit conduct". In response to the rejection, the U.S. Congress enacted the PROTECT Act to amend the provision, limiting the ban to any visual depiction "that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct" (18 U.S.C. § 2252(B)(b)).

Accession by other non–Council of Europe states

The Convention was signed by Canada, Japan, the United States, and South Africa on 23 November 2001, in Budapest. As of October 2022, the non–Council of Europe states that have ratified the treaty are Argentina, Australia, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel,
Japan, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, the Philippines, Senegal, Sri Lanka, Tonga and the United States.

Although Egypt has not signed off on the Convention, Egyptian President el-Sisi's government in 2018 has legislated two major computer-crime related laws. Targeting social networking service such as Facebook and Twitter, the legislation criminalizes fake news and terrorism, setting a flag on accounts which carry more than 5,000 subscribers or followers. The early legislation had been criticized by Amnesty International, thus websites can appeal to the courts within 7 days of blacklisting.

In fact India too "was reconsidering its position on becoming a member of the Budapest Convention because of the surge in cybercrime, especially after a push for digital India.