Protecting human rights, democracy and the rule of law in the digital environment

COUNCIL OF EUROPE

# ACTION AGAINST CYBERCRIME

www.coe.int/**cybercrime**

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

# ACTION AGAINST CYBERCRIME

## The convention on cybercrime

The Convention on Cybercrime known also as the "Budapest Convention" is regarded as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to date. It serves as a guideline for any country developing domestic legislation on cybercrime and as a framework for international co-operation between State Parties to this treaty.

**The Budapest Convention provides fo**r:

- the criminalisation of conducts;
- procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime;
- and for efficient international co-operation.

The Convention is supplemented by a **First Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature** committed through computer systems (ETS 189) and a Second Additional Protocol on enhanced international co-operation and disclosure of electronic evidence (CETS 224).

The treaty is open for accession by any country. In fact, under Article 37 any State can become a Party by "accession" if the State is prepared to implement the provisions of this treaty. In addition, a State can become a Party by "ratification": whether becoming a Party through ratification or accession, the end-result is the same. Parties to the Convention can also become Parties to the two Protocols without the need for a further request for accession.

By June 2024, 75 States were Parties to the Convention, 2 countries had signed it and 16 countries had been invited to accede. These States participate as members (Parties) or observers (signatories or invitees) in the Cybercrime Convention Committee (T-CY).

**T-CY (Cybercrime Convention Committee)** among other things assesses implementation of the Convention by the Parties, adopts Guidance Notes or prepares additional legal instruments.

Capacity building programmes – managed by the specialised **Cybercrime Programme Office** of the Council of Europe (C-PROC) in Romania – help countries worldwide to build the necessary capacities to implement the Budapest Convention, its protocols or to follow up to recommendations of the Cybercrime Convention Committee.

## Benefits for Parties

Any country may make use of the Convention on Cybercrime as a guideline, check list or model law, and a large number already makes use of this opportunity. However, becoming a Party to this treaty entails additional advantages since the Convention provides a **legal framework for international co-operation** not only with respect to cybercrime, but with respect to any crime involving electronic evidence; Parties to the Convention can sign and ratify the **Second Additional Protocol to the Budapest Convention, which provides additional and expedited tools for enhanced co-operation and disclosure of electronic evidence**; Parties are members of the T-CY and share information and experience, assess implementation of the Convention, or interpret the Convention through Guidance Notes; every Member State is able to participate in the negotiation of future instruments and the further evolution of the Convention; Parties to the Convention engage with each other in trusted and efficient co-operation.

Morover, **private sector entities** as well are more likely to co-operate with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime

and electronic evidence in place, including the safeguards of Article 15.

Additionally, States requesting accession or having acceded may become priority countries for **capacity building programmes**. Such technical assistance is to facilitate full implementation of the Convention and to enhance the ability to co-operate internationally.

## The First Additional Protocol

The First Additional Protocol covering the **criminalisation of acts of a racist and xenophobic nature committed through computer systems** (ETS189) entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international co-operation set out in the Convention in this area.

Benefits for signatories are numerous:

- **A strong legal framework** for countering xenophobia and racism in cyberspace by providing a clear set of guidelines for the investigation and prosecution of these crimes.
- **Enhanced international co-operation** in the investigation and prosecution of crimes relates to xenophobia and racism online, which is particularly important given the cross-border nature of many of these offences.
- **Increased protection** for victims related to xenophobia and racism online, and effective measures to ensure that they are able to access justice and receive support.
- **Improved awareness** and education about the harms of xenophobic and racist acts committed through computer systems. Morover, The Protocol encourages the implemen-tation of measures to prevent these forms of hate.

The First Additional Protocol was opened for signature on 23 January 2023. As of June 2024, 36 States were Parties and a further 10 had signed the First Protocol.

## The Second Additional Protocol

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions. As a response, the Second Additional Protocol to the Convention on Cybercrime (CETS 224) provides a **legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information**, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

Key features of the Protocol are, among others, direct request to registrars in other jurisdictions to obtain domain name registration information; direct co-operation with service providers in other jurisdictions to obtain subscriber information; government-to-government co-operation and expeditious co-operation in emergency situations; joint investigation teams and joint investigations.

The Second Additional Protocol was opened for signature on 12 May 2022. As of June 2024, 46 States had signed the Second Protocol and 2 States had ratified it.

## The Convention on Cybercrime

known also as the "Budapest Convention" is regarded as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to date.

The Convention is supplemented by a First Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) and a Second Additional Protocol on enhanced international co-operation and disclosure of electronic evidence (CETS 224).

COUNCIL OF EUROPE

**@ DIGITAL GOVERNANCE**

Protecting human rights, democracy and the rule of law in the digital environment

Social Media

Council of Europe
# Digital Governance

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy, and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE