Lund University Summer School in Digital Human Rights
Lund, Sweden, 22 – 26 June 2026

Cybercrime (part 1): International legal frameworks

Alexander Seger
Strasbourg, France
former Executive Secretary, Cybercrime Convention Committee, Council of Europe

Cybercrime (part 2): Criminal justice action on cybercrime: Human rights implications

Agenda

- Introduction: Problems to be addressed by international frameworks
- International treaties on cybercrime:
  - "Budapest" Convention (2001) and protocols (2003 and 2022) (Council of Europe)
  - "Hanoi" Convention (United Nations)
  - Comparing these treaties
- Conclusions

Introduction — Problems that international legal frameworks need to address

Offences

1. Offences **against** the confidentiality, integrity and availability of computer systems and data

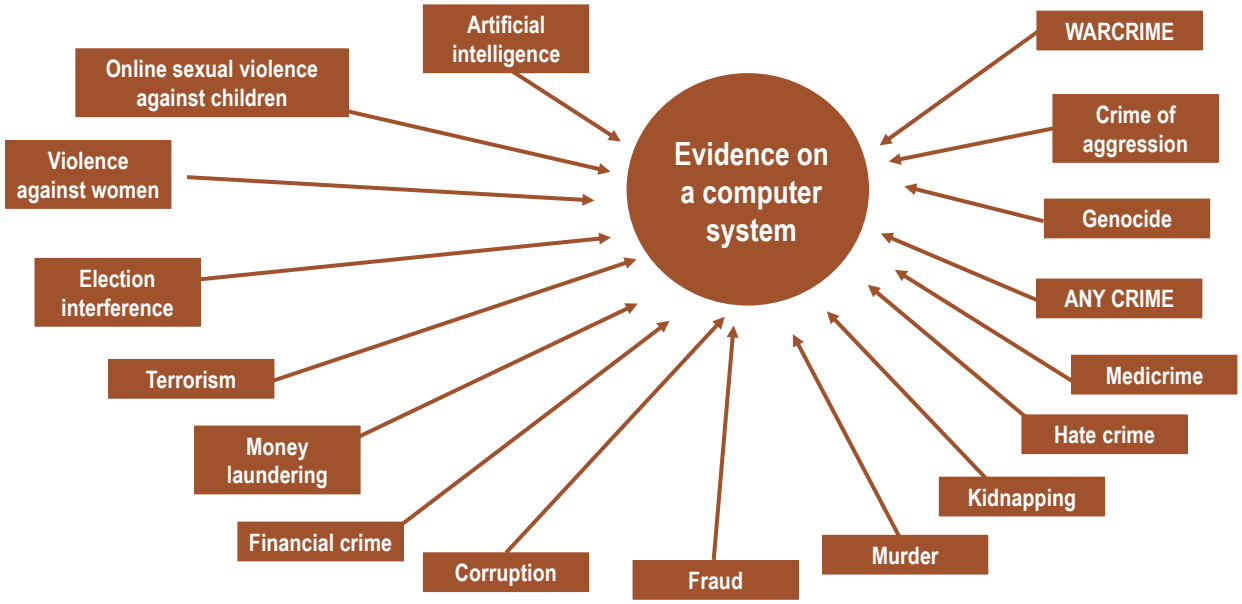
Examples:
- Illegally accessing a computer or data ("hacking")
- Illegally intercepting computer data
- Interfering with computer data (altering, deleting, stealing data, etc. e.g. via malware)
- Interfering with computer systems (denial of service attacks, ransomware attacks, etc.)
- Development or making available of **tools** to commit such offences

2. Offences **by means** of computer systems or data

Examples:
- Forgery (e.g. setting up a phishing website)
- Fraud (e.g. "man-in-the-middle-attack" etc. to deceive a computer system to obtain an economic benefit)
- Production, distribution, making available, possessing, accessing child sexual abuse materials ("child pornography")
- Non-consensual dissemination of intimate images (e.g. "sextortion")
- Solicitation (grooming) of children for sexual offences
- Offences related to intellectual property rights

3

Introduction — Problems that international legal frameworks need to address



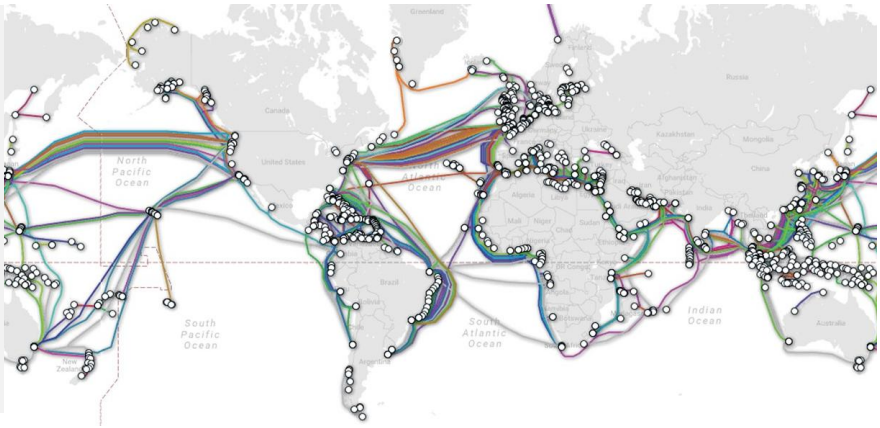
4

Introduction

Problems that international legal frameworks need to address

Electronic evidence = evidence to be obtained for use in criminal proceedings

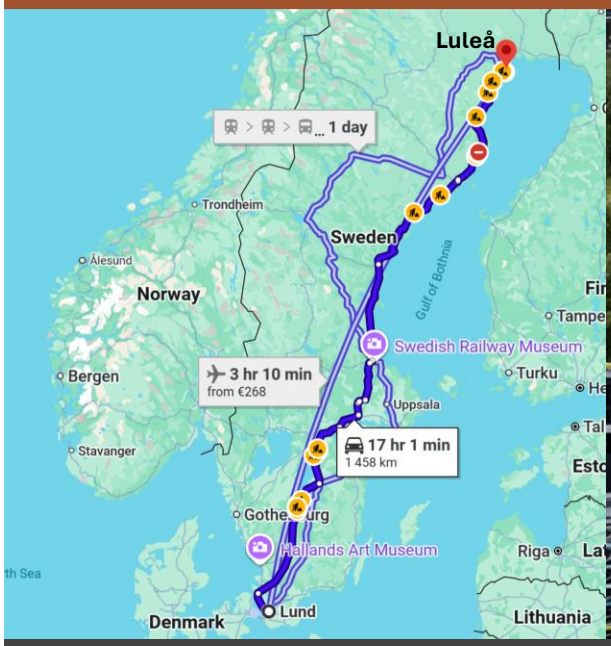
- Where is the crime?
- Where is the data / evidence?
- Who has the data / evidence?
- What law applies?
- What boundaries for law enforcement?



5

Introduction

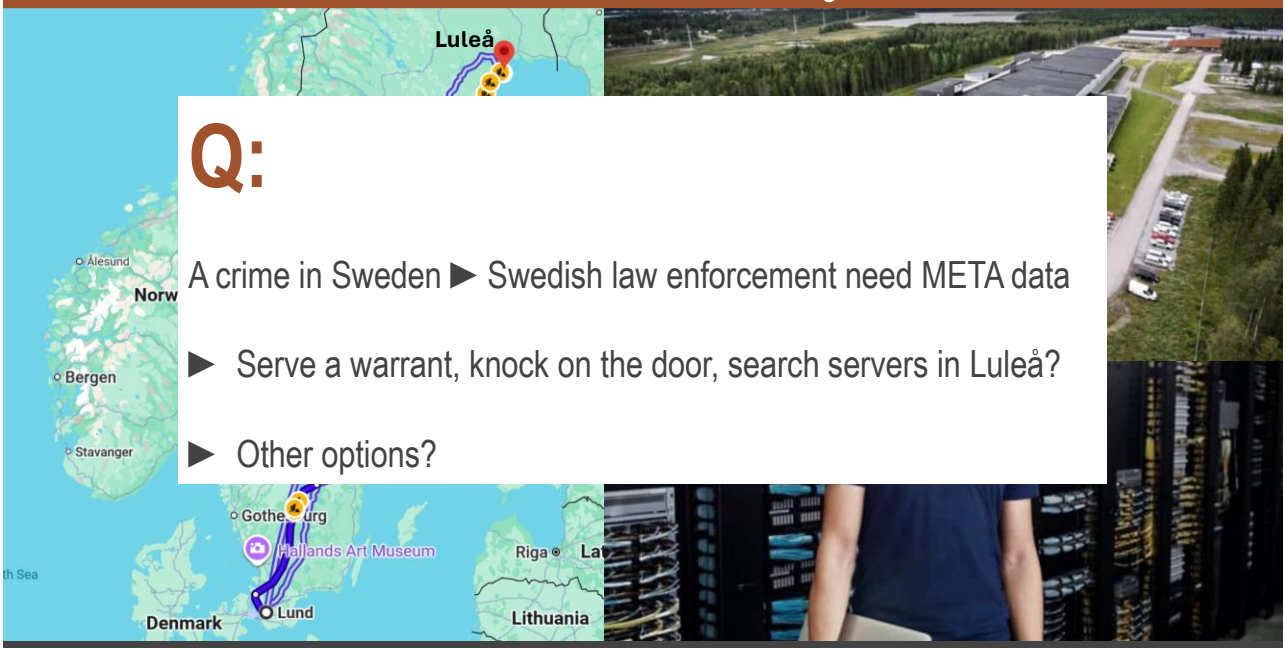
Problems that international legal frameworks need to address



Source: https://siecledigital.fr/2016/09/30/facebook-data-center-suede/

6

Introduction
Problems that international legal frameworks need to address



Q:

A crime in Sweden ► Swedish law enforcement need META data

► Serve a warrant, knock on the door, search servers in Luleå?

► Other options?

7

Introduction
Problems that international legal frameworks need to address

Summary: Challenges to be addressed by international treaties on cybercrime and electronic evidence

- **Criminalizing** offences **against and by means** of computer systems and data
- **Procedural powers to collect electronic evidence** not only in relation to these offences but e-evidence of any offence
- **Obtaining volatile e-evidence** that may be somewhere "in the cloud" or in multiple or shifting jurisdictions
  - Government-to-government cooperation?
  - Direct access to computer systems in other jurisdictions?
  - Direct cooperation with service providers in other jurisdictions?
  - Protection of sovereignty?
  - Protection of rights of individuals?
  - Different types of data/evidence with different levels of sensitivity/protection?

8

International treaties on cybercrime and electronic evidence

- **Convention on Cybercrime** of the Council of Europe ("Budapest Convention") of 2001 with protocols (2003 & 2022)
- Convention against cybercrime of the United Nations ("Hanoi Convention") of 2025
  - Official title: "**United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes**"

9

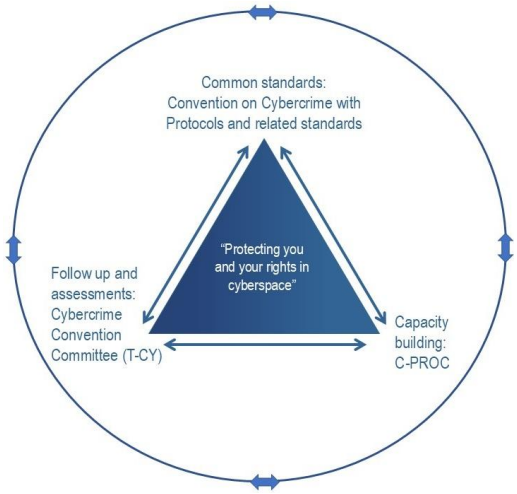
The framework of the Budapest Convention

- **Convention** on Cybercrime (Budapest, 2001)
  1. Specific offences
  2. Procedural powers
  3. International cooperation
- **1st Protocol** on Xenophobia and Racism via Computer Systems (2003)
- **2nd Protocol** on enhanced cooperation and disclosure of electronic evidence (2022)
- **Guidance Notes**

NB: Cybercrime & e-evidence!

As of May 2026:

82 Parties and 16 "Observer States"



10

Content of the Budapest Convention

Criminalising conduct
- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

Limited by safeguards

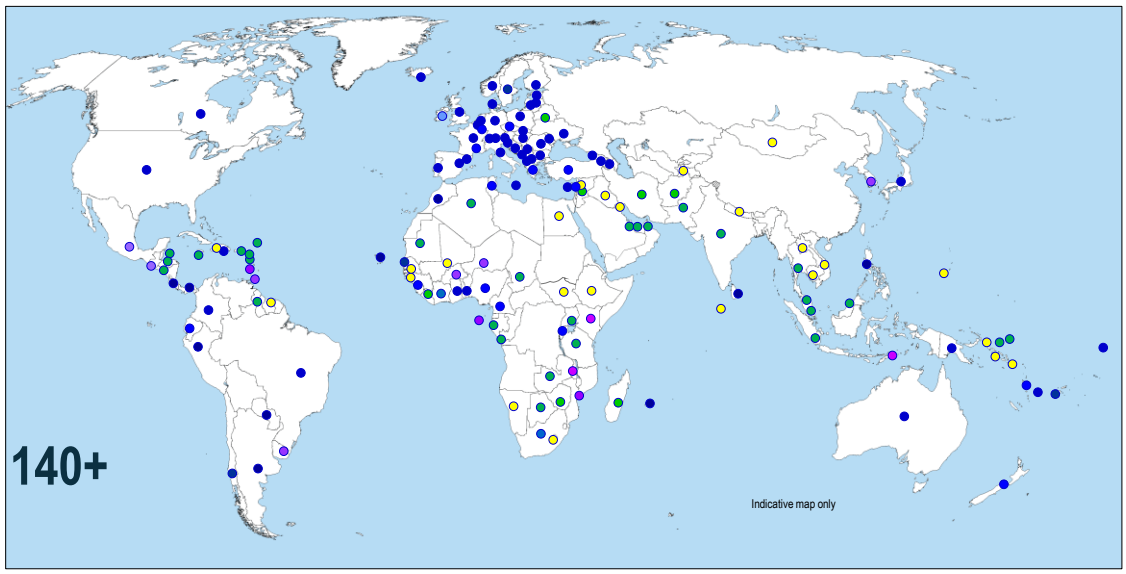
+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Cybercrime and e-evidence:
Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

11

Reach of the Budapest Convention



12

Second Protocol to the Budapest Convention on e-evidence

Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

- Opened for signature May 2022
- As of May 2026: 52 signatories (Costa Rica, Hungary, Japan and Serbia have ratified it)

Q

- **Why only 4 ratifications in 4 years?**
- **Signature vs ratification?**

13

Second Protocol to the Budapest Convention on e-evidence

Chapter II: Measures for enhanced cooperation

Article 6	Request for domain name registration information	→ Public-2-Private
Article 7	Disclosure of subscriber information	→ Public-2-Private
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data	→ Public-2-Public
Article 9	Expedited disclosure of stored computer data in an emergency	→ Public-2-Public
Article 10	Emergency mutual assistance	→ Public-2-Public
Article 11	Video conferencing	→ Public-2-Public
Article 12	Joint investigation teams and joint investigations	→ Public-2-Public

Subject to safeguards, including for the protection of personal data (Article 14)

14

T-CY Guidance Notes

Guidance Notes:

- Common understanding between the Parties
- Adopted by consensus
- Keeping the Convention up-to-date and adapting to evolving technology, techniques and forms of crime

15

Current work by the Cybercrime Convention Committee (T-CY)

Mapping study on virtual assets and relevance of the Convention on Cybercrime
(January 2025 – June 2026 ► **study adopted**: Provisions of the Convention are largely applicable to virtual assets and virtual asset service providers ► recommendations for follow up)

Ongoing: **Working Group on artificial intelligence** (January 2025 – October 2026)

To prepare a mapping study on cybercrime, electronic evidence and artificial intelligence (AI), including options and recommendations for further action by the T-CY.

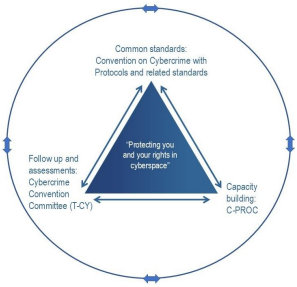
The mapping study shall focus on the specific links between cybercrime, electronic evidence and artificial intelligence, and address issues such as:

- Offences committed against and by means of AI systems[3], and applicability of current criminal law, including the Convention on Cybercrime and its First Protocol on Xenophobia and Racism.
- The use of AI systems for the prevention, detection, investigation and prosecution of offences, for the collection of electronic evidence and for international cooperation, and the applicability of current criminal law and agreements, including the Convention on Cybercrime and its Second Protocol.
- The applicability of human rights and rule of law safeguards, chain of custody, territoriality and jurisdiction, and other conditions and principles in this regard.

16

The framework of the Budapest Convention: some take-aways

- Treaty is 25 years old
- Reach to all regions of the world
- Keeps evolving and adapting (protocols, guidance notes, working groups)
- Emphasis on human rights and rule of law safeguards
- Keeps growing
- "Community of trust"[?]



17

The Hanoi Convention of the United Nations

"United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes"

- Opened for signature in Hanoi, Vietnam, in October 2025 ► "Hanoi Convention"
- As of May 2026:
  - 73 signatories (**including Sri Lanka**)
  - 3 parties (Azerbaijan, Qatar, Vietnam)

18

The Hanoi Convention of the United Nations: Structure

- Chapter I: General provisions
- Chapter II: Criminalisation
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement
- Chapter V: International cooperation
- Chapters VI–IX: Preventive measures, Technical assistance, Mechanism of implementation, Final provisions

19

The Hanoi Convention of the United Nations: Safeguards

- Article 6 on “respect for human rights”
- Article 21.4 with procedural guarantees
- Article 24 on conditions and safeguards, which is similar to Article 15 BC
- Article 36 on the protection of personal data [de facto a ground for refusal]
- Article 40.22 on non-discrimination within the context of mutual legal assistance [grounds for refusal]

20

Comparing Hanoi and Budapest conventions

Example: Offences

Art.	Budapest Convention	Art.	Hanoi Convention
2	Illegal access	7	Illegal access
3	Illegal interception	8	Illegal interception
4	Data interference	9	Interference with electronic data
5	System interference	10	Interference with an information and communications technology system
6	Misuse of devices	11	Misuse of devices
7	Computer-related forgery	12	Information and communications technology system-related forgery
8	Computer-related fraud	13	Information and communications technology system-related theft or fraud
9	Child pornography	14	Offences related to online child sexual abuse or child sexual exploitation material
10	Copyright infringements	-	
-		15	Solicitation or grooming for the purpose of committing a sexual offence against a child
-		16	Non-consensual dissemination of intimate images
-		17	Laundering of proceeds of crime

21

Comparing Hanoi and Budapest conventions

Core concepts and measures:

- Drawn from the BC on Cybercrime (2001)
- Complemented by provisions adapted from the UN Conventions on Transnational Organised Crime (UNTOC, 2000) and Corruption (UNCAC, 2003)

► **Consistency**

New in UN treaty:

- Solicitation or grooming of children for sexual offences (Article 15)
- Non-consensual dissemination of intimate images (Article 16)
- Adapted from UNTOC and UNCAC: measures on money laundering and crime proceeds

NOT in UN treaty:

- IPR offences
- Art. 32 on transborder access to data
- Xenophobia and racism (First Protocol to BC)
- None of the measures of the Second Protocol to the BC on enhanced cooperation and disclosure of electronic evidence (2022):
  - Direct cooperation with service providers and registrars in other Parties (articles 6 and 7)
  - Expedited cooperation in emergency situations (articles 9 and 10)

22

Comparing Hanoi and Budapest conventions

Reservations and declarations:

- Budapest Convention: Limited to specific provisions. Article 42: "No other reservations may be made".
- Hanoi Convention: Open-ended, only limited by **object and purpose test**.
  - ► **Risk of uneven, ambiguous or deferred implementation by parties to the Hanoi Convention**
    - ► **Preventing effective international cooperation**

Hanoi Convention: **Examples of reservations** made upon ratification

Qatar: Reservation to child abuse articles

(1) The State of Qatar does not consider itself bound by the provisions of Articles (16), (15), and (14) of the Convention, as they contradict the provisions of Islamic Sharia, national legislation, and the social and cultural values of the State of Qatar.

Vietnam

1. The Socialist Republic of Viet Nam declares that the provisions of the United Nations Convention against Cybercrime are non-self-executing. The implementation of provisions of this Convention shall be in accordance with constitutional principles and substantive law of the Socialist Republic of Viet Nam, on the basis of bilateral or multilateral cooperative agreements with other States and the principle of reciprocity.

23

Conclusion

- Adoption of the Hanoi Convention by the United Nations is an important political achievement given the current fractured international context
- The Hanoi Convention is broadly consistent with the Budapest Convention, no obvious contradictions ► States may join both conventions
- For Parties to the Budapest Convention the Hanoi Convention offers additional options for cooperation with States that are not parties to the Budapest Convention
- For criminal justice practitioners, the Budapest Convention will remain the more relevant framework in the years to come
- The tools of the Second Protocol on e-evidence have NOT been incorporated in the Hanoi Convention
- **Key conditions for the effectiveness of these treaties: TRUST between parties**
  - Key condition for trust: parties meet their obligations and respect the conditions of the treaty
    - Key conditions for democratic countries: **Parties respect the human rights and rule of law requirements of the treaty**

24

Discussion

Q & A

Cybercrime (part 2): Criminal justice action on cybercrime ► Human rights implications

Alexander Seger
Strasbourg, France
former Executive Secretary, Cybercrime Convention Committee, Council of Europe

Agenda

- Cybercrime and e-evidence: General human rights considerations
- Risks arising from
  - Criminalization
  - Procedural powers to investigate and collect electronic evidence
  - International cooperation
- Human rights and rule of law requirements under “Budapest” and “Hanoi” conventions
- Risks remaining

27

Action on cybercrime and human rights: General considerations

Scenario: a 12-years old boy ….

Q: human rights violation?

28

Action on cybercrime and human rights: General considerations

General consideration: "Positive obligations"

European Court of Human Rights

- Governments have to provide for effective measures, including through criminal law, to protect individuals against interference with their human rights by others

= Not providing for effective measures may be considered a violation of human rights

- Applicable also to crime online and use of criminal law tools of the Budapest Convention (See ECtHR: K.U. v Finland 2008)

29

Action on cybercrime and human rights: General considerations

Human rights and rule of law standards are global (ECHR, African Convention, Inter-American Convention, ICCPR)

Criminal law measures on cybercrime and e-evidence may interfere with fundamental rights

An interference must:

- be prescribed by law (clear, precise, accessible, foreseeable, overseen by an independent body etc.)
- pursue a legitimate aim (rights or reputation of others, national security, public order etc.)
- be necessary and proportionate (pressing and substantial need, least restrictive means to achieve the stated aim, etc.)

Risks, conditions and safeguards regarding:

- Criminalization
- Procedural powers (cybercrime and e-evidence)
- International cooperation

+ Impact of laws and measures on cybercrime and e-evidence on other rights (privacy, freedom of expression etc.) AND on rights of others (third parties)

30

Action on cybercrime and human rights: Criminalization

Risks arising and conditions and safeguards needed regarding:

- **Criminalization** → Q: Risks?
- Procedural powers (investigating cybercrime and collecting e-evidence)
- International cooperation

31

Action on cybercrime and human rights: Criminalization

Risks arising and conditions and safeguards needed regarding:

- **Criminalization**: Risks to freedom of expression (ICCPR Art. 19)
  - **Chilling effects** on journalists, activists, researchers, and political opponents
  - Criminalization of online speech under **vague cybercrime offences**
  - Basis for Strategic Litigation Against Public Participation (**SLAPPs**)*.

*SLAPPs are illegitimate and abusive lawsuits designed to intimidate, harass and silence legitimate criticism. For Guidance on SLAPPs see Council of Europe Recommendation CM/Rec(2024)2 on countering the use of strategic lawsuits against public participation (SLAPPs)

32

Action on cybercrime and human rights: Criminalization

Example: Nigeria Section 24 of the Cybercrime (Prohibition, Prevention, etc.) Act, 2015

(1) "Any person who knowingly or intentionally sends a message or other matter by means of computer system or network that:
(a) Is **grossly offensive or phonographic or an indecent obscene or menacing character** or causes any such message or matter to be so sent; or
(b) He knows to be false, for the **purpose of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety** to another or caused such a message to be sent: commits an offence under this act and shall be liable on conviction to fine of not more than N7,000,000.00 or imprisonment**.**

(2) Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network-
(a) **Bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person**;
(b) containing any **threat to kidnap any person or any threat to harm the person of another**, …

… commits an offence under this act

33

Action on cybercrime and human rights: Criminalization

CNN World Watch Listen Live TV Sign in

World / Africa

A Nigerian woman reviewed some tomato puree online. Now she faces jail

By Nimi Princewill, CNN
6 minute read · Updated 10:56 PM EDT, Wed March 27, 2024

Abuja, Nigeria (CNN) — A Nigerian woman who wrote an online review of a can of tomato puree is facing imprisonment after its manufacturer accused her of making a "malicious allegation" that damaged its business.

Chioma Okoli, a 39-year-old entrepreneur from Lagos, is being prosecuted and sued in civil court for allegedly breaching the country's cybercrime laws, in a case that has gripped the West African nation and sparked protests by locals who believe she is being persecuted for exercising her right to free speech.

34

Action on cybercrime and human rights: Criminalization

Octopus Project

www.coe.int/cybercrime
Link

Considerations (examples):

- For legislators
  - The three-tier test of legality, proportionality and necessity is the key safeguard against excessive restrictions to the freedom of expression.
- For policy makers
  - Public figures shall be required to tolerate a greater degree of criticism.
  - Consider multistakeholder approach to combating disinformation.
- For criminal justice practitioners
  - Criminal law needs to be used as a last resort for addressing both disinformation and defamation.

35

Action on cybercrime and human rights: Procedural powers

Risks arising and conditions and safeguards needed regarding:

- Criminalization
- **Procedural powers (investigating cybercrime and collecting e-evidence)**
- International cooperation

Q: Risks?

36

Action on cybercrime and human rights: Procedural powers

Risks arising and conditions and safeguards needed regarding

- **Procedural powers to investigate and collect electronic evidence:**
  - **Risks to privacy and data protection (ICCPR Art. 17)**. Example: overbroad search warrants; bulk collection of data.
  - **Risks to due process and fair trial (ICCPR Art. 14)**. Examples: Classified investigative methods; limited ability to challenge legality of data collection; chain-of-custody problems, opaque forensic tools and other evidentiary issues.
  - **Protection against arbitrary search and seizure (ICCPR Art. 17).** Examples: Seizure of devices instead of targeted extraction or production of data; remote searches without notice; weak judicial oversight.
  - **Non-discrimination and abuse of power (ICCPR Art. 2 and 26).** Examples Selective enforcement against dissenters; lack of transparency of surveillance powers.

37

Action on cybercrime and human rights: International cooperation

Risks arising and conditions and safeguards needed regarding:

- Criminalization
- Procedural powers (investigating cybercrime and collecting e-evidence)
- **International cooperation** → Q: Risks?

38

Action on cybercrime and human rights: International cooperation

Risks arising and conditions and safeguards needed regarding

► **International cooperation**

- Request for cooperation motivated by political investigations/prosecutions or discrimination
- Lack of dual criminality
- Lack of human rights and rule of law conditions and safeguards in requesting or in requested country
- Cooperation leading to capital punishment in requesting country

39

Human rights and rule of law requirements under "Budapest" and "Hanoi" conventions

Human rights and rule of law requirements under the "Budapest" Convention

► General: Link to human rights and specific COE and UN human rights treaties, incl. on data protection (Preamble)

► Criminalisation:
- Limited list of offences against and by means of computers
- Declarations and reservations

► Procedural powers on cybercrime and e-evidence of any crime:
- **Article 15 conditions and safeguards**
  - Obligations pursuant to international HR treaties, principle of proportionality
  - Judicial or other supervision, grounds justifying application, limitation of scope and duration
- Specified data needed in specific criminal investigations

► International cooperation
- Broad cooperation
- Grounds for refusal
- Confidentiality and use limitation

+ T-CY assessments
+ Capacity building
+ "Community of trust"
+ Accession procedure

40

Human rights and rule of law requirements under "Budapest" and "Hanoi" conventions

Human rights and rule of law requirements under the "Budapest" Convention
► Second Protocol on e-evidence

Subject to a particularly strong system of safeguards:

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
- Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty
- Articles specify types of data to be disclosed
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided

41

Human rights and rule of law requirements under "Budapest" and "Hanoi" conventions

Hanoi Convention:
Human rights and rule of law concerns expressed <u>prior and during the negotiation</u>

- Treaty may "permit or facilitate repression or suppression of political activity, expression, conscience, opinion, belief, assembly or association; or permit or facilitate discrimination or persecution based on personal characteristics"
- Definitions and concepts: cybercrime v. "information crime"
- Criminalization: overbroad list and scope of offences
- Domestic investigations and prosecution:
  - Misuse of intrusive procedural powers
  - Freezing and confiscating property/assets to target individuals, civil society, businesses, service providers etc.
- International cooperation: Parties may be obligated to cooperate even in cases where HR are violated.
- Free, open and global internet with multi-stakeholder governance v. sovereign, government-controlled cyberspace

42

Human rights and rule of law requirements under “Budapest” and “Hanoi” conventions

“Hanoi” Convention: Human rights and rule of law safeguards in the convention as adopted:

- Article 6 on “respect for human rights”
- Article 21.4 with procedural guarantees
- Article 24 on conditions and safeguards (which is similar to Article 15 BC)
- Article 36 on the protection of personal data [de facto a ground for refusal]
- Article 40.22 on non-discrimination within the context of mutual legal assistance [grounds for refusal]

Art 36: … A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data;

43

The Hanoi Convention of the United Nations: Safeguards

UN Ad Hoc Committee /
Final session (August 2024):

- Iran requested 6 rounds of voting to remove safeguards from the draft treaty

44

The Hanoi Convention of the United Nations: Safeguards

UN Ad Hoc Committee /
Final session (August 2024):

- Iran lost, safeguards remained in the treaty

But:

- **Some States suggested that they would not respect those safeguards …**

45

Human rights and rule of law requirements under “Budapest” and “Hanoi” conventions

“Hanoi” Convention: Risks remaining

- Risk that some States will not respect human rights and rule of law conditions. Conference of States Parties (COSP) unlikely to review compliance.
- Risk of targeting assets of individuals, private sector organisations, media or civil society organisations through combination of provisions on fraud, money laundering, corporate liability, participation and attempt, and **crime proceeds**.
- Risk of supplementary criminalization through a protocol (negotiations to commence two years after adoption of the convention [i.e. January 2027] as per draft UNGA resolution). [Note: informal discussion have commenced. Russia submitted draft text in June 2026]

46

Conclusions

- **Key conditions for the effectiveness of treaties: TRUST between parties**
  - Key condition for trust: parties meet their obligations and respect the conditions of the treaty
    - Key condition for democratic countries: **Parties respect the human rights and rule of law requirements of the treaty**
  - Treaties or not, some States will misuse measures on cybercrime and e-evidence to violate rights
  - Other States will refuse to cooperate with them

47

Conclusions

Human rights and rule of law standards are global (ECHR, African Convention, Inter-American Convention, ICCPR)

Criminal law measures on cybercrime and e-evidence may interfere with fundamental rights.

An interference must:

- be prescribed by law (clear, precise, accessible, foreseeable, overseen by an independent body etc.)
- pursue a legitimate aim (rights or reputation of others, national security, public order etc.)
- be necessary and proportionate (pressing and substantial need, least restrictive means to achieve the stated aim, etc.)

Ensure that these conditions are met when addressing cybercrime and e-evidence through:

- ► Criminalization
- ► Procedural powers (cybercrime and e-evidence)
- ► International cooperation

\+ Impact of laws and measures on cybercrime and e-evidence on other rights (privacy, freedom of expression etc.) AND on rights of others (third parties)

48