Proposal for a United Nations Convention on Cybercrime

by
Judge Stein Schjolberg (Ret.)[1]
Norway

Introduction

A United Nations convention is needed for the global society to achieve standards and norms for security, peace, and justice in cyberspace. Regional and bilateral agreements will not be sufficient. The international law, such as the Geneva Conventions are mainly covering State behaviors.

From the year 2000 United Nations General Assembly adopted several Resolutions and participated in the global development of regulating cyberspace. The global organization of United Nations such as the International Telecommunication Union (ITU)[2] in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna became also leading organizations in the development.

Today the developments of the global IT companies have been so rapid and the impact on the global society so enormous, without developing any international regulations and guidelines for cyberspace. The global private IT companies have now been the leading organizations on global Internet governance, instead of United Nations organizations. A growing problem has occurred in many countries on the law enforcements inability to obtain information in investigations, even if they have a court order to do so. It may be argued that in 2022 globally challenges to the protection of personal data and other data from criminal activities are now coming from the global private IT companies, without any global Internet governance guidelines.

Countries around the world are now realizing that cyberspace must be regulated to protect their sovereignty, national information infrastructures, and its citizens. Searching for a common ground on legal measures, and a common understanding of the need for a dialogue on cybersecurity and cybercrime has been in focus for the leaders and lawmakers in the world.

More than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity on the global level.

Would it be possible to find a global common ground on legal measures in a United Nations convention?

---

[1] Judge Stein Schjolberg has been an international expert on cybercrime for United Nations institutions and many international organizations in more than 40 years. He has written several books and publications on cybercrime.
See his last book (March 2022)
https://www.amazon.com/United-Nations-Internet-Governance-Convention-ebook/dp/B09WM22K3H/ref=sr_1_2?crid=1UFNXV7N0BGBM&keywords=stein+schjolberg&qid=1648458597&sprefix=stein+schjolberg%2Caps%2C243&sr=8-2
See also https://cybercrimelaw.net/Cybercrimelaw.html

[2] See https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

General provisions

The principles of State sovereignty applies in cyberspace.

The principle of State sovereignty applies in cyberspace.
A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.
A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.[3]

It began with the Peace of Westphalia in 1648. It is often argued that the Peace of Westphalia resulted in a general recognition of the exclusive sovereignty of each party over its lands, people, and agents abroad. These Westphalian principles, especially the concept of sovereign states, became central to international law and the prevailing world order. The principle of territorial sovereignty was codified in the Covenant of the League of Nations in 1919, and The Charter of the United Nations reaffirms the principle of territorial integrity in Article 1 and 2.
The UN Group of Government Experts statements in 2013 and 2015 recognized that there is no reason why the principle of sovereignty should not apply in the cyber context as it applies in every other domain of State activity. Every sovereign state is entitled in cyberspace to take what measures it pleases for its own territory and citizens.

Global cybersecurity prevention measures.

(Should be developed by an expert on global cybersecurity prevention measures)

A global approach on main cybersecurity issues should be included as a prevention of cybercrimes and cyberattacks to promote open sharing of knowledge, information, and expertise between all countries.
A convention should give a broad understanding of what kind of concerns shall be addressed and what sort of measures must be taken on global cybersecurity to provide peace, justice, and security in cyberspace.

Lawful access to the content of communications.

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.[4] 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?*

---

[3] See Cambridge University Press https://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf
[4] 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," he said. "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, including: *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.

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 such government in an intelligible format.
States shall ensure that the entity provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.
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.

Editor responsibility

1.Each State shall have a sovereign right to develop laws including legal responsibility for web editors.
2.Web editors are responsible for the content and images used on a website and have the final responsibility for the websites content.
3. Web editors provides liability for providers and users of an "interactive computer service" who publish information provided by third-party users. A provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

International law enforcement

(Should be developed by an expert on INTERPOL global coordination in cybercrime prevention, detection, and investigation, and global public-private partnerships for investigation through INTERPOL)

INTERPOL has since 1981 been the leading international police organization on global prevention, detection, and investigation of cybercrime.

INTERPOL seeks to facilitate global coordination in cybercrime investigation and provide operational support to police across its 195 member countries. It is very important that the investigators of cybercrime may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient cross-border cooperation when cyberattacks involves multiple jurisdictions. INTERPOL has also established a rapid information exchange system for cybercrimes through the global police communications system I-24/7, where INTERPOL collects, stores, analyses, and shares information on cybercrime with all its member countries.

INTERPOL has signed partnership agreements with other global agencies and the private sector. These agreements are part of INTERPOL´s cooperation with global private sector operators to provide support on investigation and capacity building on cybercrime. A global cybercrime convention should include a common understanding of the need for standards on global public-private partnerships for investigation through INTERPOL. A partnership should avoid dealing with classified information to share information and knowledge more freely with the private sector.

Criminalization

Substantive criminal law

Measures on substantive criminal law should be based on the Budapest Convention.

The Budapest Convention on cybercrime was open for signature on November 23. 2001. The Budapest Convention is ratified by 66 States, including 21 States outside Europe, and is signed but not followed by ratification of 2 States (March 2022).[5] Substantive criminal law in the Convention contains of Articles against:
Article 2 – Illegal access;
Article 3 – Illegal interception;
Article 4 – Data interference;
Article 5 – System interference;
Article 6 – Misuse of devices;
Article 7 – Computer-related forgery;
Article 8 – Computer-related fraud;
Article 9 – Offences related to child pornography;
Article 10 – Offences related to infringements of copyright and related rights;

Additional content

Principles on legal measures in the additional content should in a United Nations Convention on Cybercrime include conducts developed by the new technology, after the Council of Europe Convention on Cybercrime was adopted in 2001.

Global cyberattacks on national information infrastructure are one of the most serious national security threats. States shall adopt such legislative and other measures and are encouraged to continue taking appropriate legal measures to protect 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, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

A convention should include special principles for criminal conducts in social networks. The development of unacceptable behaviour in social networks must be followed very closely. Smart technology will change the way people live, interact, and work in the future.

[5] See https://www.coe.int/en/web/cybercrime/the-budapest-convention

Online child sexual abuse and sexual exploitation constitutes serious violations of fundamental rights, in particular the rights of children to the protection and care necessary for their well-being. Serious criminal offences such as sexual abuse and sexual exploitation of children require a comprehensive approach covering the protection of child victims and the prevention of the phenomenon. After the introduction of the global communications in cyberspace and the social media, online child sexual abuses and sexual exploitation has been increasingly spreading to such extent that it requires in 2022 a comprehensive United Nations approach for the prevention of such online abuses.
Each State has a sovereign right to control that no social media information crossing its border and includes online child sexual abuse and sexual exploitation of children.

Procedural measures

Procedural measures should be based on the Budapest Convention Second Additional Protocol.

The Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was adopted on November 17, 2021, on the 20th anniversary of the Budapest Convention.[6] It is recommended to consider adopting the principles on:

- *Procedures enhancing direct cooperation with providers and entities in other Parties.*
- *Procedures enhancing international cooperation between authorities for the disclosure of stored computer data.*
- *Procedures pertaining to emergency mutual assistance.*
- *Procedures pertaining to international cooperation in the absence of applicable international agreements.*
- *Conditions and safeguards.*
  Final provisjons.

Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace are essential for a global investigation and prosecution and should apply on the collection of evidence in electronic form of all criminal offences. Information may be stored in cloud computing anywhere in the world. A global cybercrime convention should ensure that the procedural elements for investigation and prosecution includes measures under international human rights law.

An International Court for Cyberspace

Global regulation should include principles for establishing an International Court for Cyberspace, as a United Nations Court. It is necessary since United States, Russia, and China have not ratified the Rome Statute of the International Criminal Court in The Hague.

The developments of global cyberattacks, against critical information infrastructures of sovereign States should be protected by an International Court under the United Nations. An International Court for Cyberspace is a missing link in the international legal system. It will be of great importance for peace and justice in cyberspace and a signal from the United Nations and the global community that global cyberattacks are not tolerated. An International

[6] See https://www.coe.int/en/web/conventions/new-treaties

Court for cyberspace may be a judicial institution complementary to national criminal jurisdictions.

Establishing an International Court for Cyberspace by the Charter of the United Nations includes that all members of United Nations are parties to the Court Statute. A permanent and independent United Nations Court may serve Cyberspace in a more consistently way and be a judicial institution complementary to national jurisdictions.

Proposal for a United Nations Convention on Cybercrime

(First edition)

Stein Schjolberg
Chief Judge (Ret.)
Norway

Introduction

Recognizing that regulation on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.

Noting that The Council of Europe Convention on Cybercrime was adopted on November 8. 2001 and opened for signature in Budapest November 23, 2001. The Convention is ratified by 66 States (December 2021), including 21 States outside Europe. A 2nd Additional Protocol to the Convention on Cybercrime was approved at a meeting on June 7-9. 2017, and the proposal was adopted by the Council of Europe on November 17, 2021.

Recognizing that the United Nations Congresses on Crime Prevention and Criminal Justice has been organized every fifth year since 2005.

Recalling that the GCA Chairman Report (2008) in International Telecommunication Union (ITU) considered the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, and countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal systems and practice.

Noting that more than 125 countries have signed and/or ratified cybersecurity and cybercrime conventions, declarations, guidelines, or agreements, having resulted in fragmentation and diversity at the international level.

Recalling that the United Nations Office on Drugs and Crime (UNODC) has since 2011 organized Intergovernmental Expert Groups for developing proposals on national and international legal responses to cybercrime.

Noting that the United Nations General Assembly Resolution of December 27. 2019 on Countering the use of information and communications technologies for criminal purposes was adopted by a recorded vote of 79 in favor and 60 against, with 30 abstentions.

Recognizing that searching for a global common ground on legal measures in a United Nations regulation should be a priority.

Noting that States should discuss a common ground on legal measures in a United Nations regulation that may be based on some Articles in the Council of Europe Cybercrime Convention, including additional content. It may also be based on some Articles in *The Second Additional Protocol to the Convention on Cybercrime* (2021), including additional content. Other Articles take into consideration the existing global instruments and efforts to coms.
Noting that the principle of State sovereignty applies in cyberspace.

Chapter 1
State Sovereignty

The principle of State sovereignty applies in cyberspace.
A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.
A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.

Chapter 2.
Global Cybersecurity Prevention Measures

2.1. Preventive measures

Article 2.1.1.
States are encouraged to continue taking appropriate legal measures to protect 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, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

Article 2.1.2.

In collaboration with appropriate partners, States should promote a better understanding of the cybersecurity-related challenges and risks posed by emerging technologies on existing legal measures and facilitate the exchange of case studies and good practices at the national, regional, and international level.

Article 2.1.3.

States are urged to design and develop any appropriate legal measures in accordance with their human rights obligations.

Given the rapid advancements in technology, measures taken by organizations and countries need to evolve to keep pace with the rate of change. This brings new complexities to the challenge of cybersecurity, requiring close examination from a variety of different perspectives.

Chapter 3.
Global Law enforcement

3.1. Investigation measures

INTERPOL shall be the leading international police organization on global prevention, detection, and investigation of cybercrime. INTERPOL facilitates global cooperation and coordination on cybercrime investigation and provide operational support to law enforcements across its 195 member countries.

INTERPOL is committed to be a global coordination body for the prevention, detection, and cooperation of cybercrime for investigative support, field operations, training, and networking. It is very important that the investigators of cybercrime may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient cross-border cooperation when cyberattacks involves multiple jurisdictions.

3.2. Strategies for cooperation and coordination

INTERPOL shall have the following strategies:
1.Enhance international law enforcement cooperation for a timely and effective global response to cybercrime.
2. Reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms in addressing cybercrime.
3. Close gaps and bridge divides in capabilities, capacity and information sharing across the globe to overcome the challenges of investigating cybercrime.

3.3. INTERPOL Public-Private Partnerships

INTERPOL shall sign partnership agreements with other global agencies and the private sector to provide support for investigation and capacity building on cybercrime.
Maximize prevention efforts through Public-Private Partnerships for proactive disruption of cyber threats and their ecosystem.
A partnership should avoid dealing with classified information to share information and knowledge more freely with the private sector.

Chapter 4.
Substantive criminal law

Article 4.1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c. "service provider" means any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Additional content:

Article 4.2. Illegal access

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, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Additional content:

Article 4.3. Illegal interception

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, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Additional content:

Article 4.4. Data interference

1. 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, the damaging, deletion, deterioration, alteration, or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Additional content:

Article 4.5. System interference

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, the serious hindering

without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Additional content:

Article 4.6. Misuse of devices

1.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. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed, or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5,

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this Article.

Additional content:

Article 4.7. Computer-related forgery

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 input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Additional content:

Article 4.8. Computer-related fraud

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 causing of a loss of property to another person by:

a. any input, alteration, deletion, or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Additional content:

Article 4.9. Offences related to combating online child sexual abuse

1.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 following conduct:

a) producing child pornography for the purpose of its distribution through a computer system.
b) offering or making available child pornography through a computer system.
c) distributing or transmitting child pornography through a computer system.
d) procuring child pornography through a computer system for oneself or for another person.
e) possessing child pornography in a computer system or on a computer-data storage medium.

2.For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

f) a minor engaged in sexually explicit conduct.
g) a person appearing to be a minor engaged in sexually explicit conduct.
h) realistic images representing a minor engaged in sexually explicit conduct.

3.For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4.Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Additional content:

Each State 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 international cyber pornography 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 pornography, including blocking technology, filtering technology, or similar technology as measures aimed at stopping the distribution on the national territory.

Appropriate legal measures also need to be taken by all relevant stakeholders to implement effective programmes 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 abuse, and to put in place mechanisms to detect and prosecute offenders while identifying and protecting victims. In this regard, ITU should continue to strengthen the Child Online Protection programmed as a platform to work with partners and stakeholders to promote the exchange of knowledge, information, activities, and outcomes on all aspects including legal measures that can facilitate and support country action on this critical issue.

Article 4.10. Additional Articles

Cyberattacks on critical communications and information infrastructures

States shall adopt such legislative and other measures and are encouraged to continue taking appropriate legal measures to protect 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, and prevent any disruption or destruction that may cause significant impact to, and failure to function of, such critical infrastructures.

Chapter 5
Procedural measures

5.1. Lawful access to content of communications

Article 5.1.1.
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 5.1.2.
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.

5.2. Court Order

Article 5.2.1.
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 such government in an intelligible format.

Article 5.2.2.
States shall ensure that the entity provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.

Article 5.2.3.
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.

5.3. Jurisdiction

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Chapter 4 of this Convention, when the offence is committed:
a. in its territory; or
b. on board a ship flying the flag of that Party; or
c. on board an aircraft registered under the laws of that Party; or
d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this Article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Chapter 4 of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 5.4. Additional Chapters

5.4.1. Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence
It is recommended to consider adopting the principles on:

- *Procedures enhancing direct cooperation with providers and entities in other Parties.*
- *Procedures enhancing international cooperation between authorities for the disclosure of stored computer data.*
- *Procedures pertaining to emergency mutual assistance.*
- *Procedures pertaining to international cooperation in the absence of applicable international agreements.*
- *Conditions and safeguards.*
  Final provisjons.

5.5. Editor responsibility
1.Each State shall have a sovereign right to develop laws including legal responsibility for web editors.
2.Web editors are responsible for the content and images used on a website and have the final responsibility for the websites content.

3. Web editors provides liability for providers and users of an "interactive computer service" who publish information provided by third-party users. A provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.