CyberSouth+

Enhanced co-operation on cybercrime and electronic evidence in the Southern Neighbourhood region

CyberSouth+ launching event | Lisbon, Portugal | 17 – 18 April 2024

Session 4

▶ Freedom of expression and cybercrime

Alexander Seger, Head of Cybercrime Division, Council of Europe

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe

www.coe.int/cybercrime

1

Countering cybercrime: Human rights considerations

2

Countering cybercrime: Human rights considerations

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.

3

Countering cybercrime: Human rights considerations

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**, any demand or request for a ransom for the release of any kidnapped person, to extort from any person firm association or corporation any money or other thing of value; or
(c) containing any **threat to harm the property or reputation** of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association or corporation, any money or other thing of value;

commits a offence under this act

4

Variations of such provisions also in other countries!

Concern: Cybercrime laws increasingly used to address speech in broad and vague terms

► "Prescribed by law? Clear, precise, foreseeable? Necessary? Proportionate?

Examples:

- Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or councelling commission of an offence, commits an offence, and shall be punishable …
- Anyone who knowingly uses information and communication systems and networks in order to produce, spread, disseminate, send or write false news, false data, rumours, false or falsified documents or documents falsely attributed to others with the aim of infringing the rights of others or harming public safety or national defence or spreading terror among the population shall be punished by five years' imprisonment and a fine …
- 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 …

Countering cybercrime: Human rights considerations

Human rights and rule of law risks:

- **Criminalisation:** overbroad list and scope of offences. 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"
- **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 human rights are violated.

7

Countering cybercrime: Human rights considerations

European Court of Human Rights: "positive obligations"

- ► 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)

8

Countering cybercrime: Human rights considerations

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

Conditions and safeguards regarding:

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

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.)

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

9

Countering cybercrime: Human rights considerations

Octopus Project

www.coe.int/cybercrime

Link

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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.

10

Q & A

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

Procedural powers limited by Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

13

Convention on Cybercrime: Conditions and safeguards

Second Protocol on e-evidence

Means for a more effective criminal justice response:

- Direct cooperation with service providers in other jurisdictions to obtain subscriber information
- Direct requests to registrars to obtain domain name registration information
- More effective means to obtain subscriber information and traffic data through government-to-government cooperation
- Expeditious cooperation in emergency situations
- Joint investigations and video-conferencing

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

14

"European" human rights and rule of law requirements?

African Charter on Human and Peoples' Rights (ACHPR)

Article 1

"The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Charter and shall undertake to adopt legislative or other measures to give effect to them."

Article 9

1. Every individual shall have the right to receive information.
2. Every individual shall have the right to express and disseminate his opinions within the law.

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa**,
(adopted at its 65th Ordinary Session, held from 21 October to 10 November 2019, in Banjul, Gambia)

Charte Africaine des Droits de l'Homme et des Peuples

Article 1

Les Etats membres de l'Organisation de l'Unité Africaine, parties à la présente Charte, reconnaissent les droits, devoirs et libertés énoncés dans cette Charte et s'engagent à adopter des mesures législatives ou autres pour les appliquer.

Article 9

1. Toute personne a droit à l'information.
2. Toute personne a le droit d'exprimer et de diffuser ses opinions dans le cadre des lois et règlements.

► Commission Africaine des Droits de l'Homme et des Peuples: DÉCLARATION DE PRINCIPES SUR LA LIBERTÉ D'EXPRESSION ET L'ACCÈS À L'INFORMATION EN AFRIQUE (2019)
(adoptee à Banjul en 2019)

17

Accession to the Convention on Cybercrime: considerations
Adhésion à la Convention sur la cybercriminalité: considérations?

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)**

Principle 9 ► conditions for a justifiable limitation of the exercise of the right to freedom of expression and access to information

"1.States may only limit the exercise of the, if the limitation:
- a. is prescribed by law;
- b. serve a legitimate aim; and
- c. is a necessary and proportionate means to achieve the stated aim in a democratic society.

2. States shall ensure that any law limiting the rights to freedom of expression and access to information:
- a. is clear, precise, accessible and foreseeable;
- b. is overseen by an independent body …
- c. effectively safeguards against abuse …

18

► Commission Africaine des Droits de l'Homme et des Peuples:
DÉCLARATION DE PRINCIPES SUR LA LIBERTÉ D'EXPRESSION ET L'ACCÈS À L'INFORMATION EN AFRIQUE (2019)

Principle 9 ►Les restrictions justifiables

"1. Les États ne peuvent restreindre l'exercice des droits à la liberté d'expression et à l'accès à l'information que lorsque cette restriction :

a. est prévue par la loi;
b. répond à un objectif légitime ; et
c. est un moyen nécessaire et proportionné pour réaliser le but visé dans une société démocratique.

2. Les États veillent à ce que toute loi portant restriction des droits à la liberté d'expression et à l'accès à l'information :

a. soit claire, précise, accessible et prévisible ;
b. soit supervisée par un organisme indépendant d'une manière non-arbitraire ou discriminatoire ; et
c. protège de manière efficace contre les abus, notamment par la reconnaissance d'un droit de recours devant des juridictions indépendantes et impartiales.…

19

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa** (2019)

Principle 9 ► conditions for a justifiable limitation of the exercise of the right to freedom of expression and access to information

3. A limitation shall serve a **legitimate aim** where the objective of the limitation is:

a. to preserve respect for the rights or reputations of others; or
b. to protect national security, public order or public health.

4. To be **necessary and proportionate**, the limitation shall:

a. originate from a pressing and substantial need that is relevant and sufficient
b. have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; …

20

► Commission Africaine des Droits de l'Homme et des Peuples:
DÉCLARATION DE PRINCIPES SUR LA LIBERTÉ D'EXPRESSION ET L'ACCÈS À L'INFORMATION EN AFRIQUE (2019)

Principle 9 ► Les restrictions justifiables

3. Toute restriction vise un but légitime en vertu duquel elle aura pour objectif ce qui suit :

a. préserver le respect des droits ou la réputation de tiers ; ou
b. protéger la sécurité nationale, l'ordre public ou la santé publique.

4. Pour être nécessaire et proportionnée, la restriction doit :

a. être motivée par une nécessité urgente et impérieuse, qui soit réelle et suffisante ;
b. avoir un lien direct et immédiat avec la demande et la divulgation d'informations et être le moyen le moins restrictif de réaliser le but visé ;
c. être de nature telle que les avantages de la protection de l'intérêt déclaré l'emportent sur les problèmes induits par la demande et la divulgation d'informations, notamment en ce qui concerne les sanctions autorisée …

21

Accession to the Convention on Cybercrime: considerations
Adhésion à la Convention sur la cybercriminalité: considérations?

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)**

Principle 21 ► Protecting reputations

"1.States shall ensure that laws relating to defamation in accordance with the following standards:

a. No one shall be found liable for true statements, expressions of opinions or statements which are reasonable to make in the circumstances.
b. Public figures shall be required to tolerate a greater degree of criticism.
c. Sanctions shall never be so severe as to inhibit the right to freedom of expression.

2. Privacy and secrecy laws shall not inhibit the dissemination of information of public interest."

22

► Commission Africaine des Droits de l'Homme et des Peuples:
DÉCLARATION DE PRINCIPES SUR LA LIBERTÉ D'EXPRESSION ET L'ACCÈS À L'INFORMATION EN AFRIQUE (2019)

Principle 21 ► La protection de la réputation

1. Les États veillent à ce que les lois relatives à la diffamation soient conformes aux normes suivantes :

   a. Nul ne peut être jugé coupable pour avoir fait des observations véridiques, donné son avis ou fait des déclarations qu'il était raisonnable de faire dans les circonstances données ;
   b. Les personnages publics sont tenus de tolérer plus de critiques ;
   c. Les sanctions ne sont jamais sévères au point d'entraver le droit à la liberté d'expression.

2. Les lois garantissant le respect de la vie privée et le droit au secret n'entravent pas la diffusion d'informations d'intérêt public.

23

"Positive obligations":

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

Conditions and safeguards regarding:

► Criminalisation

► Procedural powers (cybercrime and e-evidence)

► International cooperation

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.)

24

Q & A