Additional Articles

Stein Schjolberg
Judge
January 2, 2023

Alternative for article 20
Grooming or procuring of a child for sexual purposes through a computer system

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, through a computer system grooming, making a proposal, procuring or causing a child, to meet, witness, or participate in sexual activities.
(Australia)

Alternative for Article 23
Encouragement of or coercion to suicide

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the encouragement of or coercion to suicide, including of minors, through psychological or other pressure in information and telecommunication networks, including the Internet.
(Brazil)

Cyberattacks on critical communications and information infrastructures

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, cyberattacks against their critical communication and information infrastructures, and any related asset, system, or part thereof, that are essential for the maintenance of vital societal functions such as the health, safety, security, economic, or social well-being of people.
(ITU GCA Guidelines April 22, 2021)

Ransomware attack

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, a ransomware attack when any person modifies or impairs data, malicious software, or malware, or impairs electronic communication to or from a computer, that prevents from accessing computer files, systems, or networks and demands a ransom for their return, or demands payment to do certain things including to undo damage or prevent the publication or exfiltration of data.
(FBI and Australia – Ransomware payments Bill 2021)

Smart technology

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right,

a) taking advantage of security oversights or gaps in the configuration of closed-circuit television, such as security cameras used by private businesses or built-in cameras on baby monitors used in homes and day care centers.
b) exploiting unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting.
c) using home-networking routers, connected multi-media centers, televisions, and appliances with wireless network connections as vectors for malicious e-mail.
d) gaining access to unprotected devices used in home health care, such as those used to collect and transmit personal monitoring data or time-dispense medicines.
e) attacking business-critical devices connected to the Internet, such as the monitoring systems on gas pumps.

(FBI)

Online child sexual abuse and sexual exploitation

1. Each Party shall have a sovereign right to control that no social media information crossing its border includes online child sexual abuse and sexual exploitation of children. A State enjoys sovereign authority with regard to the control of online child sexual abuse of international activities located within its territory, subject to its international legal obligations. It must be established minimum rules concerning the prevention of international websites containing online child sexual abuse, including blocking technology, filtering technology, or similar technology as measures aimed at stopping the distribution on the national territory.
2. Each Party shall develop appropriate legal measures to implement effective programs to prevent or prohibit the dissemination of online materials relating to child sexual abuse and exploitation, including taking preventive actions to detect, disrupt, and dismantle networks, organizations, or structures used for the production and/or distribution of online materials relating to child sexual abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims.

(ITU GCA Guidelines April 22, 2021)

Sexual extortion

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, sexual extortion when obtaining of money or sexual favors or perform sexual acts from someone by threatening to reveal or publish intimate pictures of them, or other evidence of their sexual activity or sexual information about them.

Grooming or procuring of a child for sexual purposes through a computer system

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, through a computer system grooming, making a proposal, procuring or causing a child, to meet, witness, or participate in sexual activities.

(Australia)

Nonconsensual dissemination of intimate images

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right,

a) knowingly publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct;
b) the publishing, distributing, transmitting, selling, making available or advertising an intimate image of a person is done with the intention to harass or cause harm to the person depicted in the image;
(CARICOM)

Encouragement of or coercion to suicide

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the encouragement of or coercion to suicide, including of minors, through psychological or other pressure in information and telecommunication networks, including the Internet.
(Brazil)

Identity Theft

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, and be applied to any person who illicitly gains possession of another person's proof of identity or uses another person's identity or an identity that is easily mistakable for the identity of another person, with intent to

a. make an illicit gain for himself/herself or for another person, or
b. cause another person loss or inconvenience.

(Norway)

Lawful access to the content of communications

In September 2014 Apple and Google declared that their mobile devices shall include the use of encryption. The decision was made without consent from the government in USA. After the decision IT companies such as Apple introduced an operating system that encrypted virtually everything contained on an iPhone, making their devices completely inaccessible without a passcode.

A growing problem has occurred in many countries on the law enforcements inability to obtain information in investigation, even if they have a court order to do so. Countries want all Internet providers to comply with judges or governments orders when communications are needed for an investigation. It remains a priority for the governments to ensure that law enforcement can obtain critical digital information to protect national security and public safety.

The US Dept. of Justice held on October 4. 2019 the Lawful Access Summit.[1] The theme of the Summit was – *Warrant-proof encryption.* The purpose was to discuss that the tech companies should open their encryption schemes to police investigating crimes, and a problem was emphasized: *Have encryption schemes turned Internet into a lawless space?*

[1] See https://www.justice.gov/olp/lawful-access

The FBI Director Christopher Wray made at the Summit the following statement:
I can tell you that police chief after police chief, sheriff after sheriff, our closest foreign partners and other key professionals are raising this issue with growing concern and urgency. They keep telling us that their work is too often blocked by encryption schemes that don't provide for lawful access. So, while we're big believers in privacy and security, we also have a duty to protect the American people.

Ministers from United States, United Kingdom and Australia sent at the Summit an open letter to Mr. Zuckerberg, Facebook, and included as follows:
We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.
In the response Facebook made a statement that it had no plans to comply.

A recommendation for legal measures on the use of encryption may follow the recommendations that was presented by the Council of Europe in 1995:[2]
Legal measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.

Court Order for lawful access

States shall ensure that a covered entity that receives a court order from a government for information or data, shall provide such information or data to the government in an intelligible format. A covered entity that receives a court order shall be responsible only for providing data in an intelligible format if such data has been made unintelligible by a feature, product, or service owned, controlled, created, or provided, by the covered entity or by a third party on behalf of the covered entity.

A regulation on lawful access to content of communications could include the following Articles:
Article 1
States shall control the use of encryption and consider minimize the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.
Article 2
States shall ensure that end-to-end encryptions are not implemented across messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.
Article 3
States should adopt legislation that would ban strong encryption. If a Court of Law issues an order to render technical assistance or provide decrypted data, the company or individual would be required to do so.

[2] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers at the 543rd meeting of the Ministers Deputies.