Budapest Convention on Cybercrime – Treaty 185

The Convention is the first internationally binding treaty on crimes committed on the Internet and other computer network, dealing particularly with infringements of copyright, computer related fraud, child pornography and violations of network security. It also contains several powers and procedures such as the search of computer networks and interception. [1]

The Convention serves as a guideline for any country developing a comprehensive national legislation against cybercrime and as a framework for international cooperation between Parties to the Convention. The Convention has been supplemented by Protocol on Xenophobia and Racism committed through computer systems.[2]

The Council of Europe have set up a dedicated website with resources and guidance to assist. [3]

Aim

The aim of the legislation was to provide a harmonised approach to tackling cybercrime, to date, the Convention has been signed by and entered into force by 61 nations in Europe and around the world. The harmonisation of this legislation is crucial as it reduces the incidence of "safe havens" but more importantly to facilitate the effective cooperation between global law enforcement agencies.

Offences

The Convention sets out four broad categories of offences which are set out in Chapter 2 article 1 - 10 of the Convention:

1) Offences against confidentiality, integrity and availability of computer data systems;
2) Computer related offences such as fraud and forgery;
3) Content related offences – child pornography; and
4) Criminal copyright infringement.

Chapter 2 Article 11 and 12 set out liability for:

1) Attempt and aiding and abetting; and
2) Corporate liability.

Chapter 2 Article 13 sets out that offences in articles 2 through 11 are punishable by proportional justice including potential jail sentence. Article 12 may be punishable by criminal or non-criminal sanctions including monetary.

Notably omissions to offences under the Convention include – identity theft, grooming of children, unsolicited emails or spam and cyberterrorism.

Procedure

Chapter 2 Section 2 addresses the challenges of digital investigation. The Convention sets out the following investigative powers:

1) expedited preservation of stored computer data;
2) expedited preservation and partial disclosure of traffic data which can identity the path through which the communication was transmitted;
3) production order which allows authorities to compel an individual or service provider offering services in its territory to submit subscriber information held relating to their services;

4) search and seizure of stored computer data;
5) real time collection of computer data; and
6) Interception of content data which includes to compel a service provider to collate or cooperate in the collection or recording of data in real time.

A Party to the Convention may establish jurisdiction under the Convention if the offence was committed:

1) in the Party's territory
2) on board a ship flying the flag of the Party
3) on board an aircraft registered under the laws of the Party
4) by one of its nationals, if the offices is punishable under criminal law where is it committed or if the office is committed outside the territorial jurisdiction of any State.

International Co-operation

Chapter 3 of the Convention sets out the principals by which each of the Parties may assist another party with an investigation by mutual assistance. This chapter is of crucial significance where the investigation has a cross border element.

Article 23 sets out the general principle relating to international co-operation stating that Parties shall co-operate with each other "to the widest extent possible".[4] Although a broad definition it is not considered to be an express statement for the principle of reciprocity.

Article 24 sets of the procedure for extradition in relation to criminal offences set out in Articles 2 to 11 of the Convention. The wording of the article states that the offences set out in Articles 2 to 11 shall be deemed to be included in any extradition treaty existing between the Parties. The article goes onto state that if there is not an extradition treaty and extradition is conditional the existence of one then the Convention is the legal basis of the extradition. Further should the Parties not make extradition conditional on the existence of a treaty then they will recognise the offenses as extraditable offences between them.

Articles 27 to 34 sets out the procedures for mutual assistance requests whereby one Party may contact another Party to assist in an investigation. The Chapter mirrors the procedures set out in the Chapter 2 of the Conventions which may be included in the mutual assistance request.

Article 35 sets out the creation of a 24/7 network to ensure that each party has a designated point of contact to provide immediate assistance in an investigation or a criminal offence proceeding within the scope of the Convention and ensure the preservation of electronic data.

1 - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

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

3 - https://www.coe.int/en/web/cybercrime

4 - Convention on Cybercrime found at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561