Octopus Project

Discussion paper: Freedom of expression within the context of action on cybercrime – Practical considerations

Strasbourg, 10 December 2023 / Provisional version

www.coe.int/cybercrime

TABLE OF CONTENTS

1 Purpose 3
2 Introduction: Freedom of expression as a fundamental right 3
3 Freedom of expression in human rights frameworks 4
3.1 The United Nations system 4
3.2 African Human Rights System 6
3.3 European Human Rights System 7
3.4 Inter-American System of Human Rights 8
3.5 League of Arab States 9
3.6 The Association of Southeast Asian Nations (ASEAN) 10
4 Freedom of expression in the context of action on cybercrime, electronic evidence, and information disorder 10
4.1 Substantive law offences 10
4.2 Procedural powers and safeguards 11
4.3 Information disorder 12
5 Challenges and solutions on cybercrime and freedom of expression in national legislation and practice 13
5.1 Countering disinformation 13
5.1.1 Issues 13
5.1.2 Solutions 14
5.2 Clarity of the law 14
5.2.1 Issues 14
5.2.2 Solutions 15
5.3 Necessity, proportionality, pressing social need 15
5.3.1 Issues 16
5.3.2 Solutions 16
5.4 Use of procedural powers 16
5.4.1 Issues 17
5.4.2 Solutions 17
5.5 Excessive criminalisation/proportionality 17
5.5.1 Issues 17
5.5.2 Solutions 17
6 Considerations 18
6.1 Considerations for legislators 18
6.2 Considerations for policy makers 18
6.3 Considerations for criminal justice practitioners 19

Contact
Cybercrime Division of the Council of Europe
Email cybercrime@coe.int

Disclaimer
This technical report does not necessarily reflect official positions of the Council of Europe, donors of the Octopus Project or Parties to the treaties referred to.

1 Purpose

In recent years, most countries around the world have undertaken legislative reforms on cybercrime and electronic evidence. In a number of countries, such legislation on cybercrime includes provisions criminalising the "dissemination of false information", "offensive messages", "causing annoyance", "spreading of rumours" and other conduct. In some instances, such provisions appear to be vague and overly broad, and raise concerns of whether such restrictions to the freedom of expression are consistent with human rights and rule of law requirements.

The present paper is, therefore, aimed at supporting policy makers, legislators and criminal justice practitioners in their development and implementation of policies and legislation on cybercrime consistent with the right to the freedom of expression.

2 Introduction: Freedom of expression as a fundamental right

The right to freedom of expression is a fundamental human right enshrined in a number of international and regional human rights law instruments, most prominent of those being Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights.[1]

The right to freedom of expression is fundamental in many ways as an enabler to enjoyment of other rights and freedoms, but also as a cornerstone of democracy and the rule of law.[2] However, the freedom of expression is not an absolute right, and can be subject to certain restrictions as provided for by law and as necessary to protect the rights and reputations of others, national security, public order and public health and morals.[3]

Protecting the freedom of expression in the context of fight against cybercrime is a matter of criminal justice, thus many principles and rules applicable to protection of free speech and opinions in traditional criminal cases would also apply to expressions online. However, there are concerns due to potential and reach of information technology and its impact on society – such concerns both regulatory and practical - that require a closer look into restrictions of the freedom of expression based on the needs of criminal justice authorities for preventing and combating cybercrime.[4]

[1] For a definitive list of these standards and instruments, please refer to https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/international-standards
[2] For more in-depth discussion on the context of the right to freedom of expression with other rights and freedoms, please refer to the Human Rights Committee General Comment No. 34 on Article 19: Freedoms of opinion and expression, found here:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/453/31/PDF/G1145331.pdf.
[3] United Nations International Covenant on Civil and Political Rights, Article 19, par. 3, among many similar provisions in other human rights instruments.
[4] Some of these concerns and discussions could be found in HAKMEH, J.: Cybercrime Legislation in the GCC Countries Fit for Purpose?, Chatham House, The Royal Institute of International Affairs, 2018.

3 Freedom of expression in human rights frameworks

3.1 The United Nations system

The global human rights framework developed under the auspices of the United Nations, such as the Universal Declaration of Human Rights (UDHR) or the International Covenant on Civil and Political Rights (ICCPR), provides for some of the earliest and most recognized references to the freedom of expression and opinion. Articles 19 of both UDHR and ICCPR establish a set of principles followed and mirrored in many other regional and national systems by providing either implementing legislation or through supporting case law.

Article 19 of the ICCPR is, in many ways, a global reference and standard for the freedom of expression as a fundamental right.[5] In a related set of standards, the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) deals with a matter of hate speech (including online).[6] In terms of standards of the United Nations on freedom of expression applicable to the online environment, the UN Human Rights Council Resolution 20/8[7] on the promotion, protection and enjoyment of human rights on the Internet affirms applicability of online domain.[8]

With more relevance to the matters related to freedom of expression and regulation pertaining to fight against cybercrime, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion submitted a Report to the UN General Assembly in 2011,[9] developing on permissible and impermissible exceptions and limitations on the right guaranteed by Article 19 of the ICCPR,[10] although with these four categories expressly set,[11] the three-tier test of legality,

[5] Human Rights Committee General Comment No.34 on Article 19: Freedoms of opinion and expression, section 22. Paragraph 1 of Article 19 requires protection of the right to hold opinions without interference, which is a right to which the Covenant permits no exception or restriction. Paragraph (2) requires States parties to guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers; however, in contrast to Paragraph (1), the enjoyment of this right can be restricted, in accordance with specific conditions set by Paragraph (3) and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality

[6] Article 4 of ICERD requires prohibition of "all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin". Retrieved at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial.

[7] Can be retrieved at: https://digitallibrary.un.org/record/731540?ln=en.

[8] Article 1 of the Resolution 20/8 reaffirms that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

[9] UNGA A/66/290, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 10 August 2011, available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A.66.290.pdf.

[10] *Ibid,* section 18 of the Report. In this context, the Special Rapporteur advocated on distinguishing between three types of expression: expression that constitutes an offence under international law and can be prosecuted criminally; expression that is not criminally punishable but may justify a restriction and a civil suit; and expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility, and respect for others.

[11] *Ibid*, p. 8 to 13 of the Report. In relation to expression that can be prosecuted under criminal law, four categories of expression were outlined that would constitute permissible restrictions to the right of the freedom of expression: child pornography/child sexual abuse material; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and incitement to terrorism.

proportionality and necessity should be applied and respected at all times.[12] Furthermore, any other type of content and expression should not be restricted, with a few examples directly referenced in the Report as expressly impermissible.[13]

Examples of case law include:

- In Kouider Kerrouche v. Algeria,[14] the Human Rights Committee found that Article 19 (3) of the ICCPR allows restrictions to be placed on the freedom of expression, but only such as are provided for by law and are necessary for the respect of the rights or reputations of others. As there could be no explanation that would show that the author's criminal trial and conviction for defamation were necessary to protect the integrity of the judiciary, a violation of article 19 (2) of the Covenant was found.[15]

- In Svetlana Mikhalchenko v. Belarus,[16] in finding a violation of Article 19 in this particular case, the Committee found that national authorities did not explain why it was necessary to restrict the freedom of the author to seek, receive and impart information in order to ensure the respect of the rights or reputations of others, or for the protection of national security or of public order, or of public health or morals.[17]

- The Working Group on Arbitrary Detention under the United Nations Human Rights Council has also looked into the matters of freedom of expression in the Opinion No. 57/2017 concerning Stella Nyanzi (Uganda) in 2017.[18] In finding multiple violations of Article 19 ICCPR with regard to prosecution and deprivation of liberty for social media posts, the Working Group did not find investigation and detention "necessary or proportional for the purposes set out in Article 19 (3) of the Covenant".[19]

[12] *Ibid*, section 37.
[13] *Ibid*, section 42. These include discussion of government policies and political debate; reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups. These particular types of content are also referenced in Resolution 12/16 on Freedom of opinion and expression adopted by the Human Rights Council on 12 October 2009 (section 5.p), available at:
https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G09/166/89/PDF/G0916689.pdf.
[14] CCPR/C/118/D/2128/2012, Views adopted by the Human Rights Committee under article 5 (4) of the Optional Protocol, concerning communication No. 2128/2012 at its 118th session (17 October-4 November 2016), retrieved at: https://www.refworld.org/cases,HRC,591ea4824.html.
[15] Sections 8.8 and 8.9 of the HRC opinion. The case concerned a claim of the author that his prosecution for insulting a public official constituted a violation of his right to freedom of expression under Article 19 ICCPR.
[16] CCPR/C/114/D/1982/2010, Views adopted by the Human Rights Committee under article 5 (4) of the Optional Protocol, concerning communication No. 1982/2010 at its 114th session (29 June-24 July 2015), retrieved at: https://www.refworld.org/cases,HRC,59316e0d4.html. The issue before the Committee was whether the author's arrest for having distributed leaflets and the seizure of the leaflets in her possession constitute an unjustified restriction of her rights as protected by article 19 of the ICCPR.
[17] Section 8.5 of the HRC Opinion.
[18] A/HRC/WGAD/2017/57, Opinions adopted by the Working Group on Arbitrary Detention at its seventy-ninth session, 21-25 August 2017, Opinion No. 57/2017, found at:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/316/71/PDF/G1731671.pdf.
The author was subject to criminal investigation under the Computer Misuse Act of Uganda for allegedly offensive social media posts toward the political leadership of the country; the charges included offences of cyber-harassment and offensive communication under the said Act.
[19] Ibid, section 57 of the HRC Opinion.

3.2 African Human Rights System

Article 9 of the African Charter on Human and Peoples' Rights (ACHPR)[20] addresses freedom of expression in the regional context of Africa. It is noteworthy that the Charter does not provide for an express list of restrictions on the right to freedom of expression but rather sets a number of limitations of general nature applicable in specific contexts.[21]

Given the wide nature of the limitations at hand, it is perhaps not surprising that more detailed guidance has been developed in Africa concerning freedom of expression. The Declaration of Principles of Freedom of Expression and Access to Information in Africa,[22] adopted by the African Commission on Human and Peoples' Rights in 2019, lists a number of principles that are important in the context of legislation and practice of cybercrime investigations.[23]

Additionally, the African Commission on Human and Peoples' Rights also called upon the States Parties to the African Charter "to repeal criminal defamation laws or insult laws which impede freedom of speech", and to "refrain from imposing general restrictions that are in violation of the right to freedom of expression".

Examples of case law include:

- The judgment of the African Court on Human and Peoples' Rights in case of Lohé Issa Konaté v. The Republic of Burkina Faso (2019) is considered a landmark case for the freedom of expression in the region.[24] In addition to finding the conviction a disproportionate interference with the applicant's guaranteed rights to freedom of expression and that public figures - such as prosecutors - must tolerate more criticism than private individuals, the Court ordered Burkina Faso to amend its legislation on defamation.[25]

[20] African Charter on Human and Peoples' Rights ("Banjul Charter"), Organization of African Unity (OAU), June 27, 1981. Available at https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf.

[21] Under Article 27 (2) ACHPR, the "rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest". Per Article 28, "every individual shall have the duty to respect and consider his fellow beings without discrimination, and to maintain relations aimed at promoting, safeguarding and reinforcing mutual respect and tolerance." And pursuant to Article 29 of the treaty, the individual is expected "not to compromise the security of the State whose national or resident he is" and "to preserve and strengthen social and national solidarity, particularly when the latter is threatened".

[22] The text of the Declaration can be retrieved at: https://achpr.au.int/sites/default/files/files/2022-08/declarationofprinciplesonfreedomofexpressioneng2019.pdf .

[23] Which include the following: Necessity of protection from interference both offline and online under Principle 5; Independent oversight and effective safeguards against abuse to already confirmed three-tier system of legality, proportionality and necessity (Principle 9); What would constitute a legitimate aim, and what would be considered a proportionate and necessary limitation, including substantial need, direct connection and use of least restrictions, as well as balancing of interests (Principle 9); Higher degree of tolerance for public officials in relation to alleged defamation (Principle 21); Review and amendment of criminal responsibility and sanctions for various offences including defamation and libel, as well as hate speech (Principles 22 and 23).

[24] Can be retrieved at: https://www.african-court.org/en/images/Cases/Judgment/Judgment%20Appl.004-2013%20Lohe%20Issa%20Konate%20v%20Burkina%20Faso%20-English.pdf. The case concerned criminal liability of the media (defamation offence) for publishing several newspaper articles that alleged corruption by a state prosecutor.

[25] So that such legislation is compliant with international standards by repealing custodial sentences for acts of defamation and to adapt its legislation to ensure that other sanctions for defamation meet the test of necessity and proportionality, in accordance with the country's international obligations. More details and analysis at: https://globalfreedomofexpression.columbia.edu/cases/lohe-issa-konate-v-the-republic-of-burkina-faso. Similar reasoning of the Court, finding a violation of Article 9 ACHPR, was also confirmed in case of Agnes Uwimana-Nkusi v. Rwanda (2021).

- In Media Council of Tanzania v. Attorney-General of the United Republic of Tanzania (2019),[26] the East African Court of Justice unanimously held that numerous provisions in Tanzania's Media Services Act violated the Treaty for the Establishment of the East African Community as they infringed the right to freedom of expression.

- In The Incorporated Trustees of Laws and Rights Awareness Initiatives v. The Federal Republic of Nigeria (2020),[27] the Community Court of Justice of the Economic Community of West African States (ECOWAS), while finding the provisions in question sufficiently established by law and serving a legitimate aim, also concluded that "such provisions are not necessary in a democratic society and disproportionately violate the right to freedom of expression, guaranteed by Articles 9 (2) and ACHPR and 19 of the ICCPR."[28]

- In the follow-up judgment of the Registered Trustees of the Socio-Economic and Accountability Project (SERAP) v. The Federal Republic of Nigeria (2022),[29] the ECOWAS Court reconfirmed that "vague and arbitrary nature of Section 24 of the Cybercrime Act of 2015 is not in conformity with Article 9 of the ACHPR and Article 19 of the ICCPR" and instructed the respondent State to repeal the legislation.[30]

3.3 European Human Rights System

The system is represented by the European Convention of Human Rights (ECHR). It protects the human rights of people in countries that belong to the Council of Europe.

An important aspect of some content related offences[31] is that these may trigger freedom of expression concerns and should be always considered to represent freedom of expression protected under Article 10 of the ECHR.

However, the protection of freedom of expression offered by Art. 10 of the ECHR is not absolute. Art. 10.2 allows for certain restrictions, in particular when such ideas or expressions violated the rights of others. A particular expression must directly contribute to social harm and there should be a 'pressing social need' to restrict such expression.[32] These restrictions must meet the three-part cumulative test of legality, legitimacy of aim and proportionality.

[26] The decision can be consulted at the following link: https://www.mediadefence.org/resource-hub/wp-content/uploads/sites/3/2021/04/Media-Council-of-Tanzania-v-Attorney-General-of-Tanzania-2019.pdf. The Court has particularly detailed on its deliberation whether the contested legal Act in question (the Media Service Act of 2016) was sufficiently clear and foreseeable in terms of the principle of legality; in this case, the Act in question was not deemed to be precise enough to pass this test.

[27] The judgement can be found at the following address: http://www.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_16_20.pdf. The applicants alleged that the provisions of Section 24 of Cybercrime (Prohibition, Prevention, etc.) Act 2015, which criminalised communication of offensive or insulting messages, violated the right to freedom of expression enshrined in both ACHPR and ICCPR.

[28] *Ibid*, section 164.

[29] Decision available at the following address: https://serap-nigeria.org/download/download-ctc-of-judgment-by-ecowas-court-of-justice-prohibiting-prosecution-for-cyerstalking/#.

[30] *Ibid*, Operative Clause of the decision.

[31] Without delving into discussion on defamation and fake news as a self-sufficient subject matter, some of the terms used in this document reflect upon the attempts of UNESCO to provide definitions of some of these terms distinguishes between disinformation, misinformation, and mal-information (Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training).

[32] See e.g. European Commission for Democracy through Law (Venice Commission), Türkiye, Urgent joint opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft amendments to the Penal Code regarding the provision on "false or misleading information" issued pursuant to article 14a of the Venice Commission's Rules of procedure, 7 October 2022, para 59-61. [hereinafter referred to as Venice Commission, 2022].

The Convention is interpreted by the European Court of Human Rights (ECtHR) whose judgments are binding and their legal status is that of mandatory legal norms. Therefore, the text of the ECHR must be read together with the Court's case law.

Examples of case law include:

- Brzeziński v. Poland (App. No. 47542/07, 25 July 2019)[33] – ECtHR cautioned against the dangers of 'fake news', but underlined the importance of protecting political speech, particularly of opposition, during elections. The Court further emphasised that even statements that may be false, should be protected if a matter of 'undoubted' public interest is concerned.

- Lingens v. Austria (Application no. 9815/82) 8 July 1986[34] – The limits of acceptable criticism are accordingly wider as regards a politician as such than as regards a private individual. A politician lays himself open to close scrutiny of his every word and deed by both journalists and the public at large and must consequently display a greater degree of tolerance.

- Salov v. Ukraine (Application No. 65518/01, 6 September 2005)[35] – ECtHR underlined that "Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that the information might not be truthful".

3.4 Inter-American System of Human Rights

The right to freedom of expression in the Inter-American System is regulated by Article 13 of the American Convention on Human Rights (ACHR). Like other instruments, ACHR specifies the restrictions to the freedom of expression. The right to expression may be enforced by individuals against their State before the Inter-American Commission on Human Rights (IACommHR).

Inter-American Court of Human Rights (IACtHR) was established to provide interpretation of the provisions of the ACHR. It hears and rules on human rights violations by either the IACommHR or a state party.

Equally, as is the case with other mechanisms, States should ensure that any restrictions on freedom of expression comply with the international law three-part test requirements of legality, legitimacy of aim and proportionality.

The Declaration of Principles on Freedom of Expression was adopted by Inter-American Commission on Human Rights in 2000. It underlines that when information of public interest is disseminated, and such information may interfere with public official's reputation, the protection of a person's reputation should only be guaranteed through civil sanctions.[36]

---

[33] ECtHR, Brzeziński v. Poland (App. No. 47542/07), 25 July 2019 (see especially paragraphs 20, 53, 54, 56, 58, 59).
[34] See ECtHR, Lingens v. Austria (Application no. 9815/82) 8 July 1986.
[35] ECtHR, Salov v. Ukraine (Application No. 65518/01), 6 September 2005.
[36] Inter-American Commission on Human Rights, Declaration of Principles on Freedom of Expression, Inter-American Commission on Human Rights, 2000, Principle 10.

It also stipulates that laws that penalize offensive expressions directed at public officials, generally known as "desacato laws," restrict freedom of expression and the right to information.[37] Furthermore, it states that in democratic societies, public figures must be more, not less, open to public scrutiny and criticism and these laws must be repealed where they still exist.[38]

Examples of case law include:

- Herrera-Ulloa v. Costa Rica (ser. C No. 107, July 2, 2004)[39] - IACtHR held that Costa Rica's criminal defamation law violated Article 13 of the ACHR. IACtHR further underlined that by requiring Herrera-Ulloa to prove the statements quoted in his articles, authorities placed an excessive limitation on his freedom of expression. Such a requirement could restrict journalism and have thus a negative impact on public debate.

- Kimel v. Argentina (ser. C No. 177, May 2, 2008)[40] - IACtHR pointed out that expressions concerning the acts carried out by public officials in the exercise of their duties, enjoy a greater degree of protection. The IACtHR established the existence of an obvious public interest in knowing how a public official (a judge in this case) discharged his duties and investigated a massacre perpetrated during the military dictatorship. Furthermore, since the expressions did not concern the public official's private life and were rather part of value judgments on the performance of the judiciary, they should be protected under the ACHR.

3.5 League of Arab States

The Arab Charter on Human Rights is the principal regional human rights instrument for the League of Arab States.[41] It enshrines the right to freedom of expression in Article 32. Its paragraph 2 specifies in which cases this right may be restricted.

In 2014, The Arab Court of Human Rights was established by a Statute, but it is not operational and has not heard any cases yet.

Most of the States from this region have not yet become Parties to the ICCPR, the only applicable provision under global rights instruments (although of a non-binding nature) would be Article 19 of the UDHR which upholds the right of freedom of expression. Together with the Arab Charter on Human Rights, it provides the minimum rights to which persons in this region are entitled.[42] However, the countries of this region have been criticised for enacting cybercrime laws that contain provisions criminalising a wide spectrum of content, using vague language that might create risk of abuse and raise concerns about disproportionate restrictions on freedom of expression.[43]

---

[37] *Ibid.,* principle 11.
[38] *Ibid.,* paragraphs 50, 52.
[39] See IACtHR, Herrera-Ulloa v. Costa Rica, ser. C No. 107, July 2, 2004.
[40] See IACtHR, Kimel v. Argentina, ser. C No. 177, May 2, 2008.
[41] Arab Charter on Human Rights, UN Office of the High Commissioner for Human Rights, League of Arab States, https://digitallibrary.un.org/record/551368?ln=en
[42] HAKMEH, J.: Cybercrime Legislation in the GCC Countries Fit for Purpose?, Chatham House, The Royal Institute of International Affairs, 2018, p. 17.
[43] *Ibid.,* p. 2.

3.6 The Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN) Human Rights Declaration that provides for freedom of expression with more broader restrictions[44] is not a legally binding instrument.
There is also no monitoring mechanism that would have power to issue binding decisions. Nevertheless, those ASEAN member states that are parties to global human rights instruments such as ICCPR, should abide by their obligations under these instruments.

During the COVID 19 pandemic many countries of the region adopted new laws or expanded their fake news/false news laws to counter the crisis and counter spreading of disinformation. Some of their provisions have attracted the interest of the international community and various reviews and recommendations were issued by international bodies. More specifically, these recommendations called for clearly formulated provisions, non-criminal sanctions or not using the laws for political purposes against opponents,[45] including journalists[46].

4 Freedom of expression in the context of action on cybercrime, electronic evidence, and information disorder

4.1 Substantive law offences

The Budapest Convention on Cybercrime remains, at the time of writing, the key international source of legal standards with regard to cybercrime and electronic evidence in criminal cases. The Budapest Convention primarily aims to respond to threats of cybercrime and resolve challenges of electronic evidence in criminal cases by providing guidance and regulations on substantive law, procedural powers and international cooperation, and is also used as a practical tool for criminal justice authorities to enforce criminal justice in cyberspace.

Although the Convention is not a human rights instrument *per se*, as a criminal justice instrument, it is based strongly on the requirements of the rule of law and protection of fundamental rights and freedoms in all aspects of its enforcement. By extension, ensuring that the freedom of expression and related rights are protected and respected falls within the scope of the Convention and its related standards.[47]

[44] "(…) for the purpose of securing due recognition for the human rights and fundamental freedoms of others, and to meet the just requirements of national security, public order, public health, public safety, public morality, as well as the general welfare of the peoples in a democratic society." Association of Southeast Asian Nations (ASEAN), ASEAN Human Rights Declaration, 18 November 2012.
[45] See e.g. Asia Centre, Defending Freedom of Expression: Fake News Legislation in East and Southeast Asia, 2021, 63 p.
[46] See e.g. Asia Centre, Media freedom in South East Asia: Repeal Restrictive Laws, Strengthen Quality Journalism, 2022, 41 p.
[47] Budapest Convention on Cybercrime (2001), Preamble of the Convention. The Preamble to the Budapest Convention already provides an express reference to the freedom of expression and the need to find the proper balance between law enforcement action and protection of fundamental rights. The Preamble also goes further in referencing the European Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations International Covenant on Civil and Political Rights along with other treaties as guidance and reaffirms "the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers."

While each State Party shall criminalise a set of offences contained within the Convention text, the Convention does not provide for an exhaustive list of content-related offences. The First Additional Protocol[48] concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS 189) primarily addresses digital or online content of a racist and xenophobic nature, requiring States Parties to the Protocol to criminalise such offences.

Beyond the provisions of the First Additional Protocol, one notable exception to the neutral approach of the Budapest Convention to illegal content can be found under Article 9 on Offences related to child pornography, where, as per the Explanatory report of the Convention, "the term "without right" allows a Party to take into account fundamental rights, such as freedom of thought, expression and privacy."[49]

4.2 Procedural powers and safeguards

Procedural powers[50] conferred upon the Parties to the Budapest Convention are powerful tools that have the potential to interfere with various rights and freedoms of individuals affected. Therefore, misuse of procedural powers beyond legitimate reasons of criminal investigations could be a risk to the freedom of expression, especially where particularly intrusive measures, such as seizure executed in relation to computer systems and communications equipment (primarily of the media, but also in respect to any individual or legal person) or monitoring/interception, could also be used as a pretext to suppress legitimate opinions, speech or expression.

Article 15 of the Convention requires Parties to ensure that the powers and procedures established under the Convention are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments. Powers and procedures must also be reasonable and "consider the impact on the rights, responsibilities and legitimate interests of third parties", including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact.[51]

Paragraph 3 of Article 19 of the Convention on computer search and seizure empowers competent authorities to seize or similarly secure computer data that has been searched or similarly accessed, including power of seizure of computer hardware and computer data storage media. The official interpretation of the provision is specifically open to the possibility of applying these powers beyond the purposes of gathering evidence to "be applied in situations where danger or social

[48] Available at: https://www.coe.int/en/web/cybercrime/first-additional-protocol. The Protocol establishes the types of content that are, for the States Parties to the Protocol, expressly excluded from the scope of protection accorded by applicable principles of the freedom of expression.

[49] Explanatory Report to the Convention on Cybercrime, section 103. In should be still noted that this potential defence should be, in all circumstances, interpreted and applied within the context of three-part test of legality, proportionality and necessity.

[50] Section 2 of the Convention on Cybercrime. The procedural powers that can be used by the States Parties include expedited preservation, expedited disclosure, production orders, search and seizure, real-time monitoring and interception. While different powers could be applied to secure electronic evidence in a context of a criminal case, Article 15 of the Budapest Convention provides for a set of safeguards and guarantees limiting their application.

[51] Explanatory Report to the Convention on Cybercrime, section 148. It could be thus additionally argued that concept of "rights, responsibilities and legitimate interests of third parties" under paragraph 3 of Article 15 directly refers to other fundamental rights, including freedom of expression. This interpretation is also based on the assumption that practical application of procedural powers, ranging from preservation of data to interception of content, in many cases directly limits the ability of persons to receive, disseminate or share information and data without limitations.

harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography."[52]

4.3 Information disorder

In recent years, disinformation has increased dramatically across the world. While providing for a plurality of voices, a democratisation of access to information and a powerful tool for activism, the Internet also created new technological vulnerabilities. False content has a potentially damaging impact on core human rights and even the functioning of democracy. Disinformation can serve to confuse or manipulate citizens, create distrust in international norms, institutions or democratically agreed strategies; disrupt elections; or fuel disbelief in key challenges such as climate change.[53]

The Council of Europe addresses "disinformation" as verifiably false, inaccurate or misleading information deliberately created and disseminated to cause harm or pursue economic or political gain by deceiving the public, while "misinformation" would refer to verifiably false, inaccurate or misleading information disseminated without an intention to mislead, cause harm, or pursue economic or political gain[54]. UNESCO also[55] adds "mal-information" as information that is based on reality, used to inflict harm on a person, social group, organization or country.

States have been trying to counter disinformation through different tools, including by introducing new legislation and criminalising specific behaviours online. This, in some cases, happens at the detriment of the right to freedom of expression.

The Venice Commission, in its opinion no. 1102 / 2022[56] regarding the provision on "false or misleading information", acknowledged that information disorder (misinformation, disinformation and mal-information) is indeed one of the important issues of these days since online platforms have become wide-open channels for private and public debate. Hatred and other harmful speech are spreading through them with the help of manufactured amplification and there is a global need to tackle the serious problems of disinformation campaigns, with presumed impact on election results and subsequently on governments and the constitutional order of states.

However, introducing measures to counter disinformation carries serious risks of interfering with freedom of expression and careful consideration is required when identifying solutions to this global problem as they can lead to censorship and limit legitimate content. Moreover, the criminalisation of disinformation can be used by governments against criticism and opposition, causing self-censorship and limiting freedom of expression.[57]

[52] *Ibid*, section 198. A set of specific conditions and safeguards could be necessary in this respect, precluding application of this power to enable takedowns or otherwise rendering inaccessible of information that could be deemed "illegal" under national law but otherwise protected under the freedom of expression; such safeguards should include, at the very least, the three-part test of legality, proportionality and necessity.

[53] The impact of disinformation on democratic processes and human rights in the world, Study of the EU Parliament, 2021.

[54] See Committee of Experts on the Integrity of Online Information (MSI-INF), Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, December 2023.

[55] Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training (unesco.org).

[56] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PI(2022)032-e.

[57] "General prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression (…) and should be abolished." Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies.

In the recommendation of the Council of Europe Committee of Ministers to member States on combating hate speech[58], criminalisation should also be used as last resort and only for the most serious expressions of hate speech, clearly defined. Member States should use clear and precise terminology and definitions, and refrain from using vague[59] and blanket[60] terms in their legislation addressing hate speech.

The 2018 EU Report "Tackling Online Disinformation: A European Approach"[61] underlined that the main threat is disinformation, not 'fake news' or misinformation and, even against the most serious threat, the response should include a multi-stakeholder approach, and not merely the criminalisation of certain behaviours.

5 Challenges and solutions on cybercrime and freedom of expression in national legislation and practice

The objective of this part is to demonstrate application of principles identified above to specific circumstances in legislation and practice.

5.1 Countering disinformation

New laws in different regions of the world, adopted or amended to fight cybercrime have been used by governments to introduce criminal offences that do not refer to cybercrime but try to counter disinformation. In some cases, they are alleged to have been misused to crack down on political dissent and suppress freedom of expression and the media, further undermining already compromised democratic structures and institutions. In other instances, laws are interpreted liberally by courts to label journalists' findings that question, for example, corruption in the public sector as disinformation.

5.1.1 Issues

- Criminalisation of conducts that refer generically to spreading of information online.
- Use of vague, broad, confusing terminology when referring to both the description of the criminal conduct and of the value/interest protected; this also includes interpretation by the courts of law of otherwise generally worded provisions.
- Criminalisation of defamation, with severe sanctions and lack of consideration of alternative civil and/or administrative sanctions.

and Elections, CDL-AD(2019)016.

[58] Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech - Freedom of Expression (coe.int).

[59] "Misleading information" (if relevant), "false information to mislead," "publicly disseminating" (or "overtly disseminating"), "disturbance of the public peace", "general well-being" (or "public health" or "general health"), "in a way conducive" (or "in a manner conducive"), "within the framework of the activities of an organisation". Examples taken from: Venice Commission, Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe, 7 October 2022, para 39.

[60] Such as "false news" or "non-objective information". See e.g. Venice Commission, Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, CDL-AD(2019)016, para. 90.

[61] With updates as of 2023, at https://digital-strategy.ec.europa.eu/en/node/3060/printable/pdf.

- Lack of clarity on procedural powers in relation to investigation/prosecution of the introduced offences.
- Introduction of offences that are already regulated in other domestic legislation offline (e.g. extortion, attack on public order etc.).
- Lack of consideration of existing domestic legislation, already protecting citizens or state/s interest at stake.

5.1.2 Solutions

- Criminalisation used only as a last resort.
- Clear and precise terms of the criminal conduct and of the value/interest protected.
- Consider decriminalisation of defamation or using non-custodial sentencing commensurate to societal/individual harm.
- Use of procedural powers proportionate to the conduct in question, with applicable safeguards and guarantees.
- Minimising regulation where already covered by law.

5.2 Clarity of the law

Legal certainty and quality of the law are crucial in setting limitations on the freedom of expression. Qualitative requirements of accessibility and foreseeability should apply,[62] so that the law is foreseeable if it is formulated with sufficient precision to enable the citizen to regulate their conduct, i.e. to foresee the consequences of a given action.[63] In other words, the wording of the law has to be sufficiently clear.[64]

5.2.1 Issues

- Vague language of prohibited speech: no exact definitions of terms provided for by law or no criteria in the law against which it is possible to make the assessment objectively and consistently. For example, terms such as “false statements”, “false information to mislead,” “overtly disseminating”, “disturbance of the public peace”, “general well-being”, “in a way conducive”, “within the framework of the activities of an organisation”, “insults[65] ”, “harassment”.
- Overbroad language: Even though terms are defined, they offer a very broad interpretation. Examples include “rumours that may make a person lose their credibility” or “obscene, lewd, lascivious or indecent proposals, suggestions or requests”.
- There are concerns about the extent to which the national legal systems have a clear understanding of what constitutes ‘indecent’ material, “repeatedly”, instilling “reasonable

[62] See, for example, ECtHR, Delfi AS v. Estonia, [GC],16 June 2015, no. 64569/09, paragraph 120, and VgT Verein gegen Tierfabriken v. Switzerland, 28 June 2001, no. 24699/94, paragraph 52.

[63] Delfi AS, ibidem, para. 121. The relevant law is foreseeable, when “the applicant’s act, at the time when it was committed, constituted an offence defined with sufficient precision by domestic and/or international law to be able to guide the applicant’s behaviour and prevent arbitrariness” (Žaja v. Croatia, 4 October 2016, no. 37462/09, paragraph 93, with further references).

[64] See detailed analysis in the Case-law guide of the ECtHR on freedom of expression (Article 10 ECHR). In addition, if the law criminally sanctions a certain conduct, the lack of specificity could further entail the violation of the principle of legality (*nullum crimen sine lege*) as granted by Article 7 ECHR.

[65] Ideas or beliefs from ridicule, abuse, criticism, or other ‘attacks’ seen as offensive are protected under international law. See UN General Assembly, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,” paragraph 21, UN Doc. A/74/486 (9 October 2019).

fear" and how this should be determined, as the concepts are not defined by law or jurisprudence.

- Consequence: Very broad provisions may apply to a variety of circumstances, both online and offline.[66]
- Risk of criminalising news reporting by journalists based on interviews or declarations by others.

5.2.2 Solutions

- Scope of application of respective provisions should be clarified through the use of clearly defined terms.
- Criteria to assess the authenticity of the content to be included in the law.
- Limiting the scope of the criminalisation: restricting the applicability of the provision, requiring specific intent of the perpetrator.
- Provisions should be limited only to statements of facts and not to value judgements (as expressions of an opinion). The latter cannot be tested as true or false.
- If intermediaries may be held criminally liable for assisting with dissemination (ISPs including social media platforms) of illegal content online and under what circumstances, those questions should be answered directly in the law.[67]
- The punishment of a journalist for assisting in the dissemination of statements made by another person should not be envisaged since it would seriously hamper the contribution of the press to the discussion of matters of public interest.[68] The imposition of a prison sentence for a press offence is only permissible in exceptional circumstances, notably where other fundamental rights have been seriously impaired, for example, in the case of hate speech or incitement to violence.[69]

5.3 Necessity, proportionality, pressing social need

Information disorder (misinformation, disinformation and mal-information) is indeed one of the important issues since in the online environment information and hate is spread more easily. There is a global need to tackle such problems in cyberspace, especially when it comes to disinformation campaigns, with presumed impact on election results and on governments and the constitutional order of states.[70]

That said, it needs to be established whether there is a pressing social need and whether the interference is "proportionate to the legitimate aim pursued". There may be, in principle, a pressing social need to regulate certain aspects of spreading illegal content online: for example, spreading

[66] These circumstances may vary from a public statement in the context of a conference to a "like" or "retweet" in the virtual world. The border between public and private spheres in the online environment is blurred. Does a post on Facebook accessible only to one´s Facebook friends amount to "public dissemination"? See e.g. Venice Commission, Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe, 7 October 2022, paragraph 47.
[67] Note however that in the ER to the First Additional Protocol to the Budapest Convention it is stated that persons cannot be held criminally liable for any of the offences in this Protocol, if they have not the required intent. See paragraphs 25 and 45 of the ER to the First Additional Protocol to the Budapest Convention.
[68] See e.g. ECtHR, Kuliś v. Poland, 18 March 2008, no. 15601/02, pararaph 38, Thoma v. Luxembourg, 29 March 2001 no. 38432/97, paragraph 64, or Saygili and Falakaoğlu v. Turkey, 21 October 2008, no. 39457/03, paragraph 23.
[69] Council of Europe Committee of Ministers, Recommendation CM/Rec(2016)4, on the protection of journalism and safety of journalists and other media actors, paragraph 6.
[70] See for example, Venice Commission, CDL-AD(2019)016, Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, paragraph 99.

of disinformation may endanger important public interests (for example national security, public safety, public order or public health), or deliberate dissemination of disinformation considered an abuse of freedom of expression and the right to impart information.

It needs to be looked how the domestic legal framework regulates the issues at stake (some aspects of the illegal conduct may be already regulated through other domestic laws) and whether introduction of new criminal provisions is needed: assessing whether there are less restrictive means and measures available to pursue the stipulated legitimate aims, and recognising the importance of using the least restrictive measure when addressing a pressing social need.

In order for a measure to be considered proportionate and necessary in a democratic society, there must be no other means of achieving the same end that would interfere less seriously with the fundamental right concerned.[71]

5.3.1 Issues

- Non limitation of the scope and fact that the provisions may apply to any individual (journalists, activists, politicians, critics of the government, service providers, any individuals).
- The chilling effect, risk of self-censorship and the right to anonymity on the Internet (in particular in times of elections).
- Criminal sanctions may not be proportionate, since there is a risk they may constitute a form of (self-)censorship intended to discourage the press from expressing criticism.[72]
- Increased maximum sentence if the offence is committed anonymously.[73]

5.3.2 Solutions

- Using other less intrusive means alternative to criminalisation. For example, requiring service providers to promptly remove illegal content upon complaint. Further measures to consider: reporting systems; the transparency of algorithms; existing fact-checking partnerships or initiatives; establishing how to deal with sponsored content, etc.
- Establishment of specialised units to counter dissemination of illegal content online.
- Quick and effective refutations of false claim publicly through various means (including through social media).

5.4 Use of procedural powers

Procedural powers to secure and access electronic evidence are highly specialised tools that often determine the success of investigations into the cases of cybercrime but also other criminal offences where electronic evidence plays a key role.

However, application of specific measures may be highly intrusive in terms of privacy, thus creating additional risks for the freedom of expression. This is even more relevant in cases where substantive law establishes vague exceptions to the freedom of speech and expression as criminal

[71] ECtHR, Glor v. Switzerland, 30 April 2009, no. 13444/04, para. 94.
[72] ECtHR, Bédat v. Switzerland, [GC], 29 March 2016, no. 56925/08, paragraph 79.
[73] "Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet", ECtHR, Delfi AS v. Estonia, [GC],16 June 2015, no. 64569/09, paragraph 147.

offences, enabling the possibility for such powers to be applied in the context of criminal investigations. Lack of proper safeguards and guarantees multiplies such risks even further.

5.4.1 Issues

- Criminalisation of sharing of information that is false, deceptive, misleading or inaccurate, without context or clarity.
- Lack of judicial oversight for search and seizure of computer systems and data.
- Police discretion of whether to seek judicial authorisation for oversight while engaging in surveillance and use of forensic tools in criminal investigations.
- Already established practice of discretionary procedural powers used against political opposition and civil society in the context of ongoing elections.

5.4.2 Solutions

- Legislation should be clear and precise.
- Criminalisation in respect to free speech should be the last resort.
- Judicial oversight should be applicable to all procedural powers that are intrusive, such as search and seizure and interception/monitoring.
- Such oversight should not be discretionary but compulsory, leading not only to inadmissibility of collected evidence but also possibilities to seek remedies against misuse of procedural powers.
- Use of intrusive procedural powers in respect of sensitive and vulnerable groups should be strictly regulated.

5.5 Excessive criminalisation/proportionality

In a specific set of legal discussions ongoing for several years, the judicial system affirmed the principle of proportionality in relation to the offence of online libel. This positive example further reinforces the need for proper judicial oversight and access to justice as crucial elements to protect the freedom of expression.

5.5.1 Issues

- Criminal liability for Facebook posts alleging corruption of public officials may be permissible exception to the freedom of expression.
- The criminal sanctions for online libel/defamation were set higher than for the “traditional” offences.
- Imprisonment for online libel, in theory, was argued to be a mandatory sentencing option. For traditional libel, a fine can be imposed in lieu of imprisonment.

5.5.2 Solutions

- Discrepancies between online and traditional offences are unjustified, especially where milder sentencing is applied in the latter case.
- Even where only monetary sanctions are used, the amount should be proportionate to the offence in question.
- Peculiar circumstances of each case should dictate the degree of sentencing, rather than rigid application of mandatory thresholds in question.

6 Considerations

6.1 Considerations for legislators

- The **three-tier test of test of legality, proportionality and necessity** is the key safeguard against excessive limitations on the freedom of expression. Such restrictions should be always:

  - prescribed by law;
  - serve a legitimate aim; and
  - necessary and proportionate means to achieve the stated aim in a democratic society.

  Independent oversight (judicial or similar) to verify application of the three-tier test is necessary, as majority of the case law on the subject matter relate to one or several parts of this test not being complied with.

- **Clear and precise legislation and use of terms** should be ensured to avoid any ambiguous interpretation. The laws must be:
  - clear, precise, accessible and foreseeable;
  - overseen by an independent body in a manner that is not arbitrary or discriminatory; and
  - effectively safeguard against abuse including through the courts.

  Laws limiting the freedom of expression should not be used by the State to specifically target opposition, journalists and minorities/vulnerable groups. Any person whose right it is interfered with, shall have the right to recourse to the court of law.

6.2 Considerations for policy makers

- **Follow best practice of establishing permissible and impermissible exceptions** to the freedom of speech in line with globally agreed principles. In terms of criminalisation of conduct, consider the standard set by the UN Special Rapporteur on *permissible* (child abuse material, incitement to genocide, discriminatory speech and incitement to terrorism) and *impermissible* (government policies/political debate; reporting on human rights, government activities and corruption in government; election campaigns, peaceful demonstrations or political activities; expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups) exceptions to the freedom of speech.

- **Public figures shall be required to tolerate a greater degree of criticism.** Both law and practice should ensure that public officials have a higher degree of tolerance toward criticism, whether justified or unjustified, and criminal justice should not be used by default to tackle such criticism.

- **Consider multistakeholder approach to combating disinformation**. Proper reporting, self-regulation initiatives, fact-checking partnerships, transparency of

algorithms and decision-making, and, in general involvement of the industry and civil society can bear more effective results rather than targeting every instance with criminal justice action.

6.3 Considerations for criminal justice practitioners

- **Criminal law needs to be used as a last resort for addressing both disinformation and defamation, as well as any other type of speech and expression that does not necessitate criminal liability or sanctions**. Universal and regional instruments, applicable case law and other legal documents (such as The Declaration of Principles of Freedom of Expression and Access to Information in Africa) could provide good guidance in this respect. Criminal provisions on defamation and libel should, if applied in practice, be punishable by monetary or similar sanctions not involving deprivation of liberty.

- **Procedural powers applicable to electronic evidence should be always used subject to relevant safeguards and guarantees, most importantly under independent judicial oversight.** Misuse of powers should be prevented by legislating and applying strong safeguards and opportunities for redress available should such abuse happen. Discussions on takedown and blocking of infringing content should be expressly separated from the matters of legislation implementing the Budapest Convention.