Vienna/Warsaw, 5 December 2025

Joint Opinion-Nr.: FOE-UZB/550/2025 [NS]

JOINT OPINION ON THE DRAFT LAW OF UZBEKISTAN ON THE PROTECTION OF USERS' RIGHTS ON ONLINE PLATFORMS AND WEBSITES

UZBEKISTAN

This legal analysis was prepared jointly by the Office of the OSCE Representative on Freedom of the Media and by the OSCE Office for Democratic Institutions and Human Rights.

This Opinion has benefited from contributions made by Ms**. Nevena Krivokapic Martinovic**, Coordinator for Freedom of Expression and Online Media at SHARE Foundation; and **Dr. Paolo Cavaliere**, Senior Lecturer of Law at the University of Edinburgh Law School.

Based on an unofficial English translation of the Draft Law provided by the requesting authority.

Office of the OSCE Representative on Freedom of the Media

Wallnerstrasse 6, 1010 Vienna, Austria
Office: +43 1 514 36 6800
https://www.osce.org/representative-on-freedom-of-media

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw
Office: +48 22 520 06 00,
www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

The regulation of digital platforms has become a global concern, as states seek to balance legitimate public interests, such as national security, public order, and the protection of rights of others, with the need to safeguard fundamental freedoms online, including freedom of expression, access to information, privacy, personal data protection and non-discrimination.

While the stated objective of the Draft Law to protect the rights of users in digital spaces is welcome in principle and the Draft Law presents a number of positive features, including safeguards related to transparency of online advertising, protection against deceptive platform practices, accessibility for persons with disabilities, enhanced user information on privacy and algorithmic systems, and a procedural safeguard granting platforms, users, and website owners the right to judicial review of regulatory measures, with suspensive effect, several of its provisions raise concerns from a human rights perspective.

In particular, the definitions of "unlawful content" and "false information" are overly broad and vague, falling short of the principle of legal certainty. In the absence of narrowly tailored definitions and robust procedural safeguards, the Draft Law risks enabling arbitrary enforcement, the suppression of legitimate online expression, and the institutionalization of a chilling effect in the online sphere.

These substantive concerns are compounded by structural deficiencies in the regulatory model, with the authorised body lacking clear guarantees of independence, contrary to international standards and recommendations. The Draft Law also fails to place meaningful limits on the powers of the authorized body, i.e., the Agency on Information and Mass Communication under the Presidential Administration.

Of particular concern, Article 17(3), which permits the wholesale blocking of websites, even when only part of the content is deemed unlawful, contradicts the principle of proportionality. This is without prejudice to cases involving content that is illegal under international law and human rights standards, where expedited measures are required in accordance with the conditions prescribed by international human rights law, provided that *ex post* judicial remedies are available to review the legality, necessity and proportionality of those measures.

The Draft Law could also more explicitly embed the responsibility of private actors to respect human rights in their activities and operations, including freedom of expression, access to information, privacy, and non-discrimination.

More specifically, and in addition to what is stated above, OSCE RFoM and ODIHR makes the following recommendations to further enhance the Draft Law's compliance with international human rights standards:

A. To explicitly incorporate in Article 6 of the Draft Law the principle of independence of the authorised body responsible for protecting users' rights on online platforms and websites, while ensuring that the legal framework

governing the establishment and functioning of such a body incorporates safeguards to guarantee its independence, including transparent, merit-based appointment and removal of leadership, with adequate safeguards against external interferences, especially from political actors; clearly defined mandates and statutory powers to prevent discretionary, arbitrary or discriminatory implementation; budgetary autonomy; internal procedures guaranteeing independent decision-making; and judicial or external independent review of regulatory actions for legality, legitimacy, necessity and proportionality; [para 28]

B. Regarding definitions:

1. to more clearly distinguish the concepts of "false information", "misinformation" and "disinformation" while ensuring that the latter only includes the type of false information, which is verifiably false and disseminated deliberately or recklessly with the intent, or reasonably foreseeable consequence, of causing harm to human rights and/or legitimate interests - such as public health, electoral processes, environment or national security, while explicitly excluding from its scope value judgments as well as satire and parody; [para 55]
2. to clarify the definition of "online platform" by reflecting the core function of enabling users to connect, interact, and disseminate information; and by enumerating examples of relevant services (e.g. social networks, search engines, video-sharing services); [para 63]

C. Regarding functions and duties of online platforms:

1. to enhance Article 7 of the Draft Law by incorporating precise content categories of material and information genuinely harmful to children and related safety measures or by delegating specifics to guidelines to be issued by the authorized body; [para 80]
2. to clarify in the Draft Law whether online platforms lose immunity from liability upon receiving user notices and gaining actual knowledge or awareness about content deemed unlawful; [para 87]
3. to expand the list of data categories for which profiling is prohibited under Article 11 of the Draft Law to also cover religious or other beliefs, trade union membership, and sexual orientation or sex life, thereby ensuring comprehensive protection of users' rights and preventing discriminatory profiling practices; [para 91]
4. to clarify procedural requirements for a submission mechanism of user complaints in Article 10 of the Draft Law, ensuring online platforms provide adequate and easily accessible information for the users about the complaint mechanism; establish clear, transparent, free of charge, user-friendly, accessible submission channels, timely acknowledgment and processing of complaints, proper documentation and tracking of complaints, and proportionate obligations for platforms based on their size; [para 93]

D. Regarding rights and obligations of online users and website owners:

1. to amend Article 18 (3) of the Draft Law by ensuring that, like the owners of online platforms and website owners, users also have the right to submit

observations on the findings issued by the Agency when challenging the orders and directives of the authorized body in a court of law; [para 95]

2. to amend Article 22 (1) (3) of the Draft Law by qualifying the liability model and adopting a more flexible and proportionate framework regarding liability of influencers and website owners for third-party content, considering such factors as the nature and severity of content, size and commercial purpose of the platform, possibility of identifying the original author, measures taken to prevent harmful dissemination; [para 98]
3. to amend Article 22 (1) (6) of the Draft Law to require that any request of individuals or entities to publish retractions should be accompanied by the related court decision ordering the publication of a retraction; [para 99]

E. Regarding unlawful content:

1. to remove the reference to vague and/or broad content-based restrictions, such as the promotion of "extremism" and "fundamentalism" – unless clearly linked to some elements of violence or other criminal means or incitement to violence as defined in accordance with international human rights standards; [para 111]
2. to include in the Draft Law the balancing test stipulating that disclosure of classified information shall not be punishable by law if public interest in such disclosure outweighs/prevails over potential harm resulting from it, while providing for an explicit public interest exemption – ensuring that disclosures made for the purpose of exposing human rights abuses, public wrongdoing, corruption, abuse of power, or other serious violations of law are not prohibited or penalised; [para 117]
3. to consider broadening the scope of prohibited expression of hatred that constitutes incitement to discrimination, hostility or violence to cover other grounds, beyond national, racial or religious hatred, including characteristics such as colour, language, nationality, national or ethnic origin, age, disability, sex, gender identity, and sexual orientation; [para 118]
4. to supplement Article 13 with a clear prohibition of online violence against women, in particular, of the non-consensual distribution of intimate images, online harassment and stalking, including the threat to disseminate non-consensual images or content; [para 120]

F. Regarding legal consequences for distribution of unlawful content:

1. to reconsider the Draft Law provisions allowing the blocking of entire websites based on a single item of unlawful content e.g. a single failure to comply with the removal order, as this may violate the principle of proportionality, and instead consider more targeted measures, such as blocking specific illegal material, with whole-site blocking permitted only in narrowly defined cases and with separate, specific justification; [para 130]
2. to clarify the meaning of "systematic failure" as referred to in Article 16 of the Draft Law as a basis to file the claim with the court seeking reduction of an online platform's data transmission rate; [para 132]
3. to consider including in the Draft Law a possibility to request a correction of inaccurate information instead of an outright removal to protect the integrity of public discourse while balancing the right to reputation with freedom of expression; [para 133]

4. to require in Article 20 of the Draft Law that the applicants provide evidence demonstrating the falsity of the information in order to request its removal. [para 134]

These and additional Recommendations, are included throughout the text of this Opinion, highlighted in bold.

According to the mandate, OSCE Representative on Freedom of the Media assists the OSCE participating States in their continuing commitment to the furthering of free, independent and pluralistic media including inter alia by providing legal reviews of draft and existing laws.

As part of its mandate to assist OSCE participating States in implementing their OSCE human dimension commitments, ODIHR reviews, upon request, draft and existing laws to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENTS

I. INTRODUCTION

1. On 26 May 2025, the First Deputy Director of the Agency on Information and Mass Communication under the Administration of the President of the Republic of Uzbekistan (hereinafter "Agency") sent to the OSCE Representative on Freedom of the Media (hereinafter "RFoM") a request for a legal review of the Draft Law of Uzbekistan on the Protection of Users' Rights on Online Platforms and Websites (hereinafter "the Draft Law").
2. On 18 June 2025, RFoM responded to the Agency confirming readiness to prepare a legal analysis of the Draft Law to assess the compliance of the Draft Law with international human rights standards and OSCE human dimension commitments.
3. On 23 June 2025, as per an established practice, RFoM invited the OSCE Office for Democratic Institutions and Human Rights (hereinafter "ODIHR") to prepare a Joint Opinion drawing on both institutions' expertise and respective mandates, to which ODIHR responded positively on 30 June 2025.
4. This Joint Opinion was prepared in response to the above request. RFoM and ODIHR conducted this assessment within their respective mandates to assist OSCE participating States in the implementation of their OSCE human dimension commitments.[1]

II. SCOPE OF THE JOINT OPINION

5. The scope of this Joint Opinion covers only the Draft Law submitted for review. Thus limited, the Joint Opinion does not constitute a full and comprehensive review of the entire legal and institutional framework governing online platforms and websites, freedom of expression, access to the Internet and freedom of the media in Uzbekistan.
6. The Joint Opinion raises key issues and provides indications of areas of concern. In the interest of conciseness, it focuses more on those provisions that require amendments or improvements than on the positive aspects of the Draft Law. The ensuing legal analysis is based on international and regional human rights standards, norms and recommendations as well as relevant OSCE human dimension commitments. The Joint Opinion also highlights, as appropriate, good practices from other OSCE participating States in this field. When referring to national legislation, RFoM and ODIHR do not advocate for any specific country model; they rather focus on providing clear information about applicable international standards while illustrating how they are implemented in practice in certain national laws. Any country example should always be approached with caution since it cannot necessarily be replicated in another country and has always to be considered in light of the broader national institutional and legal framework, as well as country context and political culture.

See, in particular, Copenhagen 1997 (Annex 1: Permanent Council Decision No. 193, Mandate of the OSCE Representative on Freedom of the Media). See also the CSCE/OSCE, Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE (Copenhagen Document), CSCE/OSCE, 29 June 1990), para. 9.1; Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE, (Moscow Document), CSCE/OSCE, 3 October, 1991, paras. 9.1 and 26; and CSCE Budapest Document 1994, Towards a Genuine Partnership in a New Era (Budapest Document), CSCE/OSCE, 21 December 1994, Chapter VIII, para. 36. See also OSCE Ministerial Council Decision No. 3/18, "Safety of Journalists", 12 December 2018, p. 3, which calls upon OSCE participating States to *"[b]ring their laws, policies and practices, pertaining to media freedom, fully in compliance with their international obligations and commitments and to review and, where necessary, repeal or amend them so that they do not limit the ability of journalists to perform their work independently and without undue interference (…).*"

7. Moreover, in accordance with the *Convention on the Elimination of All Forms of Discrimination against Women*[2] (hereinafter "CEDAW") and the *2004 OSCE Action Plan for the Promotion of Gender Equality*[3] and commitments to mainstream gender into OSCE activities, programmes and projects, the Joint Opinion integrates, as appropriate, a gender and diversity perspective.

8. This Joint Opinion is based on an unofficial English translation of the Draft Law provided by the Agency, which is attached to this document as an Annex. Errors from translation may result. Should the Joint Opinion be translated in another language, the English version shall prevail.

9. In view of the above, RFoM and ODIHR would like to stress that this Joint Opinion does not prevent RFoM and ODIHR from formulating additional written or oral recommendations or comments on respective subject matters in Uzbekistan in the future.

III. LEGAL ANALYSIS AND RECOMMENDATIONS

1. Relevant International Human Rights Standards and OSCE Human Dimension Commitments

10. The right to freedom of expression and to receive and impart information is a fundamental right, as well as an enabler of other human rights and fundamental freedoms and a guardian of democratic values.[4] The full enjoyment of this right is one of the foundations of a free, democratic, tolerant and pluralistic society in which individuals and groups with different backgrounds and beliefs – including historically marginalized and underrepresented segments of society – can voice their opinions and participate freely in public affairs. The right to freedom of expression, along with the existence of free, independent and pluralistic media, is also necessary for facilitating the effective and well-informed participation of citizens in the conduct of public affairs and holding government accountable. While underlining the importance of protecting the right to freedom of expression and access to information, it should also be balanced with the protection of individuals' reputation, the need to ensure equality and non-discrimination, and legitimate public interests as stipulated by relevant international human rights treaties.

11. The right to freedom of expression and to receive and impart information is enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR)[5] and is guaranteed by Article 19 of the International Covenant on Civil and Political Rights (ICCPR),[6] which provides that *"everyone shall have the right to hold opinions without interference"* and that *"everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."* Article 19 of the ICCPR establishes the principle of medium

2 *UN Convention on the Elimination of All Forms of Discrimination against Women* (hereinafter "CEDAW"), adopted by General Assembly resolution 34/180 on 18 December 1979. Uzbekistan deposited its instrument of ratification of this Convention on 20 July 1981.

3 See *OSCE Action Plan for the Promotion of Gender Equality*, adopted by Decision No. 14/04, MC.DEC/14/04 (2004), para. 32.

4 See UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur and the African Commission Special Rapporteur on Freedom of Expression and Access to Information (hereinafter "International Mandate-Holders on Freedom of Expression"), *Joint Declaration on Media Freedom and Democracy*, 2 May 2023.

5 See the *Universal Declaration of Human Rights* (UDHR), United Nations, General Assembly resolution 217 A. adopted 10 December 1948, Article 19.

6 See *International Covenant on Civil and Political Rights* adopted by the UN General Assembly by resolution 2200A (XXI) of 16 December 1966. Uzbekistan ratified the Covenant on 28 September 1995.

neutrality by noting that these rights can be exercised regardless of the medium used. Freedom of the media is derived from freedom of expression, since the media and journalists are regarded as important "deliverers" of public interest information and facilitators of public debate. In General Comment No. 34 on Article 19 of the ICCPR, the UN Human Rights Committee further underlines the essential role of a free, uncensored and unhindered press or other media as a cornerstone of a democratic society, also elaborating recommendations pertaining to legislative and administrative frameworks for the regulation of the mass media.[7]

12. The right to freedom of expression is not absolute and can be limited under specific circumstances. Restrictions on the right to freedom of expression must, however, be compatible with the strict requirements set out in Article 19 (3) of the ICCPR. Notably, they must be provided by law (test of legality), pursue one of the legitimate aims listed exhaustively in the text of Article 19 (3)[8] (test of legitimacy), be necessary and proportionate, and constitute the least intrusive measure among those effective enough to reach the designated objective (test of necessity and proportionality). In addition, pursuant to Article 26 of the ICCPR, restrictions shall not be discriminatory. The requirement that restrictions to freedom of expression need to be provided by law means not only that restrictions need to be based on a law, but such law must also be precise, certain and foreseeable. Laws need to be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[9] Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific aim(s) they are pursuing. Additionally, Article 20 of the ICCPR requires states to outlaw any propaganda for war and "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence".

13. While Uzbekistan is not a Member State of the Council of Europe (CoE), Article 10 of the European Convention on Human Rights and Fundamental Freedoms (ECHR),[10] the case law of the European Court of Human Rights (ECtHR) in the field of freedom of expression and freedom of the media, and other CoE instruments, as well as related documents such as opinions of the European Commission for Democracy through Law of the CoE (Venice Commission) may nevertheless be relevant, persuasive and useful from a comparative perspective.[11] In particular, for the purposes of protecting users' rights online and media regulation, a number of CoE Recommendations are highly relevant and may serve as examples of regional good practice, such as the Recommendations on the roles and responsibilities of internet intermediaries,[12] on the impacts of digital technologies on freedom of expression,[13] on the human rights impacts

7 UN Human Rights Committee, General Comment No. 34 *"*on Article 19 Freedoms of Opinion and Expression of the ICCPR", CCPR/C/GC/34, 12 September 2011, in particular paras. 13-18 and 39-42.

8 i.e., (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public), or of public health or morals.

9 See UN Human Rights Committee, General Comment No. 34 *"*on Article 19 Freedoms of Opinion and Expression of the ICCPR", CCPR/C/GC/34, 12 September 2011, para. 25, which states: "*a norm, to be characterized as a 'law', must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.*" See also, e.g., ODIHR, Guidelines on Democratic Lawmaking for Better Laws, ODIHR, 16 January 2024, para. 12 and Principle 16; and Venice Commission, Rule of Law Checklist, CDL-AD(2016)007, 18 March 2016, para. 58. In addition, see, for the purpose of comparison and example of good regional practice, European Court of Human Rights (ECtHR), *The Sunday Times v. the United Kingdom (No. 1)*, no. 6538/74, 26 April 1979, where the Court ruled that "*the law must be formulated with sufficient precision to enable the citizen to regulate his conduct, by being able to foresee what is reasonable and what type of consequences an action may cause*."

10 See European Convention on Human Rights (ECHR), Council of Europe, entered into force on 3 September 1953, Article 10.

11 See documents available at <https://www.coe.int/en/web/freedom-expression/media>.

12 See CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018.

13 See CoE Recommendation CM/Rec(2022)13, "Recommendation of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression", Council of Europe, Committee of Ministers, adopted on 6 April 2022.

of algorithmic systems,[14] on a Guide to Human Rights for Internet users,[15] on a New Notion of Media,[16] on Gender Equality and Media[17] and on Principles for Media and Communication Governance.[18]

14. Similarly, while Uzbekistan is not a member of the European Union (EU), references are made to relevant EU regulations for illustrative and comparative purposes, especially the Digital Services Act, since some of the provisions of the Draft Law seem to mirror part of its content.

15. At the OSCE level, there are a number of commitments in the area of freedom of expression, access to information and freedom of the media. In particular, the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE in 1990 (1990 Copenhagen Document) proclaims the right of everyone to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. Restrictions to the exercise of this right are only possible if they are prescribed by law and consistent with international standards.[19] OSCE participating States also reaffirmed *"the right to freedom of expression, including the right to communication and the right of the media to collect, report and disseminate information, news and opinion"* in paragraph 26 of the Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE (1991 Moscow Document).[20] Moreover, in 1994 in Budapest, OSCE participating States reiterated that "*freedom of expression is a fundamental human right and a basic component of a democratic society*" committing to *"take as their guiding principle that they will safeguard this right"* and emphasizing in this respect, that *"independent and pluralistic media are essential to a free and open society and accountable systems of government*".[21]

16. In its Decision 3/18, adopted on 7 December 2018, the OSCE Ministerial Council called upon the OSCE participating States to fully implement all OSCE commitments and international obligations related to freedom of expression and media freedom and to make their laws, policies and practices pertaining to media freedom fully compliant with their international obligations. In particular, the Decision noted that, where necessary, States should review, repeal or amend such laws, policies or practices "*so that they do not limit the ability of journalists to perform their work independently and without undue interference (…).*"[22]

17. The OSCE RFoM is specifically mandated to observe relevant media developments in all OSCE participating States and to advocate and promote full compliance with OSCE principles and commitments regarding freedom of expression and free media,[23] including in online spaces. The OSCE RFoM, together with the freedom of expression mandate-holders from the UN, the African Commission on Human and Peoples' Rights (African

14 See CoE Recommendation CM/Rec(2020)1, "Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems", Council of Europe, Committee of Ministers, adopted on 8 April 2020.
15 See CoE Recommendation CM/Rec(2014)6, "Recommendation of the Committee of Ministers to member States on a Guide to human rights for Internet users", Council of Europe, Committee of Ministers, adopted on 16 April 2014.
16 See CoE Recommendation CM/REC(2011)7, "Recommendation of the Committee of Ministers to member States on a new notion of media", Council of Europe, Committee of Ministers, adopted on 21 September 2011.
17 See CoE Recommendation CM/Rec(2013)1, "Recommendation of the Committee of Ministers to member States on gender equality and media", Council of Europe, Committee of Ministers, adopted on 10 July 2013.
18 See CoE Recommendation CM/REC(2022)11, "Recommendations of the Committee of Ministers to member States on principles for media and communication governance", Council of Europe, Committee of Ministers, adopted on 6 April 2022.
19 See Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE (Copenhagen Document), CSCE/OSCE, 29 June 1990), para. 9.1.
20 See Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE, (Moscow Document), CSCE/OSCE, 3 October, 1991, para. 26.
21 See CSCE Budapest Document 1994, Towards a Genuine Partnership in a New Era (Budapest Document), CSCE/OSCE, 21 December 1994, Chapter VIII, para. 36.
22 See OSCE Ministerial Council Decision No. 3/18, "Safety of Journalists", 12 December 2018, p. 3.
23 See, Copenhagen 1997 (Annex 1: Permanent Council Decision No. 193, Mandate of the OSCE Representative on Freedom of the Media).

Union) and the Organization of American States, have adopted a series of Joint Declarations, which offer practical guidance covering current universal challenges to freedom of expression and freedom of the media.[24] Importantly, the *2023 Declaration on Media Freedom and Democracy* outlines the broader legal and policy framework necessary to ensure that media can perform their crucial watchdog function in a democratic society.[25] A number of reports and guidance documents published by the OSCE RFoM, including the Special report on legal harassment and abuse of the judicial system against the media (2021),[26] Safety of Journalists Guidebook (3rd ed., 2020),[27] Resource Guide on the Safety of Female Journalists Online (2020),[28] Guidelines for monitoring online violence against female journalists (2023),[29] Policy Manuals "Spotlight on Artificial Intelligence and Freedom of Expression" (2022)[30] and "Safeguarding Media Freedom in the Age of Big Tech Platforms and AI" (2025)[31] are also of relevance for the present Joint Opinion.

18. Content available on the Internet is, in principle, subject to the same human rights regime as traditional media, such as printed materials and speech. Resolution 20/8 of the United Nations Human Rights Council (UN HRC) affirms 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*".[32] As such, all forms of audio-visual as well as electronic and internet-based modes of expression are protected.[33]

19. In the context of the freedom of expression and access to information on the Internet, the importance of the role of online intermediaries should be underlined. By offering alternative and complementary means or channels for the dissemination of media content, they ensure broad outreach and speedy access to information. At the same time, there is also a risk of censorship operated by authorities through intermediaries, as well as private censorship (in respect of media to which intermediaries provide services or of content they carry). In this respect, legislation governing intermediaries that introduce restrictions to freedom of expression and access to information, including by holding them legally liable for failing to prevent access to content deemed to be illegal, should comply with the strict requirements set out in of Article 19 (3) of the ICCPR to ensure consistency with international standards.[34] As mentioned in the CoE Recommendation on Internet Intermediaries, *"[w]here intermediaries produce or manage content available on their platforms or where intermediaries play a curatorial or editorial role, including through the use of algorithms, State authorities should apply an approach that is graduated and differentiated. States should determine appropriate levels of protection, as well as duties and responsibilities according to the role that intermediaries play in content production and dissemination processes, while paying due attention to their obligation to protect and promote pluralism and diversity in the online distribution of content.*"[35]

---

24 See Joint Declarations, UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur and the African Commission Special Rapporteur on Freedom of Expression and Access to Information (hereinafter "International Mandate-Holders on Freedom of Expression").

25 See Joint Declaration on Media Freedom and Democracy, International Mandate-Holders on Freedom of Expression, 2 May 2023.

26 See Special Report on Legal Harassment and Abuse of the Judicial System Against the Media, OSCE-RFoM, 23 November 2021.

27 See Safety of Journalists Guidebook, OSCE/RFoM, 3rd edition, 10 November 2020.

28 See Safety of Female Journalists Online Resource Guide, OSCE/RFoM, 30 October 2020.

29 See Guidelines for monitoring online violence against female journalists, OSCE/RFoM, 3 October 2023.

30 See OSCE/RFoM, *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual*, 2022.

31 See OSCE/RFoM, *Safeguarding Media Freedom in the Age of Big Tech Platforms and AI*, Policy Manual, 2025.

32 See UN Human Rights Council, *2012 Resolution 20/8 on the Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/RES/20/8, 16 July 2012, para. 1.

33 UN Human Rights Committee (CCPR), *General Comment no. 34 on Article 19: Freedoms of opinion and expression*, 12 September 2011, para. 12.

34 See e.g., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of 9 October 2019*, para. 30.

35 See *CoE Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, adopted on 7 march 2018, para. 1.3.9.

2. GENERAL COMMENTS

20. While the stated objective of establishing a legal framework to protect the rights of users of digital spaces is welcome in principle, as further elaborated below, several provisions, especially those related to "unlawful content" and content removal, are broad and vague and have the potential to unduly restrict the right to freedom of expression and access to information, especially in the absence of adequate safeguards and access to effective remedies (see Sub-Section 8 *infra*). Without these safeguards, the Draft Law risks resulting in arbitrary enforcement and unduly limiting freedom of expression and access to information in practice.

1.1. Roles and Responsibilities of Private Actors

21. The effective enjoyment of the right to freedom of expression and access to information in the digital environment depends on both state and non-state actors. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has repeatedly stressed, private companies, particularly major online platforms – play an essential role in shaping the digital public sphere and must respect human rights in their operations.[36] The UN Guiding Principles on Business and Human Rights (UNGPs) affirm that business enterprises have a responsibility to "*[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts*".[37]Chapter I of the Draft Law could be supplemented **to better underline the corporate responsibility to respect human rights, including but not limited to freedom of expression, access to information, privacy and personal data protection, and non-discrimination.** For this purpose, it is important that online platforms and websites include in their terms of service relevant principles of human rights law, especially with respect to content-related actions, so that they will be guided by the same requirements of legality, legitimacy, necessity and proportionality, and non-discrimination that bind state regulation (see para. 12 *supra*).[38]

22. The Draft Law could also require **the online platforms and websites to carry out human rights due diligence to identify, prevent, and mitigate any adverse human rights impacts of their technologies and operations/actions**. The authorized body could assist in developing a methodology for such human rights' due diligence exercise (see also Sub-Section 5 *infra*).

23. **Key principles embedded in the UNGPs, such as inclusive stakeholder engagement, transparency, risk assessment, and access to remedy, should also be reflected at the outset, under Chapter 1**.[39]

24. It must be acknowledged that where regulatory or judicial orders contradict international human rights standards, online platforms or websites may face pressure to prioritize compliance with domestic law and such orders to avoid sanctions,[40] rather than applying international standards of necessity and proportionality for the sake of respecting users' rights. As emphasized by the UN Special Rapporteur on the promotion and protection of

36 See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report on Freedom of Expression and the Private Sector in the Digital Age*, A/HRC/32/38, 2016.
37 UN Human Rights Council, *Guiding Principles on Business and Human Rights* (A/HRC/17/31, 2011), Principle 13.
38 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Content Regulation in the Digital Age* (A/HRC/38/35, 2018), para. 45.
39 See e.g., OHCHR B-Tech & CDT Europe, *Fostering Responsible Business Conduct in the Tech Sector – the Need for Aligning Risk Assessment, Transparency and Stakeholder Engagement Provisions under the EU Digital Services Act with the UNGPs* (2023).
40 See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report to the UN Human Rights Council*, A/HRC/17/27, 16 May 2011, para. 42.

the right to freedom of opinion and expression, censorship measures should never be delegated to private entities, and intermediaries should not be held liable for refusing to take action that infringes individuals' human rights.[41] Moreover, any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences[42] (see also Sub-Section 2.2).

25. Therefore, it is important that the provisions of the Draft Law, especially those concerning content removal, comply with the strict tripartite test governing restrictions to freedom of expression (see further Sub-Section 8 on Unlawful Content) and are framed with adequate effective safeguards to prevent their misuse under the pretext of legal compliance, including to restrict political criticism or silence dissent.

1.2. Institutional Framework for the Implementation of the Draft Law

26. The primary duty to protect human rights, including the rights of users of online platforms and websites, rests with the state. The UNGPs clarify that *"[i]n meeting their duty to protect, States should […] enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically assess the adequacy of such laws and address any gaps*".[43] This means that the Draft Law must not only impose obligations on online platforms and websites but also ensure that the state's duties to protect and respect users' rights are also reflected and that enforcement mechanisms do not create avenues for arbitrary or politically motivated restrictions. In this respect, the new monitoring and enforcement powers of the designated authority/authorised body under the Draft Law (i.e., the Agency as per Article 6 of the Draft Law) should be carefully analysed to ensure that the scope of these powers is narrowly circumscribed, in accordance with Uzbekistan's commitments under international human rights law and OSCE standards on media freedom (see also Sub-Section 5).

27. Although the institutional design of the Agency is not part of the Draft Law and goes beyond the scope of this Opinion, its independence from both other public bodies and private actors remains paramount, particularly given the new powers it has been granted in relation to the digital services industry. Indeed, as underlined by the UN Special Rapporteur, "*any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory*".[44] From a comparative perspective, the CoE Recommendation on the independence and functions of regulatory authorities for the broadcasting sector[45] emphasises that regulatory bodies must have the authority to adopt regulations and guidelines, while operating within procedures that *"clearly affirm and protect their independence"*. Although this Recommendation did not originally address digital platforms, the underlying rationale applies equally to modern converged regulators, since online platforms increasingly perform functions comparable to traditional media – disseminating news, shaping public debate, and moderating content. Without institutional, functional, and financial independence, regulatory actions risk being influenced by political or commercial

41 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011 Report, A/HRC/17/27, para. 75.
42 *Ibid.* 2011 Report, A/HRC/17/27, para. 70.
43 *Ibid*., Principle 3.
44 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011 Report, A/HRC/17/27, para. 69.
45 See CoE Recommendation CM/Rec(2000)23, "Recommendation of the Committee of Ministers to member States on the independence and functions of regulatory authorities for the broadcasting sector", Council of Europe, Committee of Ministers, adopted on 20 December 2000.

pressures, undermining protection of users' fundamental rights, including freedom of expression and access to information.

28. To ensure independence in practice, **several safeguards are recommended and should be reflected in the applicable legislation governing the establishment and functioning of the authorised body.** These include: **transparent and merit-based appointment and removal procedures for its leadership, with adequate safeguards against external interferences, especially from political actors; clearly defined mandates and statutory powers to prevent discretionary, arbitrary or discriminatory implementation; budgetary autonomy to avoid dependence on political authorities; internal procedural safeguards that guarantee independent decision-making, ensuring that decisions are reasoned, properly documented, and subject to appeal; and judicial or external independent review mechanisms to assess the legality and proportionality of regulatory actions**. Implementing such measures would enable the authorised body to exercise its expanded powers in full independence, effectively, impartially, and in accordance with the rule of law, while fostering public confidence in digital governance. It is recommended that **Article 6 of the Draft Law explicitly incorporates the principle of independence of the authorised body while ensuring that the legal framework governing the establishment and functioning of such a body incorporates the safeguards outlined above to ensure its independence**, or that a new body that demonstrably fulfils the criteria of independence be identified to carry out the relevant functions.

RECOMMENDATION A.

To explicitly incorporate in Article 6 of the Draft Law the principle of independence of the authorised body responsible for protecting users' rights on online platforms and websites, while ensuring that the legal framework governing the establishment and functioning of such a body incorporates safeguards to guarantee its independence, including transparent, merit-based appointment and removal of leadership, with adequate safeguards against external interferences, especially from political actors; clearly defined mandates and statutory powers to prevent discretionary, arbitrary or discriminatory implementation; budgetary autonomy; internal procedures guaranteeing independent decision-making; and judicial or external independent review of regulatory actions for legality, legitimacy, necessity and proportionality.

3. AIM AND SCOPE OF THE DRAFT LAW

29. Article 1 of the Draft Law sets out its aim and scope, stipulating that it seeks to protect the rights of users of websites and online platforms "operating within the territory of the Republic of Uzbekistan".

30. The reference to online service providers "operating within the territory" of a state is vague and legally indeterminate. Without further clarification, this wording may create uncertainty both for regulators and for service providers. On the one hand, it may be interpreted too narrowly, covering only those service providers that are physically or legally established in Uzbekistan (e.g., those with a registered office, servers, or subsidiaries in the country). On the other hand, it may be interpreted too broadly, extending to any website or platform accessible to users in Uzbekistan, regardless of whether the provider has a meaningful presence or commercial nexus in the country.

31. International practice shows that jurisdiction over online service providers is generally grounded either in the place of establishment of the provider (or "country of origin" principle[46]) or in a substantial connection to the regulating state, such as targeted commercial activity or a significant user base in that jurisdiction.[47] Jurisdiction may also be determined based on the place where the acts entailing liability produce their harmful effects or the country of the nationality of the victims.[48]

32. Accordingly, to ensure legal certainty and to reflect international practices, the Draft Law would benefit from clearly defining the criteria to determine when an online service provider is considered to be "operating within the territory of Uzbekistan". Such criteria could include the provider's place of incorporation, the location of its infrastructure, targeted commercial activity, or the scale of its user base in Uzbekistan. Without such clarification, the Draft Law risks either undermining the protection of users' rights or imposing disproportionate obligations on foreign online platforms. Overly broad jurisdictional claims risk creating conflicts of law, legal uncertainty, and barriers to the exercise of the right to receive and impart information and ideas regardless of frontiers, while overly narrow interpretations may leave users without effective remedies.

33. **It is thus recommended to amend the Draft Law to include clearer and more objective criteria to determine when an online service provider is considered to be "operating within the territory of Uzbekistan".**

34. Article 4 of the Draft Law defines the fundamental principles for the protection of users' rights on online platforms and websites, including "*1. Legality; 2. Priority of users' rights; 3. Ensuring the right of users to seek, receive and disseminate any information in accordance with the law; 4. Prohibition of censorship with respect to content; 5. Creation of conditions to ensure access to the global Internet; Comprehensive cooperation with owners of online platforms and website owners*".

35. Among the principles that are listed, this provision states that users' rights should be given "priority". While the intention of this formulation appears to be commendable, although it could be made more explicit that users' rights should be prioritized over business or commercial considerations, the practical implementation of the principle of "priority of users' rights" remains unclear. The digital communication sphere is complex and dynamic, and different users' rights often come into conflict with one another. For instance, one user's right to freedom of expression and to disseminate information may directly clash with another user's right to privacy or protection of reputation. Similarly, the right to access and receive information may at times conflict with the right to restrict the processing of personal data.

---

46 This principle is applied, for instance, in the EU E-Commerce Directive; see *Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce (E-Commerce Directive)*, Article 3 (country-of-origin principle). See also *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Article 2.

47 See e.g., Council of Europe, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, para. 10 (stating that jurisdiction should be based on a "substantial connection" such as establishment, targeted activity, or user base). See also *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, Recital 16 and Article 2; *Regulation (EU) 2022/2065*, Article 3(e) using "substantial connection" criterion (whether the service provider specifically targets users in a country, for instance by using a particular language, or has a significant user base there, measured against the size of the population). See also, as an example, UK Online Safety Act 2023, Sec 4(5) and Sec 4(6)(b) also using "substantial connection" criterion such as creating "material risk of significant harm to individuals".

48 See e.g., Articles 4 (2) (b) of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography"*, to which the Republic of Uzbekistan acceded on 23 December 2008, requires States Parties to "*take such measures as may be necessary to establish its jurisdiction over the offences referred to in Article 3, paragraph 1, […] [w]hen the victim is a national of that State*". See also, *UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*, 29 November 1985, para. 5, which underlines that "*Judicial and administrative mechanisms should be established and strengthened where necessary to enable victims to obtain redress through formal or informal procedures that are expeditious, fair, inexpensive and accessible*". See also, as a comparison, with respect to acts entailing tortious, delictual or quasi-delictual liability, CJEU, *Dumez France SA and Tracoba SARL v. Hessische Landesbank and others*, C-220/88, 11 January 1990, para. 20.

36. In international human rights law, there is no predefined hierarchy among these rights. The ICCPR, as interpreted by the Human Rights Committee, recognizes that freedom of expression, right to privacy, reputation, and data protection rights must be considered as equal, co-existing rights that may come into tension with one another. In such cases, states and other decision-makers are required to conduct a balancing exercise based on the principles of necessity, proportionality, and legitimacy of aims. The UN Human Rights Committee in its General Comment No. 34 on Article 19 of the ICCPR has stressed that restrictions on freedom of expression must be narrowly tailored to protect competing rights and cannot be based on abstract or overly broad justifications. Likewise, the ECtHR has consistently applied a case-by-case proportionality analysis when balancing freedom of expression against rights to privacy and reputation under Article 8 of the ECHR.

37. Accordingly, a general legal requirement to "prioritize users' rights" risks being void of substantive meaning, as it does not indicate which rights take precedence in situations of conflict, nor does it set out the method by which competing rights are to be balanced or reconciled. It may also lead to inconsistent or arbitrary interpretations, particularly if left to private companies without clear guidance from the law or from independent regulatory/judicial oversight.

38. Instead, the Draft Law could benefit from refining this principle, for example, by clarifying that no blanket hierarchy exists among human rights (e.g., the rights to impart, seek, and receive information, the right to equality and non-discrimination, the so-called "personality rights" such as privacy and reputation, and data protection rights[49]). Any conflicts should be resolved through a balancing test conducted by competent independent authorities and/or challengeable before a judicial authority, on a case-by-case basis, in line with international human rights standards (see also Sub-Section 2.1 above).

39. Article 4 refers to the "*Creation of conditions to ensure access to the global Internet"*, which could be further clarified to reflect a broad and comprehensive understanding of access. This should include not only the accessibility of online platforms and websites to persons with disabilities, including visual, hearing, physical, cognitive impairments[50] – but also broader measures to ensure meaningful access to all. These should encompass affordability, non-discriminatory availability across different regions and population groups, and the promotion of digital literacy and education to enable effective and informed use of and access to the Internet.[51] As emphasized by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, **accessibility, affordability and non-discrimination** are also fundamental principles for the governance of online platforms and the Internet, as universal access to the Internet is an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress.[52] In particular, it is essential that the Draft Law when adopted should be interpreted, applied and enforced without discrimination, also taking into account multiple and intersectional forms of

---

E.g., including but not limited to the rights to be informed and to consent to the data processing, to access, to rectification, "to be forgotten", to restriction on processing, to data portability, not to be subject to a decision based solely on automated processing, including profiling; see e.g., *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

50 i.e., ensuring their compliance with international web accessibility standards such as the *W3C Web Content Accessibility Guidelines* (WCAG), see <https://www.w3.org/WAI/>.

51 See UN General Assembly, *Resolution 78/213 Promotion and protection of human rights in the context of digital technologies*, 22 December 2023, para. 8.

52 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *2011 Report*, A/HRC/17/27; see also *Joint Declaration on Media Freedom and Democracy*, International Mandate-Holders on Freedom of Expression UN/OAS/OSCE/ACHPR, 2 May 2023.

discrimination and that special measures may be needed to address specific needs or correct existing inequalities.[53] **Article 4 should be supplemented in this respect.**

40. Finally, it is important to recall that states have **a positive obligation to promote a free, independent and diverse communications environment, including media diversity and online pluralism more generally**, which is an important instrument of addressing disinformation and promoting democracy.[54] **Article 4 of the Draft Law could also explicitly emphasize such a positive obligation.**

4. DEFINITIONS

41. Article 3 of the Draft Law provides for definitions of key terms used in the Draft Law.

4.1. Bloggers and Influencers

42. The Draft Law defines a "blogger" as a user of an online platform who publishes content of any kind on their account or public page, "*including for the purpose of discussion by other users of the platform*". It then defines an "influencer" as a blogger "with more than ten thousand subscribers".

43. These definitions may raise some concerns. First, the creation of statutory definitions of "blogger" or "influencer" is not very wide-spread internationally, although an increasing number of countries tend to regulate "bloggers" and "influencers" or at least address such phenomena in soft law and policy documents, and define such terms therein.[55] In most jurisdictions, online content creators are regulated under general legal frameworks concerning freedom of expression, media, advertising or intermediary liability, rather than being assigned a specific statutory label. Second, the proposed definition of "blogger" in the Draft Law is overly vague and excessively broad. It risks encompassing virtually any social media user who shares text, images, or videos with their contacts, regardless of the intent, frequency, or scope of dissemination. Such an expansive definition would blur the distinction between private communications and activities of genuine public relevance.

44. By contrast, in ordinary usage, a "blogger" generally refers to an individual who operates or contributes to a blog – i.e., a regularly updated digital space containing articles, opinions, or commentary, often structured around particular themes or experiences, and intended for a general audience. This understanding implies two elements absent from the Draft Law's definition: (i) a degree of regularity or periodicity in publishing, and (ii) an intention to make content accessible to the general public, rather than restricting it to a closed circle of contacts.

45. From a legal-drafting perspective, defining "blogger" as a separate statutory category appears unnecessary and may create practical difficulties in enforcement. Many states refrain from doing so, relying instead on general provisions regulating online content and applying the same baseline human rights protections regardless of whether the author is a professional journalist, a civil society actor, or a regular private individual. It is worth recalling that a variety of entities or individuals, who are not professional media actors, deserve certain aspects of the enhanced protection as long as they carry out "journalistic function" by producing and publishing information in public interest – whether through print, online or other media – including non-governmental organizations, human rights

See e.g., CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018, para. 1.1.5.

54 See International Mandate-Holders on Freedom of Expression UN/OAS/OSCE/ACHPR, *Joint Declaration on Media Freedom and Democracy*, 2 May 2023.

55 See e.g., CoE, European Audiovisual Observatory, *Study on National Rules Applicable to Influencers* (2025), p. 25.

defenders but also bloggers and popular social media users, who may at times function as "public watchdogs".[56] This functional protection is not limited to professional or accredited journalists but applies broadly to the actors who produce and publish information in the public interest.[57] Should the Uzbek legislator nevertheless wish to retain a definition of "blogger", it would be advisable to more narrowly define such a term to more clearly distinguish it from private communications by referring to factors such as editorial control, periodic updating, outreach to a potentially large audience, and intent to engage in public communication.[58] Incorporating these elements would help distinguish between personal, small-scale user activity and genuine "blogging" as a form of online media, thereby ensuring legal certainty and avoiding unnecessary regulation of ordinary online users.

46. Similarly, the Draft Law's definition of "influencer" while not wide-spread in comparative law, may be found in soft law and policy documents of several countries. It is not unusual that European countries define "influencers" by referring to the numbers of their audiences, although depending on the country context or topical issues being addressed, such a numerical threshold may not necessarily adequately reflect the actual public "influence".[59]

47. The underlying policy objective – presumably, to create a legal framework for individuals who, while not being professional media actors, nevertheless have a significant impact on public opinion – is understandable. However, regulation should follow a "graduated and differentiated" approach, based on the principles of strict necessity and minimum intervention needed to achieve the legitimate interest of such regulation, which calibrates obligations and responsibilities according to factors such as size of audience, scope of dissemination, nature of content, and operational capacity.[60] This model avoids imposing uniform obligations on vastly different actors and ensures proportionality.

48. This would mean that bloggers or influencers with limited resources and outreach should not be subject to the same regulatory requirements as professional media outlets or large-scale platforms. Conversely, individuals or entities that consistently reach large audiences and exert measurable influence could be subject to enhanced transparency and accountability standards, particularly regarding advertising, sponsored content, or the dissemination of information with potential public impact. Such a framework would strike a better balance between protecting users' rights, ensuring accountability in the digital space, and avoiding undue restrictions on smaller individual content creators.

49. **It is thus recommended to revise the definitions of "blogger" and "influencer" in light of above considerations**.

56 See e.g., OSCE/ODIHR-OSCE RFoM, Interim Joint Opinion on the Draft Law of the Kyrgyz Republic on the Mass Media (as of 13 May 2023), para. 26; see also the *Inter-American Declaration of Principles on Freedom of Expression*, approved by the Inter-American Commission on Human Rights during its 108th regular session, 19 October 2000; and the European Court of Human Rights, *Magyar Helsinki Bizottság v. Hungary*, App. no. 18030/11, 8 November 2016, para. 166. See also e.g., ODIHR, *Urgent Comments on the Draft Criminal Offences against Honour and Reputation in the Republika Srpska* (11 May 2023), para. 55.

57 See the UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, para. 44. Similarly, at the CoE level, the term "journalist" is understood as any natural or legal person who is regularly or professionally engaged in collecting and disseminating information to the public via any means of mass communication (see e.g., the *Council of Europe, Recommendation No. R (2000) 7*, 8 March 2000, under "definitions").

58 As a comparison, see e.g., the definition of blogger used in Council of Europe, *Recommendation CM/Rec(2011)7 of the Committee of Ministers of the CoE to member states on a new notion of media* (adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies).

59 See CoE, European Audiovisual Observatory, *Study on National Rules Applicable to Influencers* (2025), pp. 25-39.

60 *Ibid*, para. 7. See also Joint Declaration on Media Freedom and Democracy, International Mandate-Holders on Freedom of Expression, Joint Declaration on Media Freedom and Democracy, 2 May 2023, page 6, para. (b).

4.2. False Information

50. The Draft Law defines "*false information"* as *"information that does not correspond to reality or that contains distorted facts, creating a misleading impression about individuals, objects, events, phenomena, or processes*". This single definition does not allow distinguishing concepts such as "disinformation" i.e., verifiably false, inaccurate or misleading information deliberately created and disseminated *to cause harm* or pursue economic or political gain by deceiving the public, or "misinformation", i.e., *"false information that is shared without intent to cause harm*". If the purpose of the Draft Law is to address harmful dissemination of false information, it would be advisable to supplement the Draft Law with definitions of "disinformation", to be distinguished from "misinformation".

51. At the outset, it is important to underline that not all false or inaccurate information is harmful, and only some harms – such as those that implicate public health, electoral processes, environment or national security – may warrant state intervention to prevent the dissemination of such (harmful) information or disinformation.[61] In any case, it is worth noting that there is no internationally recognized definition of "false information" and including in the legislation general vague bans on false statements, without requiring a harmful impact, should be strongly discouraged.

52. If the purpose of the Draft Law is to prevent "disinformation", it would be advisable to include a definition reflecting critical elements stated in international and regional recommendations and good practices i.e.: (i) that the information should be verifiably false (i.e., objectively proven as untrue through evidence rather than contested interpretation), (ii) that it should be capable of causing harm if disseminated; and (iii) that it should be intended to deceive the public.[62] Also, while domestic laws addressing the propagation of falsehoods are permissible in relation to matters such as fraud, perjury, false advertising and defamation, the general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events could be problematic, as specified by the UN Human Rights Committee in General Comment No. 34.[63] The definition also fails to address the element of intent, which is crucial in distinguishing between mere inaccuracies, mistakes, or subjective opinions, and deliberate attempts to deceive the public. Without the above-mentioned qualifiers of verifiably false information with the intent to deceive the public, the Draft Law risks covering a wide spectrum of content that may be inaccurate, incomplete, misleading, or still under debate, but which does not necessarily reach the threshold of "disinformation" intended to cause harm, and therefore requiring regulatory intervention.

53. Second, the current definition risks encompassing speech that is an integral part of democratic discourse and shall be protected by the right to freedom of expression and opinion. In this respect, it is essential that the definition clearly distinguishes and excludes value judgments, which are not susceptible of proof, from factual statements the existence of which can be demonstrated.[64] A requirement to prove the truth of a value

61 See Report on countering disinformation for the promotion and protection of human rights and fundamental freedoms, United Nations, Secretary General, A/77/287, 12 August 2022, para. 42. See also, as a comparison, Action Plan against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018.

62 See, as a comparison, Council of Europe, *Recommendation of the Committee of Ministers of the CoE to member States on electoral communication and media coverage of election campaigns* (adopted by the Committee of Ministers on 6 April 2022 at the 1431st meeting of the Ministers' Deputies), para. 7; *Recommendation CM/Rec(2022)11 of the Committee of Ministers of the CoE to member States on principles for media and communication governance*, adopted by the Committee of Ministers on 6 April 2022; *CoE Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner* (2024), see preamble, para. 3. See also *2022 Code of Practice on Disinformation*.

63 UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, para. 49.

64 This distinction is for instance well established in the caselaw of the ECtHR, see e.g., ECtHR, *Lingens v. Austria*, no. 9815/82, 8 July 1986), para. 46; and *McVicar v. the United Kingdom*, no. 46311/99, 7 May 2002, para. 83.

judgment is thus impossible to fulfil and infringes freedom of opinion itself.[65] In this respect, for instance, the ECtHR has emphasized that, where the national legislation or courts make no distinction between value judgments and statements of fact, which amounts to requiring proof of the truth of a value judgment, this is an indiscriminate approach to the assessment of speech and is *per se* incompatible with freedom of opinion.[66] Moreover, in many contexts – such as evolving scientific research, political commentary, or reporting on rapidly evolving events – the "truth" of certain information may be uncertain, subject to interpretation, or later revised as new facts emerge. For example, early reporting during a public health crisis or political upheaval may include provisional or contested information, which would fall under the Draft Law's broad definition even if there was no intention to mislead. Criminalizing or otherwise restricting such speech could produce a chilling effect on freedom of expression, discouraging individuals, journalists, and civil society actors from sharing information of public interest for fear of liability.

54. It is also worth recalling that the right to freedom of expression is very broad and protects all forms of ideas, information or opinions, including those that "offend, shock or disturb" the state or any part of the population, including deeply offensive expression.[67] As such, satire and parody should also be explicitly excluded from the respective limitations of speech.[68]

55. In light of the foregoing, **it is recommended that the Draft Law provides clearer definitions distinguishing between "false information", "misinformation" and/or "disinformation"** (i.e., inaccurate or misleading information deliberately created and disseminated *to cause harm* or pursue economic or political gain by deceiving the public) – reflecting the elements provided in international and regional recommendations and good practices i.e.**: (i) the information must be verifiably false, meaning that its inaccuracy can be objectively demonstrated; (ii) the dissemination must be deliberate or reckless, with the intent (or reasonably foreseeable consequence) of causing harm; and (iii) the harm in question should be directed at and/or adversely impacting human rights or concrete and legitimate interests, such as the protection of public health, electoral processes, environment or national security**. **The definition should also explicitly exclude from its scope value judgments as well as satire and parody.**

56. This would narrow the scope of regulation to genuinely harmful disinformation while safeguarding freedom of expression and debate in areas where truth and falsity are contested or evolving (see also Sub-Section 8 on "Unlawful Content").

4.3. Moderator of a Public Page

57. The Draft Law defines a "moderator of a public page" as either the owner or a user of an online platform who has the authority to post, delete, or edit content on that page. As currently drafted, this definition is overly broad and risks encompassing virtually any

65 See e.g., ECtHR, *Morice v. France* [GC], no. 29369/10, 23 April 2015, para. 126; and ECtHR, *Lingens v. Austria*, no. 9815/82, 8 July 1986), para. 46.

66 See e.g., ECtHR, *Gorelishvili v. Georgia*, no. 12979/04, 5 June 2007, para. 38; and *Fedchenko v. Russia*, no. 33333/04, 11 February 2010, para. 37.

67 See Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, International Mandate-Holders on Freedom of Expression, 3 March 2017, paragraph of the Preamble. See also UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, para. 11; and 2015 Thematic Report, UN Special Rapporteur on counter-terrorism A/HRC/31/65, 22 February 2016, para. 38. See also, as an example of good regional practice, European Court of Human Rights, *Handyside v. United Kingdom*, no. 5493/72, 7 December 1976), para. 49; and *Bodrožić v. Serbia*, no. 32550/05, 23 June 2009, paras. 46 and 56.

68 As a comparison, see for instance, Action Plan against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018, which explicitly exclude inadvertent errors, satire and parody, or clearly identified partisan news and commentary from the definition of "disinformation".

platform user, since most users have at least some abilities to edit or delete their own content. If interpreted literally, the provision would dilute the meaning of "moderator" to the point of redundancy, capturing ordinary users rather than identifying a distinct role within the governance of online spaces.

58. It appears more plausible that the drafters intended to describe a figure who is empowered to oversee and regulate the contributions of other users on a public page, whether by posting content on behalf of the page, editing content submitted by third parties, or removing material that violates internal community guidelines or applicable law. This function, in many jurisdictions and in common technical usage, is closer to the role of a "webmaster" or page administrator, rather than an ordinary user. By conflating these different functions, the Draft Law risks creating legal uncertainty and placing undue obligations on all individual users of online spaces.

59. **It is thus recommended that the current definition is revised ensuring greater clarity and precision,** to ensure that it does not inadvertently extend legal liability to ordinary users, which would risk discouraging participation in online spaces and undermining the Draft Law's stated aim of protecting users' rights.

4.4. Online Platform

60. The Draft Law defines an "online platform" as an "*information system composed of informational resources and operating on the global Internet*", and/or an "*instant messaging system*" that enables the receiving, generating, processing, posting, disseminating, or storing of content on a personal profile or public page. The definition specifies that is excludes information systems operating on the global Internet that are solely intended for the provision of financial services, e-commerce services, internal corporate communications, e-mailing, online television, and online content storage.

61. From a comparative perspective, although differing in details, examples of regional or country regulatory frameworks tend to converge on two common elements of "online platforms": (1) the core function of enabling users to connect, interact, and disseminate information; and (2) a practice of enumerating examples of relevant services (e.g., social networks, search engines, video-sharing services) to clarify the scope.[69]

62. Against this background, it is important that the Draft Law's inclusion of instant messaging services within the definition of "online platform" does not result in regulating private, interpersonal communication among a limited group of users, rather than public dissemination of information to a wider audience.[70] This distinction is crucial, not least because certain regulatory obligations that may be appropriate for public platforms could be ill-suited for private communications. Even the Draft Law itself introduces "instant

69 For example, the *CoE Recommendation on principles for media and communication governance* defines platforms as "*providers of digital services that connect participants in multisided markets, set the rules for such interactions, and make use of algorithmic systems to collect and analyse data and personalise their services"*, expressly including search engines, news aggregators, video-sharing services and social networks; *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act/EU DSA)* adopts a functional definition, describing platforms as "*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service …*" therefore capturing the essential features of services that enable wide user-to-user dissemination of information while excluding marginal functionalities; the United Kingdom's Online Safety Act defines "user-to-user services" as internet services through which "content generated directly on the service by a user, or uploaded or shared by a user, may be encountered by another user"; this is paired with a separate category for search engines, ensuring comprehensive but differentiated coverage.

70 See e.g., the *European Electronic Communications Code* defines an "interpersonal communications service" as "*a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s)*"; this definition explicitly distinguishes interpersonal communications from services where dissemination to the public is the core function; see also for instance, the *Australia's Online Safety Act* similarly enumerates "instant messaging services" and "chat services" as examples within the broader category of "electronic services", ensuring that the scope is clear while avoiding conflation with broader platform regulation.

messaging services" as a separate category later in the text, suggesting that they should be regulated differently from "online platforms".

63. Accordingly, the "**instant messaging service" should be maintained as a distinct category given the importance of keeping interpersonal communications distinct from (online) public platforms, both in terms of regulatory definitions and the obligations that may follow**. This will also help avoid legal ambiguity, prevent potential over-regulation of private communications, and bring the Draft Law into closer alignment with international recommendations and good practices. The definition of "online platform" could be aligned more closely with comparative models by: incorporating the concept of public dissemination as a core feature; enumerating examples of covered services (e.g., social networks, video-sharing sites, news aggregators, online forums); and clarifying exclusions in a way that avoids overlap with separately regulated categories such as interpersonal communications or audiovisual media.

4.5. Websites and Website Owners

64. The Draft Law defines a "website" as *"an information resource on the global Internet that does not possess the characteristics of an online platform and is accessed via a unique identifier … consisting of a domain name and characters assigned by the website owner."* Attempting to provide a legal definition of the category of "website" is, however, highly unusual from a comparative perspective. In practice, most international and regional legal frameworks deliberately refrain from codifying this notion, likely because it is already well understood in both technical and colloquial usage. For example, at the EU level, the term "website" is used repeatedly in the e-Commerce Directive and the Digital Services Act (EU DSA) without being formally defined, relying instead on the common understanding of the term.[71]

65. The Draft Law's definition of "website" should also be examined in relation to the very broad definition of "online platform". Article 3 prescribes that a website is merely an "information resource" that does not meet the characteristics of an "online platform" and is accessed via a unique network identifier. It thus seeks to define "website" only as a residual category – that is, as whatever that does not qualify as an "online platform". This approach risks creating confusion, as it effectively reduces the notion of "website" to a negative definition ("everything that is not an online platform"), rather than offering a clear, affirmative description of its characteristics.

66. The practical implication of this definitional structure is that the Draft Law's overly expansive definition of "online platform" severely limits what can still qualify as a "website". Since the definition of "online platform" includes virtually any service that allows users to post, generate, or disseminate content, websites would be confined to static internet pages that do not permit interaction, user comments, or any form of content sharing. This risks rendering the definition of "website" both obsolete and legally meaningless, as most modern websites – ranging from news portals to professional pages – incorporate some interactive features, however minimal.

67. A more suitable approach would be to define **"website" independently, in neutral technical terms, without reference to the "online platform" category**. This would ensure legal clarity, proportionality, and regulatory coherence. Another option would be

71 One notable outlier is the United States, where federal law defines a website as "*any collection of material placed in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol*." This definition, although more technically precise, demonstrates the risk of excessive formalisation, as technology evolves rapidly and protocol-based formulations can quickly become outdated.

to simply avoid defining "website" as a term which is commonly well-understood. Rather than providing a definition of "website", consideration could be given to define a broader category of "electronic service".[72] Using such a terminology would help avoid unnecessary complexity, and potential overlap, that may otherwise undermine legal certainty.

68. The Draft Law defines a "website owner" as a natural or legal person who *"independently determines the procedures for the use of the website, including the rules for posting content"*. This formulation is both uncommon in legal practice and technically imprecise. In practice, the power to determine how a website functions – such as setting user permissions, moderating content, or establishing rules of use – typically lies with the administrator or webmaster. These individuals or entities may manage the day-to-day functioning of a site without necessarily holding the legal title of ownership to the domain or hosting infrastructure.

69. The Draft Law's conflation of ownership with administrative or managerial control risks introducing confusion and may create legal uncertainty about who bears responsibility for compliance, thus, undermining effective enforcement and accountability. **A clearer distinction should be drawn between the website owner (the person or entity holding the domain or server rights) and the website administrator/webmaster (the person or entity responsible for technical and content management).**

RECOMMENDATION B.

1. To more clearly distinguish the concepts of "false information", "misinformation" and "disinformation" while ensuring that the latter only includes the type of false information, which is verifiably false and disseminated deliberately or recklessly with the intent, or reasonably foreseeable consequence, of causing harm to human rights and/or legitimate interests – such as public health, electoral processes, environment or national security, while explicitly excluding from its scope value judgments as well as satire and parody.
2. To clarify the definition of "online platform" by reflecting the core function of enabling users to connect, interact, and disseminate information; and by enumerating examples of relevant services (e.g., social networks, search engines, video-sharing services).

5. Powers of the Authorised Body in the Field of Protection of Users' Rights on Online Platforms and Websites

70. Article 6 of the Draft Law designates the Agency as the authorised state body responsible for protecting users' rights on online platforms and websites and defines its powers.

72 Relevant comparative examples include: the EU's Information Society Services Directive, which defines such services as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."; the *Recommendation CM/Rec(2022)11 of the Committee of Ministers of the CoE to member States on principles for media and communication governance*, adopted by the Committee of Ministers on 6 April 2022, which describes intermediaries as "intermediaries other than the media and platforms that are relevant for communication and dissemination of content, covering signal transmission systems irrespective of the technology used … as well as services provided via such networks (such as interpersonal communications services)."

71. Under the Draft Law, the Agency is vested with a broad and multifaceted mandate, which includes regulatory functions;[73] supervisory and compliance functions;[74] investigatory powers;[75] enforcement and sanctioning powers;[76] advisory and policy functions;[77] and international cooperation responsibilities.[78]

72. Therefore, with the Draft Law, the Agency will be given new powers in respect of digital services such as websites and platforms. The expansion of the Agency's powers reflects a comparative trend toward converged regulatory oversight across multiple communication technologies.[79] At the same time, as already mentioned under Sub-Section 2.2. above, the *independence* of regulatory and other public bodies which exercise powers in print, broadcast, other media and/or telecommunications regulation has been a long-standing standard established at the international and regional levels.[80] It is thus essential that the body exercising the powers envisaged under Article 6 is independent.

73. According to Article 6 (2) (5) of the Draft Law, the authorized body shall monitor online platforms and websites for the purpose of identifying unlawful content and refer detected violations to law enforcement authorities; it shall prepare an opinion regarding any unlawful content identified through its online platforms and websites monitoring activities, which may be conducted either *ex officio* or based on submissions received from individuals and legal entities to the authorized body (Article 14 (1)-(3)). Read together with the existing definition of "online platforms" in Article 3, this suggests that the monitoring activities are not limited to the publicly accessible data on platforms.

74. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has raised concerns regarding legislation increasing state power to collect information on and monitor Internet users' activities and content of communication without providing sufficient guarantees against abuse, thus constituting a violation of the Internet users' right to privacy and to personal data.[81] This is problematic even if such data is collected in online spaces accessible to the public.[82] Such

73 i.e., adopting regulatory legal acts, proposing measures for the implementation of existing legislation, and shaping state policy concerning users' rights.

74 i.e., overseeing adherence to legal obligations, including transparency and reporting requirements for platforms and websites.

75 i.e., requesting information on platform users, determining user statistics independently, and obtaining data in the context of pre-trial investigations or criminal proceedings.

76 i.e., issuing orders and directives to remedy violations of the law.

77 i.e., contributing to the development of state programmes and initiatives in the field of information security.

78 i.e., coordinating with foreign counterparts and aligning with global standards in regulating digital services.

79 For example, the UK's Office of Communications (Ofcom) has gradually extended its remit to include broadcasting, telecommunications, and online safety, reflecting the growing convergence between traditional media and digital platforms.

80 See Joint Declaration on Media Freedom and Democracy, International Mandate-Holders on Freedom of Expression, 2023, which underlines: *"States should ensure that all public bodies which exercise powers in print, broadcast, other media and/or telecommunications regulation, including bodies that receive complaints from the public, are independent, transparent, and effectively functioning in law and in practice. They should be protected from undue interference, particularly of a political or commercial nature. The legal status of these bodies should be clearly defined and their institutional autonomy and independence guaranteed and protected by law."* See also e.g., Joint Legal Analysis of the Draft Law on Mass Media of the Republic of Uzbekistan, OSCE/ODIHR-OSCE/RFoM, November 2020, Chapter 2, where it is underlined that "*any legitimate media regulator should enjoy political, functional, managerial and financial independence from the Government, as well as from political, commercial and other interests"*. Notably, a number of OSCE participating States have entrusted independent bodies with media regulation; see for example within the European Union, Media regulatory authorities and the challenges of cooperation (2021), European Audiovisual Observatory and the EPRA, Chapter 3. See also, as a comparison, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act/EU DSA)*, Recitals 112-113, underlying that "*competent authorities designated under this Regulation should also act in complete independence from private and public bodies*".

81 See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report to the UN Human Rights Council*, A/HRC/17/27, 16 May 2011, paras. 53-55. See also See UN Special Rapporteur on freedom of opinion and expression, Report on the Regulation of User-generated Online Content, A/HRC/38/35, 6 April 2018, para. 67, which states: "*States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the 'proactive' monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to prepublication censorship*".

82 See e.g., ECtHR, *Peck v. the United Kingdom*, no. 44647/98, 28 January 2003, para. 59; and *P.G. and J.H. v. the United Kingdom* no. 44787/98, 25 September 2001, paras. 57-59.

interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim(s) pursued.[83]

75. Article 6 (6) of the Draft Law allows the authorized body to issue orders and directives to eliminate identified violations of the Draft Law (see also Sub-Section 8 *infra*). Restrictions on access to online content could be imposed either by an order of a judicial authority or by an independent administrative authority, whose decisions would be subject to judicial review assessing the legality, necessity and proportionality of the measures. In cases concerning content that is illegal irrespective of context, such as content involving child sexual abuse material or other exceptional cases, expedited measures are required in accordance with the conditions prescribed by international human rights law, subject to effective and rapid *ex post* judicial remedies.[84] As further elaborated in below Sub-Section 8, due to broad and vague wording defining what constitutes "unlawful content", which may lead to the issuance of orders and directives to remove such content, and the risk of potential arbitrary application, it is all the more essential that restrictions are authorized by a judicial body, or by the authorized body, which should be independent from political, commercial and other undue influences, with its decisions being subject to judicial review.

76. The powers of the authorized body listed in Article 6 should also be read together with other provisions of the Draft Law. Article 7 (3) (4) of the Draft Law implies that the authorised body will be able to request not only information about the number of users but more broadly, **information about users of an online platform outside of cases where such requests are based on official requests from pretrial investigation and inquiry bodies or from a court.** Without clear and strictly circumscribed and justifiable legal grounds for such requests as well as proper judicial oversight, such powers may be subject to discretionary or arbitrary interpretation and may unduly impact on the right to privacy and protection of persona data of the users. **This provision should be reconsidered entirely.**

6. FUNCTIONS AND DUTIES OF ONLINE PLATFORMS

77. Article 7 of the Draft Law defines the functions and duties of online platform owners, some of which are further elaborated in Articles 8 to 12 of the Draft Law on interaction with law enforcement authorities, personal data protection, recommendation system and profiling, and content moderation, respectively. Article 7 (3) (1) read together with Article 7 (4) requires online platforms exceeding 100,000 daily users in Uzbekistan to designate a representative to interact with the Agency. All other functions and duties listed under Article 7 (2) and (3) would be otherwise applicable to all online platforms, irrespective of the number of users, including smaller ones. Establishing a threshold generally seeks to target large platforms due to their societal and market impact, which can differ substantially from smaller platforms. However, the Draft Law's threshold of 100,000 users in Uzbekistan corresponds to 0.26% of the population (or 0.3% of the population who are Internet users),[85] a level too low to meaningfully capture platforms with genuine societal impact. By comparison, the EU DSA establishes a threshold for "very large online platforms" at 10% of the Union population (approximately 45 million users), acknowledging that systemic risks rise disproportionately with user scale, and also exempts micro and small enterprises from a number of obligations imposed on online platforms, including in terms of reporting or internal complaint-handling system. It is to

83 See e.g., ECtHR, *Segerstedt-Wiberg v. Sweden*, no. 62332/00, 6 June 2006, para. 88.
84 See e.g., CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018, para. 1.3.2.
85 See <https://zamin.uz/en/society/168048-statistics-of-internet-users-in-uzbekistan.html>.

be noted that small platforms do not generate the same risks and should not be burdened with obligations intended for very large services. **It is therefore recommended to consider raising the threshold while reviewing the obligations imposed on all platforms with a view to avoid overburdening smaller platforms, which typically have more limited financial and operational capacities.**

78. Article 7 contains a number of positive features which *prima facie* mirror some of the protective measures that are increasingly recommended at the international and regional level, such as greater visibility of online advertising, attempts to protect against deceptive or misleading online content, accessibility to persons with disabilities and better information access for the users (e.g., privacy policy and recommendation system).

79. Especially, it is commendable that Article 7 requires to maintain technical accessibility of online platforms for persons with disabilities, taking into account their specific needs (Article 7 (3) (10)). Unless provided in other legislation, it would be advisable in this regard to adopt and implement relevant international guidance on web content accessibility for persons with disabilities[86] to help online platforms to use formats accessible or adapted for persons with disabilities (including individuals with visual impairments or intellectual disabilities).

80. Article 7 (3) (12) of the Draft Law also obliges platforms to protect children from "content harmful to their health". While protecting minors online is a global priority, it is unclear what is meant by "harmful to their health". This vague wording may be unduly limiting since the Draft Law does not specify what is meant by "harmful", which may lead to arbitrary interpretation, whereas failing to distinguish between genuinely harmful material and information, which may fall within the scope of protection of Article 19 of the ICCPR. By contrast, international standards define content harmful for children precisely and outline detailed measures.[87] **Therefore, the Draft Law could enhance the relevant provisions by incorporating precise content categories of genuinely harmful material and information for children and related safety measures directly into the Draft Law or other applicable legislation, or by delegating specifics to be issued as guidelines by the authorised body**.

---

86 See W3C Web Accessibility Initiative (WAI), *W3C Web Content Accessibility Guidelines* (WCAG), see <https://www.w3.org/WAI/>.

87 See e.g., UN General Assembly, *Resolution 78/213 Promotion and protection of human rights in the context of digital technologies*, 22 December 2023, para. 5, the importance of combating all forms of violence in the context of digital technologies, including sexual exploitation and abuse, harassment, stalking, bullying, non-consensual sharing of personal sexually explicit content, threats and acts of sexual and gender-based violence, death threats, arbitrary or unlawful surveillance and tracking, trafficking in persons, extortion, censorship, illegal access to digital accounts, mobile telephones and other electronic devices; in addition, a number of international instruments require the criminalization of the dissemination or communication of certain forms of sexually exploitative content: Articles 2 (c) and 3 (1) (c) of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography",* to which the Republic of Uzbekistan acceded on 23 December 2008, require the criminalization of "*child sexual exploitation material*"; see also, for comparison, Article 20 of the *Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention) requires the criminalization of intentional conduct, amounting to *"(a) producing child pornography; (b) offering or making available child pornography; (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; (e) possessing child pornography; and (f) knowingly obtaining access, through information and communication technologies, to child pornography*" (Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), CETS No. 201, Article 20). See also e.g., the UK Online Safety Act which requires risk assessments, content moderation including takedown procedures, restrictions on harmful content (pornography, suicide encouragement, violence, bullying, dangerous stunts), and limits on addictive or manipulative features (e.g., autoplay, streaks); Sec. 61 also defines 'Priority content that is harmful to children' as a series of content such as abusive content targeting one or more protected characteristics, incites hatred against certain protected characteristics, encourages serious violence against a person, is of a bullying nature, depicts real or realistic serious violence or injury against a person, an animal or a fictional creature, encourages dangerous challenges or stunts, ingesting or inhaling harmful substances. See also the EU *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act/EU DSA)*, which mandates that providers accessible to minors adopt "appropriate and proportionate measures" for privacy, safety, and security, with detailed guidance issued by the Commission in July 2025 on defaults, recommender system adjustments, and parental controls, among others (see Commission publishes guidelines on the protection of minors | Shaping Europe's digital future: the Guidelines set out key recommendations for service providers, including: making children's accounts private by default; adjusting recommender systems to reduce harmful content and give children greater control over their feeds; enabling children to block or mute others and preventing their addition to groups without consent; banning the downloading or screenshotting of minors' content to prevent the unwanted sharing of intimate material; disabling by default features that encourage excessive use, such as streaks, autoplay and push notifications; restricting manipulative commercial practices that promote spending or addictive behaviour; and strengthening moderation, reporting and parental control tools.

81. Some of the other obligations of online platforms' owners listed in the Draft Law may raise some concerns, or would require adjustments to ensure they are implemented in practice, as further elaborated below.

82. Generally, as noted in Sub-Section 2.1 above, it would be important to mention in Article 7, at the outset, **the duty of online platforms to respect human rights, and that their terms of service must reflect relevant principles of human rights law**, especially with respect to content governance, so that they will be guided by the requirements of legality, legitimacy, necessity and proportionality, and non-discrimination.[88] The requirement to establish a user complaints-handling mechanism (Article 7 (2) (2) and (3) and Article 10) may support online platforms with human rights due diligence process by identifying adverse human rights impacts of their activities/operations.

83. It should be noted, however, that the requirement to report daily active users (Articles 6 (7) and 7 (3) (4)), in addition to average monthly users, appears unnecessary. Monthly averages suffice to identify very large platforms and avoid intrusive daily monitoring.

6.1. Co-operation with Law Enforcement Authorities

84. Article 8 of the Draft Law requires platforms maintain emergency cooperation with law enforcement when they detect information about situations posing a threat to human life or safety.

85. First of all, the respective wording appears overly broad which could lead to over-reporting regarding every situation which might potentially give rise to such a risk. **It would be advisable to limit the scope of cooperation to situations where the risks are actual or imminent**.[89]

86. Article 8 further specifies the information to be shared: content description, time and place of posting, username, IP address, and device name. It is positive that the Draft Law provides a limited and specific list of the types of information to be provided to law enforcement authorities. This aligns with the 2022 OSCE RFoM Policy Manual "Spotlight on Artificial Intelligence and Freedom of Expression" recommending that "*law enforcement agencies should have very limited and specifically targeted access to data, narrowed to specific identifiers or specific categories*",[90] and that access should be restricted to "specific records and content".[91] Further guidance from the OSCE in this context includes recommendations that data collection by law enforcement should always be based on "concrete suspicions", and that data collected for different purposes, such as national security, should not be repurposed for use in law enforcement.[92]

87. Article 8 of the Draft Law provides that unlawful content may be identified either through user complaints (see Sub-Section 6.2 *infra*) or through the platforms' own moderation processes. The Draft Law does not impose a proactive content-detection obligation on platforms, which is welcome. However, it is unclear whether platforms lose immunity from liability upon receiving user notices about content deemed unlawful, as occurs

88 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Content Regulation in the Digital Age* (A/HRC/38/35, 2018), para. 45.

89 As a comparison, the EU Digital Services Act requires service providers to "promptly" inform law enforcement authorities when they become "aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place"; see Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act/DSA), Article 18 (1).

90 See OSCE/RFoM, *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual*, 2022, p. 98.

91 *Ibid.*

92 *Ibid.*

under the EU DSA[93] when a platform gains "actual knowledge or awareness". Clarifying this point is essential.

6.2. Complaint-handling Mechanism

88. Article 10 of the Draft Law establishes a procedure for users to submit complaints regarding content posted by other users on online platforms. Platforms are tasked with setting up the rules and procedures for handling such complaints, and mention the requirement that the mechanism should be accessible to the users. The provision is welcome in principle, as responsiveness to user feedback is a key component of platforms' broader obligation to address harmful or unlawful content and ensure users' rights to redress.

89. However, the Draft Law provides limited guidance on how platforms are expected to implement these procedures, which raises a risk that poorly designed mechanisms could frustrate the very purpose of facilitating effective user complaints. For the mechanism to be effective, it should be user-friendly, easily accessible, free of charge, with adequate information for the users about the complaint mechanism and procedure in clear, plain, intelligible and unambiguous language.[94] To ensure the user-friendliness and accessibility in practice, it is generally advisable to carry out meaningful consultation with the users about their needs, expectations, and perspectives, but also possibly consider a variety of submission options.[95] Without clear standards, platforms might adopt processes that are *de facto* inaccessible, cumbersome, or inconsistent, undermining users' ability to seek redress.[96] **In light of the above, the Draft Law could be enhanced by clarifying the procedural requirements for a submission mechanism for user complaints, ensuring that online platforms: provide adequate and easily accessible information for the users about the complaint mechanism; establish clear, transparent, free of charge, user-friendly and easily navigable submission channels; provide timely acknowledgment and processing of complaints; maintain adequate documentation and tracking to ensure accountability; and are based on proportionate requirements that take into account the size and capacity of the platform while maintaining effectiveness for users.** Such amendments would strengthen the Draft Law by making the complaint procedure functional and aligned with international and regional good practices, thereby enhancing both user protection and platform accountability.

6.3. Recommendation System and Profiling

90. Article 11 of the Draft Law addresses recommendation systems used by online platforms. The provision requires platforms to offer users the ability to opt out of personalized content and prohibits profiling based on data relating to "*racial or ethnic origin, political views, biometric or personal data enabling the identification of an individual or*

93 Under the Digital Services Act, for instance, platforms that receive such a notice are deemed to have "actual knowledge or awareness" and consequently lose their immunity.

94 See OHCHR, Access to Remedy in Cases of Business-Related Human Rights Abuse: A Practical Guide for Non-State-Based Grievance Mechanisms (2024). See also, for comparison, the EU Digital Services Act (DSA) specifies that complaint mechanisms must be user-friendly, accessible exclusively via electronic means, and remain available for at least six months. Notices must allow users to provide information that is sufficiently precise and adequately substantiated, including: a description of the alleged illegality; the URL or other details identifying the location of the content; the name and email of the complainant; a statement confirming the bona fide belief of the complainant regarding the illegality of the content (Articles 14, 16 and 20).

95 See OHCHR, Access to Remedy in Cases of Business-Related Human Rights Abuse: A Practical Guide for Non-State-Based Grievance Mechanisms (2024), pp. 27-30.

96 For comparison, the EU Digital Services Act (DSA) specifies that complaint mechanisms must be user-friendly, accessible exclusively via electronic means, and remain available for at least six months. Notices must allow users to provide information that is sufficiently precise and adequately substantiated, including: a description of the alleged illegality; the URL or other details identifying the location of the content; the name and email of the complainant; a statement confirming the bona fide belief of the complainant regarding the illegality of the content.

information about a user's health status". This approach clearly aims to safeguard fundamental rights to privacy and data protection, and its inclusion in the Draft Law is commendable.

91. However, the list of protected categories is not comprehensive, omitting several types of sensitive data that are widely recognised as deserving heightened protection, including religious or other beliefs, trade union membership, genetic data, data concerning a persons' sex life or sexual orientation.[97] Therefore, **the legal drafters should consider supplementing Article 11 of the Draft Law to include additional categories – specifically religious or other beliefs, trade union membership, and sexual orientation or sex life – to ensure comprehensive protection of users' rights and prevent discriminatory profiling practices on these grounds**. Extending the Draft Law in this manner would bring it closer to international good practices, align with established standards in comparative data protection law, and reinforce the principle that recommendation systems must respect the full spectrum of sensitive personal data when delivering personalized content to users.

6.4. Content Moderation

92. Article 12 of the Draft Law obliges platforms to: improve content moderation systems; enhance functioning of artificial intelligence (AI) technologies "in compliance with the law"; improve systems for protecting children from information harmful to their health on the online platform; improve mechanisms for countering unlawful content dissemination, as well as mechanisms for cooperating with state authorities of Uzbekistan.

93. While agreeable in principle, the obligation is expressed in vague and ambiguous terms, and is unlikely to provide service providers with sufficient guidance on the specific conduct expected of them. With respect to the first two paragraphs of Article 12, which address content moderation and AI technologies, it is worth noting that, at the international level, there is an increasing trend towards the use of automated detection tools to identify and intervene against illegal or harmful content on online platforms. While such tools can assist platforms in meeting increasingly demanding and complex regulatory obligations, their deployment raises significant concerns. These include the risk of imposing prior restraints on freedom of expression, the lack of transparency and contextual understanding[98] inherent in such technologies - making them prone to an overly broad application of rules[99] - as well as their susceptibility to bias.[100] For these reasons, OSCE guidance[101] urges States not to impose legal obligations on platforms to proactively deploy automated detection systems but instead to: (i) provide clear and detailed guidance, typically through judicial authorities, on what constitutes illegal content under the relevant legal framework, differentiating among different categories of illegality; and (ii) legally require human rights due diligence of algorithmic content moderation and data-driven business models. Against this backdrop, Article 12 does not

97 See, as a comparison, Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), Article 8, and *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, 10 October 2018; see also ECtHR, *Uzun v. Germany*, App. no. 35623/05, 2 September 2010, para. 52, where the ECtHR has emphasised that personal data should be considered sensitive when its collection or processing is likely to reveal information about an individual's conduct, opinions, or feelings. See also, as a comparison, the EU General Data Protection Regulation, which explicitly prohibits processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, health data, or data concerning a person's sex life or sexual orientation (see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)).

98 See OSCE/RFoM, *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual*, 2022, p. 25.

99 *Ibid*, p. 17.

100 *Ibid*, p. 35. See also EU Fundamental Rights Agency (EU FRA), *Bias in Algorithms – Artificial Intelligence and Discrimination* (2022).

101 See OSCE/RFoM, *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual*, 2022.

appear likely to mandate the use of such technologies, which is a positive feature. **Nonetheless, the provision would benefit from greater precision regarding the measures expected of platforms and the level of "improvement" that is to be achieved.** Where online platforms do use automated systems and algorithms, including for content moderation, it is essential to establish robust review mechanisms for evaluating their impact in practice, particularly regarding potential differences in how various groups are affected and whether the use of these systems may inadvertently perpetuate discrimination, including gender-based discrimination. Findings of such review mechanisms may support the conclusion that certain detection algorithms are not fit for purpose, particularly in the context of identifying unlawful content, and that content moderation decisions should remain subject to meaningful human oversight.[102] Hence, **the Draft Law should require platforms to conduct human rights due diligence, particularly in relation to algorithmic content moderation and data-driven business models if/when those are used, including to identify potential discriminatory impact on different groups of users.**

RECOMMENDATION C.

1. To enhance Article 7 of the Draft Law by incorporating precise content categories of material and information genuinely harmful to children and related safety measures or by delegating specifics to guidelines to be issued by the authorized body.
2. To clarify in the Draft Law whether online platforms lose immunity from liability upon receiving user notices and gaining actual knowledge or awareness about content deemed unlawful.
3. To expand the list of data categories for which profiling is prohibited under Article 11 of the Draft Law to also cover religious or other beliefs, trade union membership, and sexual orientation or sex life, thereby ensuring comprehensive protection of users' rights and preventing discriminatory profiling practices.
4. To clarify procedural requirements for a submission mechanism of user complaints in Article 10 of the Draft Law, ensuring online platforms provide adequate and easily accessible information for the users about the complaint mechanism; establish clear, transparent, free of charge, user-friendly, accessible submission channels, timely acknowledgment and processing of complaints, proper documentation and tracking of complaints, and proportionate obligations for platforms based on their size.

7. RIGHTS AND OBLIGATIONS OF ONLINE USERS AND WEBSITE OWNERS

94. Article 18 of the Draft Law grants online platforms, online users and website owners the right to appeal orders and directives issued by the Agency before a court. Submission of an appeal suspends the execution of the contested measure, and platform or website owners may submit their observations during the proceedings.

95. While this is a positive safeguard, the Draft Law limits the right to submit observations on the findings issued by the Agency to website or platform owners only, excluding

102 See e.g., See UN General Assembly, *Resolution 78/213 Promotion and protection of human rights in the context of digital technologies*, 22 December 2023; and EU Fundamental Rights Agency (EU FRA), *Bias in Algorithms – Artificial Intelligence and Discrimination* (2022), Sub-Section 3.6.

individual users whose content may be directly affected. This raises concerns regarding equality of access to judicial remedies and equality of arms, potentially undermining procedural fairness, protected under Article 14 of the ICCPR. **To ensure consistency with international standards, the Draft Law should extend the right to submit observations to all affected parties.**

96. According to the Draft Law (Article 22 (1) (2)), influencers and website owners must refrain from disseminating information that may "*lead to humiliation or discrediting of an individual, or harm the business reputation of an individual*". While protecting the reputations of others is expressly mentioned in Article 19 (3) of the ICCPR, the notion of "humiliation" is ambiguous and can overlap with reputation to the point of confusion. For greater legal certainty, it is recommended to remove this wording from Article 22.

97. Article 19(3)(a) of the ICCPR refers to the protection of the reputation or rights of others (which would also include their business reputation) as a legitimate ground for limiting the right to freedom of expression; Article 17(2) of the ICCPR also provides that everyone has the right to the protection of the law from "*unlawful attacks on [one's] honour and reputation*". The UN Human Rights Committee's General Comment No. 16 on Article 17 of the ICCPR further provide that "*[p]rovision must also be made for everyone effectively to be able to protect himself against any unlawful attacks that do occur and to have an effective remedy against those responsible*". At the same time, the protection of the right to privacy is not absolute and limited interference with private life may be justified for the protection of rights and interests of others or in the public interest. In this respect, the UN Human Rights Committee has underlined that "*the protection of privacy is necessarily relative*" and may be restricted, especially in cases where knowledge about an individual's private life is "*essential in the interests of society*".[103] In addition, "*legislation must specify in detail the precise circumstances in which such interferences may be permitted*".[104] At the Council of Europe level, the ECtHR also seeks to achieve a fair balance where freedom of expression comes into conflict with the right to respect for private life and a person's reputation.[105] As already recommended in the Joint ODIHR-RFoM Opinion on the Draft Information Code of Uzbekistan,[106] **the Draft Law should specify that restrictions on online content imposed for respect of the reputation of others are only permissible if, in individual cases, the disclosure of certain information threatens to cause substantial harm to the protected interests, and if the harm outweighs the public interest in disclosure of such information.** Moreover, the Draft Law should also incorporate an explicit defence or exemption for content that, while possibly harming the reputation of individuals or businesses, is nonetheless true and disseminated in the public interest.

98. The Draft Law further imposes certain liability on influencers and website owners for third-party content (Article 22(1) (3)) by requiring monitoring of comments and reviews and removal of illegal content. As a comparison, ECtHR case-law clarifies that such liability should be contextual and proportionate, considering: the nature and severity of content; the size and commercial purpose of the platform; the possibility of identifying

103 See General Comment No. 16, "Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", United Nations, Human Rights Committee, 8 April 1988, para. 7.

104 *Ibid.* para. 8.

105 Where freedom of expression comes into conflict with the right to respect for private life guaranteed by Article 8, the ECtHR has set forth criteria for the balancing exercise including: whether the expression contributed to a debate of general interest; the public status of the person subjected to the statement; the prior conduct of the person who is the subject of criticism; the truth defence (where the expression contains factual statements); the content, form and the consequences of the expression/publication; the severity of the sanctions; see e.g., ECtHR, *Jerusalem v. Austria*, no. 26958/95, 27 February 2001, para. 40; *Ruokanen and Others v. Finland*, no. 45130/06, 6 April 2010, para. 52; *Lindon, Otchakovsky-Laurens and July v. France* [GC], nos. 21279/02 and 36448/02, 22 October 2007, para. 59. See also Venice Commission, *Amicus Curiae Brief for the Constitutional Court of Georgia on the Question of the Defamation of the Deceased*, CDL-AD(2014)040, para. 23..

106 See OSCE/ODIHR-OSCE RFoM, *Joint Opinion on the Draft Information Code of the Republic of Uzbekistan* (2024), Section 5.1.7.

the original author; the measures taken to prevent harmful dissemination.[107]In light of this, the **drafters are encouraged to qualify the proposed model of liability for third-party content by adopting a more flexible and proportionate framework that calibrates liability of website owners and influencers according to the aforementioned criteria**.

99. Article 22 (1) (6) requires influencers and website owners to publish a retraction at the request of individuals or entities claiming that false information has harmed their honour, dignity or reputation. It should be noted at the outset that an obligation to publish a retraction constitutes an interference with freedom of expression.[108] As such, it should comply with the strict three-part test of legality, legitimacy, necessity and proportionality under Article 19 (3) of the ICCPR, with the proportionality being assessed on a case-by-case basis.[109] Accordingly, a law imposing a general duty to comply with any such request by an individual or entity would appear disproportionate, unless accompanied by a corresponding court order. **In this respect, Article 22 (1) (6) should require that such request(s) be accompanied by the related court decision ordering the publication of a retraction.**

100. Moreover, Article 22 overlaps with Articles 13, 15 and 17, particularly regarding content deemed false, defamatory, or unlawful. The Draft Law currently lacks clarity on: which procedure applies in specific cases; how obligations to comply with Uzbek legislation interact with content removal or suspension mechanisms. In this respect **it is recommended to distinguish procedures explicitly, specifying triggers and timelines for each type of intervention** (see also Sub-section 8 *infra*).

101. Finally, Article 24 (4) of the Draft Law empowers the authorized body to order rectification of the violations of the Draft Law within 30 days. This provision is substantively broad and procedurally vague. It does not define which specific violations are covered by it; it also potentially overlaps with the procedures set out in Articles 15, 17, and 22. To avoid legal uncertainty and overlapping enforcement mechanisms, the Draft Law should either clarify the scope and specific application of Article 24 (4) or consider removing it, relying instead on existing, clearly delineated procedures in Articles 15, 17, and 22.

RECOMMENDATION D.

1. To amend Article 18 (3) of the Draft Law by ensuring that, like the owners of online platforms and website owners, users also have the right to submit observations on the findings issued by the Agency when challenging the orders and directives of the authorized body in a court of law.

2. To amend Article 22 (1) (3) of the Draft Law by qualifying the liability model and adopting a more flexible and proportionate framework regarding liability of influencers and website owners for third-party content, considering such factors as the nature and severity of content, size and commercial purpose of the platform, possibility of identifying the original author, measures taken to prevent harmful dissemination.

107 See ECtHR, *Delfi AS v. Estonia*, no. 64569/09, 16 June 2015; *MTE v Hungary*, no. 22947/13, 2 February 2016; *Pihl v. Sweden*, no 74742/14, 7 February 2017; *Tamiz v. UK*, no. 3877/14, 19 September 2017.

108 See e.g., ECtHR, *Eker v. Turkey*, no. 24016/05, 24 October 2017.

109 As a comparison, see ECtHR, *Smolorz v. Poland*, no. 17446/07, 16 October 2012

3. To amend Article 22 (1) (6) of the Draft Law to require that any request of individuals or entities to publish retractions should be accompanied by the related court decision ordering the publication of a retraction.

8. UNLAWFUL CONTENT

8.1. Grounds for Classifying Information as Unlawful Content

102. Article 13 of the Draft Law lists the grounds for classifying information as unlawful content.[110] At the outset, it should be underlined that international human rights law recognizes only a limited number of types of expression which States must prohibit or render punishable (by law),[111] providing that the legal provisions are strictly interpreted in accordance with international freedom of expression standards, especially when dealing with "incitement".[112] Outside of these limited and narrowly defined exceptions, states should as a default refrain from prohibiting expression or considering certain content unlawful or illegal.

103. While several of the grounds listed in Article 13 correspond to those envisaged in international human rights law and recommendations, certain categories merit closer examination, as set out below.

---

110 i.e., 1) Information containing calls for the violent alteration of the existing constitutional order or the territorial integrity of the Republic of Uzbekistan; 2) Information containing calls for mass riots and looting, violence against citizens, or the forcible eviction of citizens, as well as information aimed at coordinating such unlawful actions; 3) False information posing or creating a threat to public order or public safety; 4) Propaganda of war, violence, and terrorism, as well as the promotion of extremism, separatism, and fundamentalism, including the use of symbols or insignia of extremist or terrorist organizations; 5) Information disclosing state secrets or other legally protected confidential information; 6) Information inciting national, racial, ethnic, or religious hatred; 7) Information, including that expressed in an obscene manner, demonstrating disrespect toward society, the state, or state symbols; 8) Information promoting narcotic drugs, psychotropic substances, and precursors; 9) Pornographic material, information promoting cruelty, or inciting acts of suicide; 10) Information aimed at persuading or otherwise involving citizens, including minors, in unlawful acts that pose a threat to their life and/or health or to the life and/or health of others; 11) Information containing links to phishing or spam resources; 12) Information that calls for, promotes, or incites the commission of other acts resulting in criminal, administrative, or other legal liability as established by law.

111 These include: "*direct and public incitement to commit genocide*", which should be punishable as per Article III (c) of the Convention on the Prevention and Punishment of the Crime of Genocide to which Uzbekistan acceded on 9 September 1999; the "*propaganda for war*" and the "*advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*", which should be prohibited as per Article 20 (1) and (2) of the ICCPR (see also OSCE RFoM, Non-Paper on Propaganda and Freedom of the Media (2015), especially with reference to propaganda for war and hatred that leads to violence and discrimination); "*all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as […] incitement to [acts of violence] against any race or group of persons of another colour or ethnic origin*", which should be an offence punishable by law according to Article 4 (a) of the ICERD; "*public provocation to commit acts of terrorism*", when committed unlawfully and intentionally should be criminalized (see UN Security Council Resolution 1624 (2005)); "*child sexual exploitation material*" which shall be criminalized as per Articles 2 (c) and 3 (1) (c) of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography", to which Uzbekistan acceded on 23 December 2008. International recommendations also call upon States to enact laws and measures, as appropriate, "*to clearly prohibit and criminalize online violence against women, in particular the non-consensual distribution of intimate images, online harassment and stalking*", including *"[t]he threat to disseminate non-consensual images or content*", which must be made illegal; see UN Special Rapporteur on violence against women, its causes and consequences, Report on online violence against women and girls from a human rights perspective (18 June 2018), A/HRC/38/47, paras. 100-101. As a comparison, General Policy Recommendation No. 7 of the European Commission against Racism and Intolerance (ECRI) recommends to make it a criminal offence to publicly incite to violence, hatred or discrimination, or to threaten an individual or group of persons, for reasons of race, colour, language, religion, nationality or national or ethnic origin where those acts are deliberate. See also Council of Europe Committee of Ministers, Recommendation CM/Rec(2022)16 on combating hate speech, adopted by the Committee of Ministers on 20 May 2022, para. 11.

112 Regarding the prohibition of incitement to discrimination, hostility or violence specifically (Article 20 of the ICCPR and Article 4 of the ICERD), it is also subject to the strict conditions of Article 19 of the ICCPR, see UN Human Rights Committee (CCPR), *General Comment no. 34 on Article 19: Freedoms of opinion and expression*, 12 September 2011, para. 11 and CERD, *General recommendation No. 35* (2013), paras. 19-20. Such forms of expression would only be prohibited and punishable by law when: (1) the expression is intended to incite imminent violence; and (2) it is likely to incite such violence; and (3) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence; taking into account a number of factors to determine whether the expression is serious enough to warrant restrictive legal measures including the context, speaker (including the individual's or organization's standing), intent, content or form, extent of the speech, and likelihood of harm occurring (including imminence); see CERD, *General recommendation No. 35* (2013), paras. 13-16; see also the *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*, in the Report of the United Nations High Commissioner for Human Rights on the prohibition of incitement to national, racial or religious hatred, United Nations General Assembly, 11 January 2013, Appendix, para. 29; and International Mandate-holders on Freedom of Expression, *Joint Declaration on Freedom of Expression and Countering Violent Extremism* (2016), para. 2(d).

8.1.1. False Information

104. Article 13 (2) (3) prohibits the dissemination of "*false information posing or creating a threat to public order or public safety*".

105. While the dangers of false information in the online sphere are well documented as it can polarize public debate, fuel violent narratives and disseminate speech inciting hatred,[113] and ultimately undermine democratic institutions and trust in electoral processes, the current wording of Article 13 grants broad discretionary powers to the authorities in determining what would qualify as "false information" (see also Sub-section 4.2. *supra*) and what would qualify as a "threat," which also should be serious enough to justify prohibition. The reliance on "public order" as an isolated justification is especially problematic.[114] As a legal standard, public order is inherently broad and context-dependent, and without further qualification or consistent judicial interpretation, the proposed wording would fail to meet the requirement of legal certainty, a core principle under the ICCPR (and the ECHR).

106. In this respect, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has noted that such vague language tends to encourage over-removal and self-censorship, as individuals and businesses seek to avoid penalties by erring on the side of caution, filtering lawful speech of uncertain legal status.[115] It should also be noted that the UN Special Rapporteur has repeatedly warned against the use of "*vague and overly broad laws to criminalize, block, censor and chill online speech*".[116] The UN Special Rapporteur has repeatedly encouraged States to adopt multi-dimensional, multi-stakeholder responses to disinformation, emphasising the role of civil society, media, international organizations, and private companies.[117]

107. **Consequently, as already recommended above in Sub-Section 4.2, the provision of Article 13 (2) (3) should provide for a more narrow and precise definition of the information qualifying as unlawful content requiring the defining elements as mentioned in Sub-Section 4.2. It should also specify what should be considered as a "threat" for the purposes of Article 13 (2) (3) as well as establish the threshold of gravity for such "threat" to warrant unlawfulness and subsequent prohibition. Otherwise, the vague and expansive wording of the proposed Article could enable disproportionate or arbitrary restrictions, generate a chilling effect on online speech, and undermine public debate.**

8.1.2. Propaganda of Terrorism and Promotion of "Extremism", and "Fundamentalism"

108. Article 13 (2) (4) qualifies as unlawful content the propaganda of terrorism and the "*promotion of extremism, separatism, and fundamentalism, including the use of symbols*

113 There is no internationally agreed definition of "hate speech". However, the term was defined by the Council of Europe Committee of Ministers in Council of Europe Committee of Ministers, Recommendation CM/Rec(2022)16 on combating hate speech, adopted by the Committee of Ministers on 20 May 2022, which distinguishes between (i) hate speech that is prohibited under criminal law; (ii) hate speech that is subject to civil or administrative law; and (iii) other offensive or harmful types of expression requiring alternative responses (in the same vein, see also: UN Office of the High Commissioner for Human Rights (OHCHR), Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (2012). The United Nations Strategy and Plan of Action on Hate Speech, launched by the UN Secretary-General in May 2019, also provides a definition of hate speech; it should be noted, however, that the latter document addresses United Nations' institutions, and not states. See also ODIHR, *Hate Crime Laws: A Practical Guide*, 2nd edition, 2022, Sub-Section 3.4.

114 See e.g., CJEU, Opinion of Advocate General Pitruzzella, Case C-380/18, ECLI:EU:C:2019:609, 2019, para. 32

115 See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report on Freedom of Expression and the Private Sector in the Digital Age*, A/HRC/32/38, 2016.

116 See Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on 'Disinformation and freedom of opinion and expression', A/HRC/47/25, 2021, para. 55; see also para. 89 where it is underlined that "*Criminal law, in particular, should be reserved for the most exceptional cases, such as incitement to violence, hatred, or discrimination*".

117 Report on "Disinformation and freedom of opinion and expression", para. 87.

or insignia of extremist or terrorist organizations". As noted above, limitations formulated in vague and overbroad terms, including terms, such as "fundamentalism" or "extremism", which lack an internationally agreed definition, will not satisfy the ICCPR requirement that restrictions need to be "prescribed by law", as this means that laws need to be formulated with sufficient precision, clarity and foreseeability. Some of the terms used in Article 13 (2) (4) are overly vague or broad and could make the implementation of the restrictions unpredictable as they may be open to varying conflicting interpretations and potentially subject to arbitrary application.

109. As regards propaganda of terrorism, UN Security Council Resolution 1624 (2005) has expressly called on states to prohibit "incitement to terrorism" (rather than its propaganda or promotion).[118] To be human rights-compliant, the offence of "incitement to terrorism or acts of terrorism" must be prescribed by law in a precise language and (a) expressly refer to the intent to communicate a message and intent that this message incite the commission of a terrorist act; (b) be limited to the incitement to conduct that is truly terrorist in nature; and (c) include an actual (objective) risk that the act incited will be committed.[119] Additionally, laws must preserve the application of legal defences or principles leading to the exempt from criminal liability in certain cases,[120] for instance to safeguard legitimate activities (such as the defence or exercise of human rights and fundamental freedoms, activities of human rights and humanitarian organizations, etc.)[121], or when the statements were intended as part of a good faith discussion or public debate on a matter of religion, education, scientific research, politics, arts or some other issue of public interest.[122] **Hence, this part of Article 13 (2) (4) should be revised to**

118 See Resolution 1624 (2005), United Nations, Security Council 14 September 2005, UN Doc. S/RES/1624 (2005), para. 1, which calls on states to prohibit, by law, incitement to commit terrorist acts.

119 See the model offence of incitement to terrorism provided by the UN Special Rapporteur on Counter-Terrorism and Human Rights in the 2010 Report on "Ten areas of best practices in countering terrorism", A/HRC/16/51, 22 December 2010, para. 31. As expressly stated by the International Mandate-Holders on Freedom of Expression *"[i]ncitement should be understood as a direct call to engage in terrorism, with the intention that this should promote terrorism, and in a context in which the call is directly causally responsible for increasing the actual likelihood of a terrorist act occurring*"; see UN Special Rapporteur on freedom of opinion and expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005 Joint Declaration, Sub-Section on Antiterrorism measures. See also e.g., International Mandate-Holders on Freedom of Expression, 2011 Joint Declaration on Freedom of Expression and the Internet, Section 8 on Security and Freedom of Expression, para. 1 (d). See also OSCE TNTD/SPMU-ODIHR, Guidebook on Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach (2014), page 42; and ODIHR, Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters" within a Human Rights Framework (2018), pages 53 and 55. See also Principle 6 of the Johannesburg Principles on Freedom of Expression and National Security (1995), adopted on 1 October 1995 by a group of experts in international law, national security, and human rights and endorsed by the UN Special Rapporteur on freedom of opinion and expression. For reference, see also, for the purpose of comparison, Article 5 of the 2005 CoE's Convention on the Prevention of Terrorism on the "*public provocation to commit acts of terrorism*", defined as "*the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed*".

120 See the model offence of incitement to terrorism provided by the UN Special Rapporteur on Counter-Terrorism and Human Rights in the 2010 Report on "Ten areas of best practices in countering terrorism", A/HRC/16/51, 22 December 2010, para. 31. As expressly stated by the International Mandate-Holders on Freedom of Expression *"[i]ncitement should be understood as a direct call to engage in terrorism, with the intention that this should promote terrorism, and in a context in which the call is directly causally responsible for increasing the actual likelihood of a terrorist act occurring*"; see UN Special Rapporteur on freedom of opinion and expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005 Joint Declaration, Sub-Section on Antiterrorism measures. See also e.g., International Mandate-Holders on Freedom of Expression, 2011 Joint Declaration on Freedom of Expression and the Internet, Section 8 on Security and Freedom of Expression, para. 1 (d). See also OSCE TNTD/SPMU-ODIHR, Guidebook on Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach (2014), page 42; and ODIHR, Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters" within a Human Rights Framework (2018), pages 53 and 55. See also Principle 6 of the Johannesburg Principles on Freedom of Expression and National Security (1995), adopted on 1 October 1995 by a group of experts in international law, national security, and human rights and endorsed by the UN Special Rapporteur on freedom of opinion and expression. For reference, see also, for the purpose of comparison, Article 5 of the 2005 CoE's Convention on the Prevention of Terrorism on the "*public provocation to commit acts of terrorism*", defined as "*the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed*".

121 And other legitimate activities, such as for education, scientific and academic research, legal assistance, journalistic or artistic purposes; see the Note on the Proposed Revision of the Definition of Terrorist Offences in Article 1 of the Council of Europe Convention on the Prevention of Terrorism (28 September 2023), ODIHR, paras. 20-24.

122 See e.g., Legal Analysis of the Proposed Bill C-51, the Canadian Anti-terrorism Act, 2015: Potential Impact on Freedom of Expression, RFoM, May 2015, pages 9-10

prohibit direct and public incitement to terrorism in a human-rights compliant manner as described above rather than its propaganda.

110. Regarding the promotion of so-called "extremism" and "fundamentalism", it must be emphasized that there is no consensus at the international level on a normative definition of "*extremism*"/"*extremist*", "*violent extremism*" or "*fundamentalism*".[123] ODIHR, the Venice Commission and other international bodies have raised concerns pertaining to "*extremism*" and "*fundamentalism*" as legal concepts and the vague and imprecise nature of such terms.[124] As noted by ODIHR and RFoM in their previous Joint Opinions on the regulation of mass media and Draft Information Code of Uzbekistan, "*the vagueness of such terms may allow States to adopt highly intrusive, disproportionate and discriminatory measures, as demonstrated by the findings of international human rights monitoring mechanisms, which point to persistent problems, in particular, with so-called "extremism" charges and the implications on the rights to freedom of religion or belief, expression, association, and peaceful assembly as well as the occurrence of unlawful arrests, detention, torture and other ill-treatment […]."*[125] **It is thus recommended to revise Article 13 (2) (4) by removing the respective wording, unless the nexus to violence is made clear and they would constitute incitement to violence defined in accordance with international human rights standards.** The concerns related to "extremism" similarly extend to so-called "extremist organizations".

111. With respect to "separatism", which isintrinsically linked to the principle of respect for territorial integrity and sovereignty of a state, this joint opinion refers to the ODIHR *Comments on the Criminalization of "Separatism" and Related Criminal Offences* (2023) and concerns raised therein. In this respect, a ban on so-called "separatist" ideas should not lead to undue interferences with the legitimate forms of expression as well as with the protection and promotion of the rights of persons belonging to national minorities.[126] With respect to the "*symbols or insignia of extremist or terrorist organizations",* Article 19 of the ICCPR not only protect the substance of the ideas and information expressed, but also the form in which they are conveyed,[127] including symbols[128] or symbolic acts.[129] Generally, States are not prevented from banning, or even criminalizing, the use of certain symbols, providing that the ban is provided by a law that is accessible and formulated with sufficient precision, clearly specifying which symbols are banned, while ensuring that the ban responds to "*a pressing social need*" and is proportionate to the

123 See 2015 Thematic Report, United Nations, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (hereinafter "UN Special Rapporteur on Counter-terrorism and Human Rights"), A/HRC/31/65, 22 February 2016, paras. 11 and 21, noting that *"[d]espite the numerous initiatives to prevent or counter violent extremism, there is no generally accepted definition of violent extremism, which remains an 'elusive* concept". See also Report on the phenomena of fundamentalism and extremism, United Nations, Special Rapporteur in the field of cultural rights, A/HRC/34/56, 16 January 2017paras. 10-11; and 2018 Report on the Mission to Uzbekistan, United Nations, Special Rapporteur on Freedom of Religion or Belief, A/HRC/37/49/Add.2, 22 February 2018, para. 51, where it is emphasized that "*when employed as criminal legal categories, vague terms such as 'extremism' and 'fundamentalism' terms are irreconcilable with the principle of legal certainty as well as being incompatible with the fundamental rights mentioned*". See also Joint Opinion on the Draft Law of Uzbekistan "On Freedom Of Conscience And Religious Organizations, OSCE/ODIHR and Venice Commission 12 October 2020, para. 30; and Joint legal analysis of the draft law on mass media of the Republic of Uzbekistan, OSCE/ODIHR-OSCE/RFoM, November 2021, pp. 18-19.

124 *Ibid.* Joint Opinion on the Draft Law of Uzbekistan "On Freedom Of Conscience And Religious Organizations, OSCE/ODIHR and Venice Commission 12 October 2020, para. 30; and 2018 Report on the Mission to Uzbekistan, United Nations, Special Rapporteur on Freedom of Religion or Belief, A/HRC/37/49/Add.2, 22 February 2018, para. 51. See also, 2020 Report on the human rights impact of policies and practices aimed at preventing and countering violent extremism, United Nations, Special Rapporteur on Counter-Terrorism and Human Rights, 21 February 2020, A/HRC/43/46, paras. 12-14.

125 See Joint legal analysis of the draft law on mass media of the Republic of Uzbekistan, OSCE/ODIHR and OSCE/RFoM, November 2021, pp. 18-19. See also Joint Opinion on the Draft Law of Uzbekistan "On Freedom Of Conscience And Religious Organizations, OSCE/ODIHR and Venice Commission, 12 October2020, para. 30.

126 See OSCE/ODIHR, Guidelines on the Protection of Human Rights Defenders, 2014, paras. 205 and 206.

127 See ODIHR, *Opinion on the Law on Countering Extremist Activity of the Republic of Moldova*, 30 December 2019, para. 35; see also ECtHR, *Oberschlick v. Austria (no. 1)*, no. 11662/85, 23 May 1991, para. 57.

128 See UN Human Rights Committee, *Shin v. Republic of Korea*, 926/2000 (2004), para. 7.2. See also e.g., ECtHR, *Vajnai v. Hungary* no. 33629/06, 8 July 2008, para. 49, where the ECtHR found a violation of Article 10 ECHR in a case where the applicant wore a five-pointed red star; see also ECtHR, *Fáber v. Hungary*, no. 40721/08, 24 July 2012), para. 36.

129 See e.g., ECtHR, *Shvydka v. Ukraine*, no. 17888/12, 30 October 2014.

legitimate aims pursued.[130] In that respect, the expression "*symbols or insignia of extremist organizations*" is not sufficiently clear and foreseeable to comply with the principle of legal certainty. **The reference to the symbols or insignia of so-called "*extremist organizations*" should be reconsidered, or at a minimum, revised and circumscribed more strictly and clearly, e.g., by expressly stating the purpose/characteristics of the movements/organizations, the symbols or insignia or which are prohibited (such as advocacy of the violent seizure of power, suppression of human rights and freedoms or incitement to hostility or violence against certain groups) or by expressly naming certain specific movements/organizations, which fulfil such legally defined criteria**.[131] **Similar concerns may be raised with respect to symbols or insignia of terrorist organizations.**

112. The above-mentioned safeguards are essential to ensure that the provision is not used to unduly restrict freedom of expression and opinion, pluralism, and legitimate political debate.[132]

8.1.3. Information Demonstrating Disrespect towards Society, State and State Symbols

113. Article 13 (2) (7) prohibits information that shows "*disrespect towards society, the state, or state symbols*". While the protection of national symbols may, in certain circumstances, constitute a legitimate interest, the UN Human Rights Committee has expressed specific concerns regarding laws on such matters as: *lese majesty*, disrespect for authority or for flags and national symbols, defamation of the head of state and the protection of the honour of public officials.[133] From a comparative perspective, the ECtHR has clarified that such protection can only serve as a *means to an end* (such as safeguarding social cohesion) rather than an end in itself.[134] At the same time, the ECtHR has underlined that where the sole intention of expression is to insult an institution or symbol, a proportionate sanction may be justified, although any interference must still be examined in light of the case as a whole — including the context, the nature of the remarks, and their contribution to public debate - so as to assess whether the restrictive measure applied was proportionate to the aim pursued and supported by relevant and sufficient reasons.[135]

114. As underlined in the 2024 Joint Opinion on the Draft Information Code of Uzbekistan,[136] legal regulation based on the overly broad and vague concepts, such as disrespectful behaviour towards society, the State and state symbols, which can hardly be properly defined for regulatory purposes, may allow for the unlimited discretion of the decision-makers and result in arbitrary and/or selective application of the Law. The proposed wording is overbroad and highly subjective, allowing for nearly limitless range of issues to fall within the scope of the ensuing restrictions. This lack of clarity could lead to arbitrary or discriminatory enforcement and would significantly affect the freedom of expression of individuals, but also of mass media outlets. The UN Human Rights

130 See e.g., ODIHR-Venice Commission, *Joint Amicus Curiae Brief for the Constitutional Court of Moldova on the Compatibility with European Standards of Law No 192 of 12 July 2012 on the Prohibition of the Use of Symbols of the Totalitarian Communist Regime and of the Promotion of Totalitarian Ideologies of the Republic of Moldova* (11 March 2013), para. 124; and ODIHR-Venice Commission, *Joint Interim Opinion on the Law of Ukraine "On the condemnation of the communist and national socialist (Nazi) regimes, and prohibition of propaganda of their symbols"* (21 December 2015), paras. 116-117.

131 See, for instance, the examples of the Czech Republic and Germany, ODIHR-Venice Commission, *Joint Amicus Curiae Brief for the Constitutional Court of Moldova on the Compatibility with European Standards of Law No 192 of 12 July 2012 on the Prohibition of the Use of Symbols of the Totalitarian Communist Regime and of the Promotion of Totalitarian Ideologies of the Republic of Moldova* (11 March 2013), paras. 33-34, 60-63 and 74-78.

132 See UN Human Rights Committee, *Concluding observations on the fifth periodic report of Uzbekistan*, 2020, paras. 20-21 and 44-45.

133 UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, para. 38.

134 See e.g., ECtHR, *Fragoso Dacosta v. Spain*, no. 27926/21, 8 June 2023, para. 27.

135 *Ibid*., para. 28.

136 See OSCE/ODIHR-OSCE RFoM, *Joint Opinion on the Draft Information Code of the Republic of Uzbekistan* (2024), Section 5.1.8.

Committee has observed that in the context of public debate concerning public figures active in the political domain and public institutions, the value placed by the ICCPR upon uninhibited expression is particularly high.[137] States should not prohibit criticism of institutions, such as the army or public administration,[138] either since such criticism is an essential element and enabler of public scrutiny, transparency and accountability of governance systems.

115. Furthermore, this provision should be considered alongside existing criminal offences of *defamation* and *insult* under the Criminal Code of Uzbekistan, which remain in force and already impose significant restrictions on speech, contrary to international and regional recommendations calling for the decriminalization of defamation and insult.[139] In addition, specific provisions criminalizing defamation of the President, state symbols, and government officials further compound these restrictions.[140]

116. In light of the above, **the proposed prohibition of "disrespect" towards society, the state, or state symbols – especially when considered in conjunction with existing criminal law provisions – raises serious concerns for freedom of expression and should be reconsidered entirely.**

8.1.4. Other Grounds

117. Article 13 (2) (5) prohibits the disclosure of state secrets or other legally protected confidential information. While the protection of certain state secrets may be justifiable for the protection of national security or public order, the provision as currently drafted does not adequately account for situations where disclosure serves the prevailing public interest. The UN Human Rights Committee has emphasized that the public's right to seek

137 General Comment No. 34 on Article 19 Freedoms of Opinion and Expression of the ICCPR, United Nations, Human Rights Committee, CCPR/C/GC/34, 12 September 2011, para. 38.

138 *Ibid.* para. 38.

139 See *OSCE Ministerial Council Decision No. 3 on the Safety of Journalists*, 12 December 2018, para. 11, calling upon the OSCE pSs to *"[e]nsure that defamation laws do not carry excessive sanctions or penalties that could undermine the safety of journalists and/or effectively censor journalists and interfere with their mission of informing the public and, where necessary, to revise and repeal such laws, in compliance with participating States' obligations under international human rights law*." International Mandate-Holders on Freedom of Expression, including the OSCE Representative on Freedom of the Media, in their 2022 Joint Declaration specifically noted: "*When women speak out about sexual and gender-based violence, States should ensure that such speech enjoys special protection, as the restriction of such speech can hinder the eradication of violence against women" and recommended that "States should decriminalise all defamation and insult actions, and enact comprehensive legislation to discourage vexatious or frivolous defamation cases and strategic lawsuits against public participation (SLAPPs) that are intended to intimidate and silence women and drive them out of public participation*" (International Mandate-Holders on Freedom of Expression, *Joint Declaration on Freedom of Expression and Gender Justice* (May 2022), para. 3(d)). See also UN Human Rights Committee (CCPR), *General Comment no. 34 on Article 19: Freedoms of Opinion and Expression*, 12 September 2011, para. 47, which notes: *"[d]efamation laws must be crafted with care to ensure that they comply with paragraph 3, and that they do not serve, in practice, to stifle freedom of expression. […] All such laws, in particular penal defamation laws, should include such defences as the defence of truth and they should not be applied with regard to those forms of expression that are not, of their nature, subject to verification. […] States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty. It is impermissible for a State party to indict a person for criminal defamation but then not to proceed to trial expeditiously – such a practice has a chilling effect that may unduly restrict the exercise of freedom of expression of the person concerned and others.*" See also the *UN General Assembly Resolution 76/173*, on the Safety of Journalists and the Issue of Impunity (A/RES/76/173), 10 January 2022, urging governments not to misuse defamation laws to censor and interfere with journalists' work and, *"where necessary, to revise and repeal such laws, in compliance with States' obligations under international human rights law";* see also *Reinforcing media freedom and the safety of journalists in the digital age – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/50/29), 20 April 2022. See also e.g., Parliamentary Assembly of the Council of Europe (PACE), *Resolution 1577 (2007) "Towards decriminalisation of defamation"*, which calls for state authorities to take the following actions, among others: abolish prison sentences for defamation; guaranteeing that there criminal prosecutions for defamation are not misused; defining the concept of defamation in more precisely in their legislation with enough precision so as to avoid arbitrary applications; making only incitement to violence, hate speech and promotion of negationism punishable by imprisonment; avoiding any increased protection for public figures; providing for appropriate legislative means for persons pursued for defamation to defend themselves, particularly the so-called 'truth defences'; setting reasonable and proportionate maxima for awards for damages and interest in defamation cases; providing appropriate legal guarantees against disproportionate awards. See also *European Commission Recommendation 2022/758*, 22 April 2022, calling upon Member States to "*specifically review their legal frameworks applicable to defamation to ensure that existing concepts and definitions cannot be used by plaintiffs against journalists or human rights defenders in the context of manifestly unfounded or abusive court proceedings against public participation*" and encourage Members States "*to favour the use of administrative or civil law to deal with defamation cases*".

140 Under these criminal provisions, penalties can be severe: sentences include imprisonment of up to five years (Article 158(3) of the Criminal Code), correctional labour, or substantial fines of up to 400 times the minimum wage (Article 138, Chapter VI of the Criminal Code, "Offences Against Freedom, Honour and Dignity").

and receive information is an essential element of Article 19 ICCPR, particularly where the media fulfils its role of scrutinizing public authorities and contributing to democratic accountability.[141] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has clarified that exceptions to the right to access information need to be justified on a case-by-case basis, and shall only apply where "*there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information*".[142] The Special Rapporteur also noted that such exceptions should be determined by an independent body, preferably a court, and not by the body holding the information in question.[143] Disclosure should not be limited in the absence of the Government's showing of "*a real and identifiable risk of significant harm to a legitimate national security interest*"[144] that outweighs the public's interest in the information to be disclosed.[145] If a disclosure does not harm a legitimate state interest, there is no basis for its suppression or withholding.[146] Similarly, the ECtHR has held that the disclosure of confidential information may, in certain circumstances, fall within the scope of protection of Article 10 ECHR, where such disclosure contributes to a matter of public concern.[147] In all cases related to the disclosure of classified information, the public's right to receive information must be carefully balanced against the potential harm caused by its disclosure. To align with these standards, **the Draft Law should be amended to include the balancing test stipulating that disclosure of classified information shall not be punishable by law if public interest in such disclosure outweighs/prevails over potential harm resulting from it. The Draft Law should also introduce an explicit public interest exemption for disclosures made for the purpose of exposing human rights abuses, public wrongdoing, corruption, abuse of power – although acknowledging that this information should never be classified in the first place, or other serious violations of law, are not prohibited or penalised.**[148]

118. Article 13 (2) (6) prohibits incitement to hatred on national, racial, ethnic, or religious grounds. This provision is consistent with Article 20(2) of the ICCPR, which requires States Parties to prohibit by law any "*advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*" and with Article 4 of the International Convention on the Elimination of Racial Discrimination (CERD)[149] requiring the States Parties to "*declare an offence punishable by law 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*". Article 20 of the ICCPR and Article 4 of the CERD do not prevent States from recognising additional protected characteristics. To enhance its effectiveness and bring it closer in line with international good practices, **the Draft Law could broaden the scope of prohibited incitement by drawing on regional instruments and recommendations, that address expression of hatred that**

141 See UN Human Rights Committee (CCPR), *General Comment no. 34 on Article 19: Freedoms of Opinion and Expression*, 12 September 2011.
142 United Nations, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report on the promotion and protection of the right to freedom of opinion and expression, A/68/362, 4 September 2013, paras. 76 (d) and 99.
143 *Ibid*, para. 99.
144 See e.g., Report on the Protection of Sources and Whistleblowers, United Nations Special Rapporteur on Freedom of Opinion and Expression, A/70/361, 2017, para. 47; and the Global Principles on National Security and the Right to Information (The Tshwane Principles), developed and adopted on 12 June 2013 by a large assembly of experts from international organisations, civil society, academia and national security practitioners, Principle 3(b).
145 See e.g., Report on the Protection of Sources and Whistleblowers, United Nations, Special Rapporteur on Freedom of Opinion and Expression, A/70/361, 2017, para. 10.
146 See the General Comment No. 34 on Article 19 of the ICCPR, United Nations, Human Rights Committee, CCPR/C/GC/34, para. 30.
147 See ECtHR, *Centre for Democracy and the Rule of Law v. Ukraine*, App. no. 10090/16, 26 March 2020; *Association Burestop 55 and Others v. France*, Apps. no. 56176/18, 56189/18, 56232/18 et al., 1 July 2021.
148 See OSCE/ODIHR-OSCE RFoM, *Joint Opinion on the Draft Information Code of the Republic of Uzbekistan* (2024), paras. 27-29.
149 International Convention on the Elimination of All Forms of Racial Discrimination (hereafter "CERD"), adopted on 21 December 1965, entered into force on 4 January 1969.

constitutes incitement to discrimination, hostility or violence on other grounds, including colour, language, nationality, national or ethnic origin, age, disability, sex, gender identity, and sexual orientation.[150] Such an extension would not only strengthen protection against discrimination and violence but also ensure greater coherence with contemporary international and regional standards. With regard to the qualification of incitement as unlawful or prohibited expression, the CERD Committee found that such form of expression would only be prohibited and punishable by law when: (1) the expression is intended to incite imminent violence; and (2) it is likely to incite such violence; and (3) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence. Assessment of the impugned expression should take into account a number of factors to determine whether the expression is serious enough to warrant restrictive legal measures including the context, speaker (including the individual's or organization's standing), intent, content or form of expression, extent of the speech, and likelihood of harm occurring (including imminence).[151] **These elements could be reflected in Article 13 (2) (6) to more narrowly circumscribe the prohibited content and reduce the risk of arbitrary or inconsistent interpretation**.

119. Article 13 (2) (9) declares pornographic material to be unlawful. While the ECtHR has recognised that certain restrictions on pornography may, in principle, pursue the legitimate aim of protecting morals, it has also emphasised that States must ensure such restrictions are proportionate. A blanket ban, such as that provided under the Draft Law, risks being overly broad and may not satisfy the proportionality requirement, particularly where it concerns adult audiences. **Less restrictive measures could be envisaged: for instance, restricting access to pornographic materials for persons under the age of eighteen, introducing age-verification mechanisms, and/or requiring targeted warnings for minors and other vulnerable groups.**[152]

120. Finally, it must be underlined that international recommendations also call upon States to enact laws and measures, as appropriate, **"*to clearly prohibit and criminalize online violence against women, in particular the non-consensual distribution of intimate images, online harassment and stalking*", including "*[t]he threat to disseminate non-consensual images or content*",** which must be made illegal.[153] **The legal drafters should consider supplementing Article 13 of the Draft Law** in this respect, though it should be acknowledged that to ensure effective mechanisms to counter online violence against women, this will also require law enforcement training, victim support mechanisms, and proper implementation of the Draft Law.

150 Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech, para. 2.

151 See CERD, General recommendation No. 35 (2013), paras. 13-16. See also the *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*, in the Report of the United Nations High Commissioner for Human Rights on the prohibition of incitement to national, racial or religious hatred, United Nations General Assembly, 11 January 2013, Appendix, para. 29; and International Mandate-holders on Freedom of Expression, *Joint Declaration on Freedom of Expression and Countering Violent Extremism* (2016), para. 2(d).

152 Recent legislative models, including the EU's Digital Services Act and the 2025 European Commission Guidelines on measures to ensure a high level of privacy, safety and security for minors online and the UK's Online Safety Act, impose specific duties of care on providers of pornographic content, focusing primarily on the protection of minors rather than prohibiting access for the general adult public. In this light, the Draft Law could be refined to narrow its scope, clarifying that restrictions are specifically aimed at safeguarding children and vulnerable groups, while respecting the principle of proportionality in relation to adult audiences.

153 See UN Special Rapporteur on violence against women, its causes and consequences, *Report on online violence against women and girls from a human rights perspective* (18 June 2018), A/HRC/38/47, paras. 100-101.

RECOMMENDATION E.

1. To remove the reference to vague and/or broad content-based restrictions, such as the promotion of "extremism" and "fundamentalism" – unless clearly linked to some elements of violence or other criminal means or incitement to violence as defined in accordance with international human rights standards.

2. To include in the Draft Law the balancing test stipulating that disclosure of classified information shall not be punishable by law if public interest in such disclosure outweighs/prevails over potential harm resulting from it, while providing for an explicit public interest exemption – ensuring that disclosures made for the purpose of exposing human rights abuses, public wrongdoing, corruption, abuse of power, or other serious violations of law are not prohibited or penalised.

3. To consider broadening the scope of prohibited expression of hatred that constitutes incitement to discrimination, hostility or violence to cover other grounds, beyond national, racial or religious hatred, including characteristics such as colour, language, nationality, national or ethnic origin, age, disability, sex, gender identity, and sexual orientation.

4. To supplement Article 13 with a clear prohibition of online violence against women, in particular, of the non-consensual distribution of intimate images, online harassment and stalking, including the threat to disseminate non-consensual images or content.

8.2. Monitoring of Online Platforms and Websites

121. Article 14 of the Draft Law deals with the monitoring of online platforms and websites. Article 14 does not appear to impose a duty on platforms to generally and proactively monitor their services for unlawful content. Instead, the responsibility lies with the Agency, which may also receive submissions from individuals and legal entities. Upon receiving information about unlawful content, the Agency must issue an opinion within one working day. At the same time, as already mentioned above, Article 8 of the Draft Law provides that unlawful content may be identified either through user complaints (see sub-section 6.2 *supra*) or through the platforms' own moderation processes.

122. This approach aligns with international and regional guidance and recommendations discouraging general monitoring obligations. The CoE Recommendation on Internet Intermediaries advises that *"State authorities should avoid any action that may lead to general content monitoring"*.[154] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression similarly recommended that States and international organizations *"refrain from establishing laws or arrangements that would require the proactive monitoring or filtering of content"*.[155] Both bodies, however, stress that governance of online content should ensure compliance of all actors with relevant international freedom of expression standards, professional standards, and human rights obligations. These include, among others, clearly defining illegal content and distinguishing it from "lawful but harmful" material, considering whether other

154 See e.g., CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018, para. 1.3.5.

155 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Content Regulation in the Digital Age* (A/HRC/38/35, 2018), para. 67.

public interest content obligations may apply, establishing proportionate sanctions for breaches of content standards, and providing accessible redress mechanisms.[156]

123. Private actors also carry responsibilities: platforms should align their content standards with international human rights law, rather than with divergent national laws or purely commercial interests[157] (see also Sub-Section 2.1 *supra*).

124. As underlined by the CoE, when state authorities are demanding intermediaries to restrict access to content, they should obtain an order by a judicial authority or by other independent administrative authority, whose decisions are subject to judicial review – except in exceptional cases, when content is *illegal irrespective of context* (e.g., child sexual abuse material) or where expedited measures are required in accordance with the conditions prescribed by Article 10 of the ECHR.[158] The CoE further stresses that States remain under an ultimate obligation to protect human rights and fundamental freedoms online, and that any regulatory system – whether statutory, self-regulatory, or co-regulatory – must include effective oversight and redress mechanisms.[159] Based on the above, the approach taken in the Draft Law to only require platforms to restrict content upon receiving a note from an authorized body corresponds to the international guidance, providing that such authorized body is independent and that there is access to an effective remedy. The latter requirement seems to be satisfied since Article 18 envisages a right to appeal the orders and directives of the authorized body by an owner of an online platform and/or their representative, an owner of a website, and a user of an online platform. Such appeal would suspend the execution of the impugned orders or directives pending a final court decision.

125. Article 14 provides that opinions of the Agency must specify the grounds and criteria based on which the content was deemed unlawful. This requirement introduces a degree of transparency and should in principle safeguard against arbitrary enforcement. The Draft Law's requirement for reasoned opinions from the authorized body should constitute a positive safeguard, provided that such opinions are sufficiently detailed, based on a human rights-based assessment of the content regulation, and subject to judicial oversight.

8.3. Legal Consequences for Distribution of Unlawful Content

8.3.1 Removal or Cessation of Distribution of Unlawful Content

126. Articles 15 and 17 of the Draft Law establish procedures for the removal or cessation of the distribution of unlawful content. Under these provisions, once the authorised body issues an opinion identifying unlawful content, it may order a website owner, platform user, or public page moderator to remove it. If these actors fail to comply or cannot be reached, the authorised body may direct the online platform itself to remove or block the content within Uzbekistan. Should the content remain accessible, the body may then petition a court to order its removal, suspend the relevant user account or page for up to six months, or both.

127. There are a number safeguards recommended to prevent arbitrary restrictions on freedom of expression online through blocking measures, including but not limited to: (i) prior notification of affected parties; (ii) an obligation on authorities to assess the impact of

156 *Recommendation CM/Rec(2022)11 of the Committee of Ministers of the CoE to member States on principles for media and communication governance*, adopted by the Committee of Ministers on 6 April 2022, para. 10.

157 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Content Regulation in the Digital Age* (A/HRC/38/35, 2018), para. 70.

158 See e.g., CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018, para 1.3.2.

159 *Ibid*, para. 1.1.3.

blocking measures, or to justify urgency where immediate action is necessary; (iii) giving an opportunity for website owners to voluntarily remove illegal content; and (iv) access to an independent adjudicatory body, such as a court, to challenge the measures.[160]

128. However, as mentioned above, the effectiveness of these safeguards may be undermined by the Draft Law's overly broad and vague definition of certain types of unlawful content heightening the risk of arbitrary, selective and/or inconsistent enforcement.

129. Furthermore, the Draft Law provides a separate procedure for websites allegedly distributing unlawful content. Under Article 17, if a website fails to comply with an order to remove content or if it is impossible to identify website's owner, the authorized body may unilaterally enter the site into the Register of platforms with reduced access speed or restricted access. Within 24 hours, the Ministry of Digital Technologies must enforce the restriction, thereby blocking access in Uzbekistan without prior judicial review.

130. Such an approach might appear disproportionate, as it allows for the blockage of entire websites, potentially on the basis of a single item of unlawful content e.g., a single instance of non-compliance with the respective removal order. This approach does not reflect the key principle of proportionality e.g., to apply the least restrictive measure possible among those effective enough to achieve the intended regulatory objective. For instance, even in circumstances that might justify blocking specific illegal material, ECtHR standards require a separate and distinct justification for blocking an entire website. In particular, the ECtHR case-law makes clear that "*the wholesale blocking of access to a website is an extreme measure which has been compared to banning a newspaper or television station*"[161] and that "[*s]uch a measure deliberately disregards the distinction between the legal and illegal information the website may contain and renders inaccessible large amounts of content which has not been identified as illegal*"[162]. **It is recommended, therefore, to reconsider this approach in the Draft Law.**

131. Article 16 of the Draft Law introduces an additional sanction: where a platform systematically fails to comply with court decisions, the authorized body may request a court order to reduce its data transmission rate in Uzbekistan. If granted, the Ministry of Digital Technologies may impose bandwidth throttling on the entire platform. The UN High Commissioner for Human Rights has recognized throttling as a form of internet shutdown, which can raise serious concerns under international human rights law.[163]

132. It should be also noted, that the scope of "systematic failure" as referred to in Article 16 of the Draft Law is not defined. It is unclear whether this refers solely to failures related to unlawful content or extends to unrelated court orders. The ambiguity gives authorities broad discretion to pressure online platforms. **It is thus recommended that the Draft Law provides for more clarity in this respect.**

8.3.2 Removal of False Information

133. Article 20 of the Draft Law defines the procedure for the removal of false information. This provision grants individuals and legal entities the right to request the removal of false information published about them on a website, public page, or online platform. If the request is denied, they may file a court claim. While the Draft Law addresses information that is both inaccurate and harmful to reputation, this provision appears to

160 See e.g., at the CoE level: the Strasbourg Court Establishes Standards on Blocking Access to Websites, Strasbourg observers, 2020, <https://strasbourgobservers.com/2020/08/26/the-strasbourg-court-establishes-standards-on-blocking-access-to-websites/>.
161 See e.g., ECtHR, *OOO Flavus and others v. Russia*, nos. 12468/15 and 2 others, ECtHR, 2020, para. 37.
162 *Ibid*.
163 *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights*, Report of the Office of the United Nations High Commissioner for Human Rights, 13 May 2022, A/HRC/50/55, paras. 4-6.

extend protection to information that is merely false, even if it does not damage reputation. As a result, its practical value may be limited. Nevertheless, the right to seek correction of inaccurate information can be considered part of broader data protection rights and may warrant safeguarding.

134. At the same time, such a provision carries a risk of misuse by individuals or entities seeking to suppress legitimate but unwelcome discussion. **To mitigate this, the Draft Law could be amended to require applicants to provide evidence demonstrating the falsity of the information in question**.

RECOMMENDATION F.

1. To reconsider the Draft Law provisions allowing the blocking of entire websites based on a single item of unlawful content e.g. a single failure to comply with the removal order, as this may violate the principle of proportionality, and instead consider more targeted measures, such as blocking specific illegal material, with whole-site blocking permitted only in narrowly defined cases and with separate, specific justification.

2. To clarify the meaning of "systematic failure" as referred to in Article 16 of the Draft Law as a basis to file the claim with the court seeking reduction of an online platform's data transmission rate.

3. To consider including in the Draft Law a possibility to request a correction of inaccurate information instead of an outright removal to protect the integrity of public discourse while balancing the right to reputation with freedom of expression.

4. To require in Article 20 of the Draft Law that the applicants provide evidence demonstrating the falsity of the information in order to request its removal.

9. RECOMMENDATIONS RELATED TO THE PROCESS OF PREPARING AND ADOPTING THE DRAFT LAW

135. OSCE participating States have committed to ensure that legislation will be "*adopted at the end of a public procedure, and [that] regulations will be published, that being the condition for their applicability*" (1990 Copenhagen Document, para. 5.8). Moreover, key commitments specify that "[*l]egislation will be formulated and adopted as the result of an open process reflecting the will of the people, either directly or through their elected representatives*" (1991 Moscow Document, para. 18.1). The ODIHR Guidelines on Democratic Lawmaking for Better Laws (2024) underline that "*all interested parties and stakeholders should have the opportunity to access the lawmaking process, be informed about it and be able meaningfully to participate and contribute*". The Venice Commission's Rule of Law Checklist also emphasizes that the public should have a meaningful opportunity to provide input and may be a useful source of good practice.

136. For consultations on draft legislation to be effective, they need to be inclusive and involve consultations and comments by the public, including civil society. They should also provide sufficient time for stakeholders to prepare and submit recommendations on draft legislation, while it is a good practice for the public authorities to provide meaningful and qualitative feedback in due time on the outcome of every public consultation, including clear justifications for including or not including certain proposals. To guarantee effective participation, consultation mechanisms must allow for input at an

early stage and throughout the entire process, meaning not only when the draft is being prepared by relevant public authorities but also when it is discussed before Parliament (e.g., through the organization of public hearings).

137. With respect to the regulation of the roles and responsibilities of intermediaries in particular, it is essential that states engage in a regular, inclusive and transparent dialogue with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments and academia, with a view to sharing and discussing information and promoting the responsible use of emerging technological developments related to internet intermediaries that impact the exercise and enjoyment of human rights and related legal and policy issues.[164]

138. In light of the above, the public authorities are encouraged to ensure that the current version of the Draft Law is subjected to further inclusive, extensive and meaningful consultations, including with representatives of civil society and of the media, offering equal opportunities for women and men to participate. According to the principles stated above, such consultations should take place in a timely and meaningful manner, at all stages of the law-making process, including before Parliament. In particular, future consultations should provide stakeholders with sufficient time to submit their feedback. As an important element of good law-making, a consistent monitoring and evaluation system of the implementation of the Draft Law and its impact should also be put in place that would continuously evaluate the operation and effectiveness of the Draft Law, once adopted.

[END OF TEXT]

164 See e.g., CoE Recommendation CM/Rec(2018)2, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", Council of Europe, Committee of Ministers, adopted on 7 march 2018, para. 12.