

SUMMARIES OF THE COUNCIL OF EUROPE TREATIES

The summaries available hereunder are designed to meet a practical need, that of supplying the public at large with concise descriptions of the Council of Europe treaties. The summaries are necessarily short and can therefore only give a first introduction to the main features of each treaty.

Subject-matter: **CYBERCRIME**

Convention on Cybercrime ([ETS No. 185](#)), open for signature, in Budapest, on 23 November 2001.

Entry into force: 1 July 2004.

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 and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and 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 international co-operation.

* * *

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ([ETS No. 189](#)), open for signature, in Strasbourg, on 28 January 2003.

Entry into force: 1 March 2006.

This Protocol entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation 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 cooperation set out in the Convention (ETS No. 185) in this area.

* * *

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse ([CETS No. 201](#)), open for signature, in Lanzarote, on 25 October 2007.

Entry into force: 1 July 2010.

This Convention is the first instrument to establish the various forms of sexual abuse of children as criminal offences, including such abuse committed in the home or family, with the use of force, coercion or threats.

Preventive measures outlined in the Convention include the screening, recruitment and training of people working in contact with children, making children aware of the risks and teaching them to protect themselves, as well as monitoring measures for offenders and potential offenders.

The Convention also establishes programmes to support victims, encourages people to report suspected sexual exploitation and abuse, and sets up telephone and internet helplines for children. It also ensures that certain types of conduct are classified as criminal offences, such as engaging in sexual activities with a child below the legal age and child prostitution and pornography. The Convention also criminalises the solicitation of children for sexual purposes ("grooming") and "sex tourism".

With the aim of combating child sex tourism, the Convention establishes that individuals can be prosecuted for some offences even when the act is committed abroad. The new legal tool also ensures that child victims are protected during judicial proceedings, for example with regard to their identity and privacy.

* * *

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence ([CETS No. 224](#)), open for signature, in Strasbourg, on 12 May 2022.

Entry into force: The Protocol will enter into force following five ratifications.

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 Protocol 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.