Guidelines to observe and assess online election campaigns

A DoP technical document

Endorsed by the DoP Implementation Meeting,

8 December, 2022

Following an inclusive review and discussion of Draft Guideline documents, the DoP organizations recognise the Guidelines as Technical Documents to aid the implementation of the Declaration of Principles. They do not require action by the political bodies of endorsing organizations (such as assemblies, councils, or boards of directors), though such actions are welcome.

Table of Contents

Background

1. The internet has significantly increased our capacity to receive and impart information, opening up new possibilities for political expression and participation, especially through online platforms.[1] By enhancing citizens' access to information, they facilitate voter awareness, engagement and mobilisation and they may reduce campaign costs for candidates and parties. They allow under-represented or marginalised groups to make their voices heard and, in countries with a diaspora eligible to vote, provide opportunities to reach voters living abroad. Wherever media pluralism and/or media freedom are limited offline, the internet often can be a source of diverse information, enabling citizens to access alternative opinions and information as well as voter education.

2. The 2020 Joint Declaration by the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE) and the Organization of American States (OAS) on Freedom of Expression and Elections in the Digital Age highlights "the importance of a dynamic media landscape, including traditional and digital media, and the increasingly essential role played by online platforms and digital technologies in protecting democratic environments".[2]

3. However, online platforms can also present a threat to the integrity of electoral processes, particularly through the dissemination of harmful content, disinformation, information manipulation and interference, privacy-invasive practices and risks of cybercrime, including hacking of accounts of politicians. Also, through their policies and targeted advertising, online platforms have the potential to significantly affect voters' choices if transparency requirements about political advertisement are not respected. Furthermore, technology companies can control the dissemination of and access to online content on their platforms and can facilitate the creation of online anti-democratic communities.

4. In some cases, access to online platforms for campaign purposes is curtailed or blocked completely by authorities, thereby denying political parties and candidates the opportunity to share their messages through online systems. In other situations, internet access is limited or non-existent and thus limits the opportunity for freedom of expression through the internet.

5. With the progressive digitalisation of electioneering and political communications, online campaigns are increasingly relevant in the context of election observation. The analysis of this aspect of the electoral process responds to the statement in the Declaration of Principles for International Election Observation (DoP) that "International election observation evaluates pre-election, election-day and post-election periods through comprehensive, long-term observation, employing a variety of techniques." The DoP also recalls that "*All observer missions must make concerted efforts to place the election day into its context and not to over-emphasize the importance of election day observations. International election observation examines conditions relating to the right to vote and to be elected, including, among other things, discrimination or other obstacles that hinder participation in electoral processes* […]."[3]

6. Certain contextual situations could disrupt traditional forms of election campaigning and contribute to a further long-term shift towards online platforms. In the case of the COVID 19 pandemic, for example, canvassing, rallies, and other grassroots gatherings were put on hold

[1] Messaging networks, such as WhatsApp, Telegram, Viber or Messenger are not included in the scope of this document due to data protection and privacy matters.
[2] *Joint declaration on freedom of expression and elections in the digital age*, April 2020, [Geneva / Vienna / Washington]: UN Special Rapporteur on Freedom of Opinion and Expression / OSCE Representative on Freedom of the Media / OAS Special Rapporteur on Freedom of Expression. https://www.osce.org/files/f/documents/9/8/451150_0.pdf
[3] Article 5, *Declaration of Principles for International Election Observation (DoP)*, October 2005.

in many countries, with online campaigning becoming the main channel for candidates and parties to mobilise support, communicate with voters and connect with their base.

7. Against this background, international election observation missions (IEOMs) are increasingly expected to assess online campaigns in their election observation methodology to assess whether key principles underpinning democratic elections are complied with in the online space.[4] The DoP states that international election observation "*is: the systematic, comprehensive and accurate gathering of information […]; the impartial and professional analysis of such information; and the drawing of conclusions about the character of electoral processes based on the highest standards for accuracy of information and impartiality of analysis*".[5]

8. During IEOMs, an exhaustive monitoring of online platforms is not feasible in practice due to the speed, reach and volume of the content produced, along with the unlimited number of web pages, accounts and websites. Like other aspects of election observation, the privacy-compliant assessment of online campaigns requires a comprehensive and transparent methodology defining the relevant applicable principles for democratic elections, the scope of observation and the analytical approach, as well as clear benchmarks for drawing conclusions and recommendations.

9. These Guidelines aim at establishing a common ground for organisations endorsing the DoP for the observation of campaigning on online platforms, websites and blogs. It is meant to be a "living document", reflecting evolving international standards and good practices as well as relevant methodological developments. This document builds on other publications on this topic produced by the United Nations Special Rapporteur on Freedom of Expression, the European Union (EU), the Organization for Security and Cooperation in Europe (OSCE), the Organization of the American States (OAS), the International Foundation for Electoral Systems (IFES), the National Democratic Institute (NDI), the Carter Center, Privacy International, Democracy Reporting International, UNESCO, the Kofi Annan Foundation, the Council of Europe and the Venice Commission.[6] It also reflects conclusions and comments elaborated in the DoP working group on online campaigning in May 2020.

Relevant international standards for online campaigns

10. Assessment of elections by IEOMs rests on international and regional human rights instruments, commitments and good practices concerning, *inter alia*, freedom of expression, the right to political participation, the right to privacy, freedom from discrimination, net neutrality[7] and access to information.

11. Freedom of expression and the right to free elections are the basic principles and, in essence, complementary. More generally, freedom of expression and the right to free elections are prerequisites of each other.

[4] In this document the term "online campaign" refers to any digital activities and messages produced by any individual or organisation and disseminated on the web to inform or persuade voters to vote for a particular option or to refrain from voting.
[5] Article 4, *DoP*.
[6] *Joint Report on Digital Technologies and Elections*, June 2019, Venice: Venice Commission / Directorate of information society and action against crime – Council of Europe; *Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts*, October 2019, [Washington]: OAS / Inter-American Commission on Human Rights; *Principles for a fundamental-rights compliant use of digital technologies in electoral processes*, December 2020, Venice: Venice Commission.
[7] On net neutrality, see *Recommendation (2016)5 on Internet freedom* (2016) Strasbourg: Council of Europe.

12. The right to **freedom of expression** is a key reference for assessing online campaigns. Several global and regional instruments have concluded that freedom of expression applies to the internet, as it does to all means of communication.[8] Restrictions to this right are legitimate if they are provided for by law and are necessary to protect an interest recognised under international law, in accordance with the "three-part test" of legality, legitimacy (public interest) and proportionality. The question of where freedom of expression ends and acceptable restrictions begin is the same whether the content is online or not. However, the online context presents additional challenges because illegal or harmful content can be created and disseminated much faster and on a far broader scale than offline. In addition, the anonymity of sources of such messaging often makes it difficult to enforce accountability responses.

13. The right to **political participation** requires freedom of expression, but it also focuses on how opinions are formed. This right, together with the right to freedom of opinion and thought, entails that voters are able to form opinions independently, free of violence or the threat of violence, compulsion, inducement or manipulative interference of any kind.[9] The concept of manipulative interference introduced by the CCPR General Comment 25 should not justify arbitrary deletion or prohibitions of certain types of content (except for incitement to hatred, incitement to violence and discrimination[10]), but it may provide a basis for discussions on the role and responsibility of technology companies, for example on content ranking, inauthentic accounts and behaviour.

14. **Transparency** has become a key principle in regulatory efforts for online campaigning.[11] Deceptive and misleading practices in content creation, information manipulation and dissemination can distort voters' perceptions and hamper access to diverse and accurate information, a pre-condition for making an informed choice in elections. Transparency has also emerged as a central principle in relation to campaign finance regulation, including spending on digital election campaigns, disclosure of financial sources, labelling of sponsored messages and micro-targeting practices.[12] Transparency is also relevant in relation to technology companies' internal policies on content moderation, algorithms and ranking.

15. International human rights law recognises the fundamental right to **privacy** and requires that effective measures be taken by states to ensure that "*information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive,*

[8]Key instruments include: article 10 European *Convention for the Protection of Human Rights and Fundamental Freedoms* (see ECtHR *Ahmet Yıldırım v. Turkey*); article 19 UN *International Covenant on Civil and Political Rights* (ICCPR); UN CCPR General Comment No. 34,; *Joint Declaration on Freedom of Expression and the Internet*, 2011, [Geneva / Vienna / Washington / Banjul]: UN Special Rapporteur on Freedom of Opinion and Expression / OSCE Representative on Freedom of the Media / OAS Special Rapporteur on Freedom of Expression /ACHPR Special Rapporteur on Freedom of Expression and Access to Information; *Declaration of Principles on Freedom of Expression in Africa*, October / November 2019, ACHPR; *American Declaration of the Rights and Duties of Man*, 1948, Bogotá: Ninth International Conference of American States. Clear references to freedom of expression were also made in recent recommendations of the Council of Europe regarding new technologies: Recommendation (2016)5 on Internet freedom; Recommendation (018)2 on the roles and responsibilities of internet intermediaries.

[9] CCPR General Comment No. 25 to Article 25, paragraph 19: "*Voters should be able to form opinions independently, free of […] manipulative interference of any kind."*

[10] As established by Article 20 of the ICCPR.

[11] Relevant reference instruments include UN CCPR General Comment No. *25*, 1996; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, 2 July, 2014, A/HRC/26/30, [New York], UN General Assembly; *Securing free and fair European elections*, Communication from the European Commission, 12 September 2018, [Brussels]: European Commission.

[12] Cf. the Joint Guidelines on Political Party Regulation by the Venice Commission and OSCE/ODIHR, Chapter XII.

process and use it"[13] Some countries or regional entities, such as the EU[14], have developed regulations on the collection and processing of citizens' personal information with a view to protecting their personal data in the digital environment. The use of private data in targeted online campaigns raises critical issues including the means of acquisition and processing of such data, the security of such data, the range of actors exploiting citizens' data in a concealed and unaccountable manner, as well as users' awareness of being subject to online targeting.

16. A cross-cutting aspect of human rights is **freedom from violence and discrimination**. In the context of online campaigns, suppression tactics, discriminatory language, hate speech and incitement to violence against specific communities and groups, like women, may promote intolerance and exclude these groups from the online and offline debate thereby hindering their political participation.[15] Candidates who become targets of this kind of speech – often women – may be pushed out of the electoral race. There are also increasing concerns related to technology companies' "unintentional bias" and the broader area of automated decision-making, which can result in discrimination against specific social, ethnic, gender or religious groups.[16]

17. Several international human rights instruments recognise the **right to an effective remedy** for human rights violations.[17] Therefore, statutory provisions and voluntary compliance measures for content moderation and removal adopted by governments and social media companies should ensure that legitimate, accessible, predictable, equitable, transparent, rights-compatible complaint mechanisms are available to users whose accounts have been suspended or content removed as well as targets of online discrimination, suppression tactics and hate speech. In addition, election management bodies (EMBs) or other institutions – law enforcement agencies, courts, electoral tribunals and regulatory bodies – should ensure effective remedies are available to address violations of citizens' rights online.

18. The UN Guiding **Principles on Business and Human Rights** stipulate that *a global standard of conduct for all business enterprises should be expected wherever they operate*. These principles make clear that business should respect human rights and set out what steps technology companies must take to ensure compliance.[18]

Scope of observation and methodological framework

[13] See paragraph 10 UN CCPR General Comment No. 16 and UN General Assembly Resolution 68/167, affirming that the rights held by people offline must also be protected online, and they called upon all states to respect and protect the right to privacy in digital communication. Other relevant international instruments include article 8 European *Convention for the Protection of Human Rights and Fundamental Freedoms*; *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, No. 108, Strasbourg: Council of Europe; article 1 *American Convention on Human Rights*; article 18 *Cairo Declaration on Human Rights in Islam*, August 1990, [Cairo]: Organization of the Islamic Conference; articles 16 and 21 *Arab Charter on Human Rights (ACHR)*, September 1994, [Cairo]: League of Arab States; *Declaration of Principles on Freedom of Expression in Africa*, October / November 2019, ACHPR.

[14] Article 17 UN *International Covenant on Civil and Political Rights* (ICCPR);EU General Data Protection Regulation (GDPR), 2016; The Economic Community of West African States (ECOWAS), 2010; Asian Pacific Economic Cooperation (APEC), 2015; The African Union Convention on Cyber Security and Personal Data Protection (2014); Association of Southeast Asian Nations (ASEAN), 2016.

[15] Article 20, ICCPR.

[16] For instance, search engines systematically down-ranking results related to a certain group or associating crimes largely with a given community. More generally, algorithms can reflect bias and lead to discrimination, although unintentionally, for example because the data used to train the algorithm mirrored existing human prejudices.

[17] See Article 2.3 ICCPR; Article 13 ECHR paragraph 5.10 of the 1990 OSCE Copenhagen Document.

[18] UN Guiding Principles on Business and Human Rights, "*business, offline and online, are obliged to take proactive measures to mitigate adverse human rights impacts that result from their business practice in accordance with Principle 13.*" https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Organisations conducting international election observation may focus their assessments on the following, often linked, aspects:

19. **General legislative and regulatory framework for freedom of the internet and digital rights**. This includes assessing whether the cyberspace in a given country is free from arbitrary or illegitimate restrictions, to what extent people can access the web without impediments, receive and impart information without undue limitations, as well as whether states take appropriate steps to protect users and to bolster digital safety while ensuring they do not unduly affect other human rights.[19] States, social media platforms and other interested stakeholders should consider working collaboratively to support an independent, diverse digital environment, conducive to a pluralistic, genuine and free online campaign.

20. **Responsibilities of EMBs and other state institutions**. In particular, assessment may focus on how some national institutions administering elections have attempted to respond to key digital threats, often in coordination and consultation with social media platforms and/or civil society organisations (CSOs). These efforts, which may include the development of codes of conduct, agreements with technology companies and social media monitoring activities, are relatively recent and it may be premature to produce general conclusions on their effectiveness and appropriateness. Nonetheless, it is crucial to observe whether these measures are in place and whether they have been effective in some host countries.

21. **Technology companies' responsibilities**. This area includes assessing the role played, according to the emerging normative trends at international level, by technology companies in addressing the risks for citizens of being manipulated during election campaigns and enhancing their accountability mechanisms. Such companies should put in place a number of measures ensuring transparency in relation to the rules that govern content and dissemination, including on data access and use by third parties. These include the release of regular reports on content curation and moderation, accounts suspended, other violations of community standards, coordinated inauthentic behaviour and information manipulation, as well as the promotion of the use of safety and verification tools for political advertising. Other good practices applied so far comprise the development of cooperation mechanisms with fact-checking initiatives and allowing researchers privacy-compliant access to data. These measures are intended to keep the public informed on steps taken to counter threats to election integrity. [20] Online platforms and technology companies should always abide by the highest standards of operation in relation to electoral processes regardless of where the elections take place. Furthermore, the efforts of platforms should be aligned with those of other actors like state institutions, civil society and academia, by working towards a common understanding on the tactics, techniques and procedures (TTPs) of information manipulation and interference and sharing data in a more standardised and transparent way.

22. **Privacy and personal data protection.**[21] The opaque acquisition, sharing and exploitation of individuals' personal data has become a central issue of concern in relation to the integrity

[19]Since 2010, three groups of governmental experts (GCEs) have been tasked by the UN General Assembly to research and report on existing and potential threats to cybersecurity and provide recommendations on how to address them. These groups emphasised that "*State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments*." UN GGE 2013 report. In 2019, the UN adopted a new resolution on cybersecurity reiterating the same principle (UN General Assembly, 12 December 2019, 74/29: *Developments in the field of information and telecommunications in the context of international security*). Also, see the CoE *Convention on Cybercrime (Budapest Convention)*, No. 185, November 2001, Budapest: Council of Europe.

[20] CoE *Recommendation (2018)2 on the roles and responsibilities of internet intermediaries*.

[21] On the relevant international instruments in the field, see above footnote 15. This principle is largely based on the framework developed by Privacy International in the context of their project *Defending democracy and dissent* (https://privacyinternational.org/landing-page/2834/defending-democracy-and-

of electoral processes.[22] Assessment may take into account data protection measures in place to guarantee respect for voters' privacy rights, as well as transparency of the election campaign. Micro-targeting may have positive aspects, for instance by allowing lesser-resourced candidates and parties to level the playing field to compete with larger ones or by allowing traditionally less engaged groups to be reached. However, this practice raises issues in relation to the lawfulness of data acquisition as well as users' vulnerability to sponsored content and the lack of transparency on why a voter is targeted and how their data was acquired. Micro-targeting also has the potential to increase division between different voter groups by creating a more homogenous information space for the targeted users and reducing plurality of information. Micro-targeting would also open opportunities for politicians to target different groups with different messages – and potentially even with conflicting messages regarding their platforms, thus reducing transparency and accountability of political actors.

23. **Political advertising**. A crucial issue during election campaigns is whether online political advertising is adequately regulated - both in terms of content transparency and oversight of campaign finance.[23] Key common features of the various efforts to regulate online political advertising include: adequate labelling of political ads, disclosure requirements to reveal who is behind the advertising, who created it and the amount of money spent; bans on campaign spending by foreign actors; and the development of voluntary transparency measures for major social networks and other internet platforms, such as public ad archives. However, online advertising generally lacks adequate regulation, often falls short on transparency, and may be used to manipulate information to impact public opinion.

24. **Online political campaign behaviour**. Candidates and political parties are increasingly relying on social networks and other digital technologies to reach voters. Online platforms have become powerful channels for candidates and parties to directly communicate with voters and mobilise supporters. The positive role of these new channels is tangible as they allow for greater access to information on alternative and diverse political opinions. However, they can also be used to disseminate deceptive political content and harmful messages.

25. **Information Manipulation**. This has become a central issue of concern with the use of online platforms to intentionally and in a coordinated manner disseminate false and/or misleading information to achieve a certain political and/or economic goal. Information manipulation has the potential to exploit existing societal polarisation, suppress independent and critical voices, generate confusion among voters, discredit fact-based information and undermine candidates, institutions and vulnerable groups. This manipulation can consist of different and integrated tactics, techniques and procedures (TTPs, e.g. coordinated or lone inauthentic actors, click farms, trolls, bots and botnets, cyborgs, other forms of manufactured amplification, etc.). Artificially generated content and dissemination may distort the genuineness of public discourse by creating an impression of widespread grassroots support for or opposition to a policy/issue or individual/group. As noted by NDI: "*Manipulation of voter and civic information dampens participation and degrades trust in election management bodies. Such conditions can destabilize political environments, exacerbate*

dissent?fbclid=IwAR0UWHyLNa0mcWqFFWTWiItmhEc9n1x7q3MSqGk5KAWvCndM4NJh2h7xeQo) and in particular the intervention *Data Exploitation and Democratic Societies*.

[22] This concern is not exclusively related to the online campaign but is also reflected in other aspects of an election, namely voter registration and voting.

[23] It is worth noting the overlap between lack of regulation for online advertising with the larger issues of lack of adequate general regulation for political finance in many countries. Online ads make efforts to oversee online campaign contributions and spending even more challenging.

potentials for electoral-related violence, pervert the will of voters, entrench authoritarians, and undermine confidence in democratic systems more broadly."[24]

26. **Hate/inciteful speech.[25]** The visibility and reach of hateful and violent content, sometimes associated with information disorder, have increased. The **UN Strategy and Plan of Action on Hate speech (2019)[26]** defines hate speech as ***"****Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is often rooted in, and generates, intolerance and hatred, and in certain contexts can be demeaning and divisive."* The Council of Europe[27] states that hate speech can be "*often part of a systematic attempt to suppress certain opinions or political dissent [and] may intimidate people to withdraw* from *social media discourse or to avoid certain subjects and opinions. It may also spill over beyond online discourse. For example, it may intimidate citizens not to attend rallies or going to vote.*"

Sources of information and data-gathering

27. IEOMs will have to apply different and complementary approaches to gather information on the online campaign. Ideally, the assessment should include three main pillars: an analysis of the legal framework related to digital rights and online campaign environment; an analysis of the digital context for the campaign, including the relevance of online platforms for electioneering purposes; and when possible, the direct observation of the online campaigns through regular tracking of relevant accounts of key electoral stakeholders.

28. The analysis of the legal framework may include the assessment of regulatory and policy initiatives for the online campaign, campaign finance regulation and the broader internet governance framework *vis-à-vis* international principles for democratic elections.

29. The analysis of the digital context should include an assessment of the digital environment, through meetings and exchanges with relevant stakeholders, including EMBs, other relevant regulatory authorities, election contestants, fact checkers, media experts, women organizations, civil society organisations active in the field of digital rights and possibly tech companies. It should provide an overview and, when possible, an assessment of the social media ecosystem and digital communication in the host country, digital literacy and the use of online platforms and other online resources by electoral stakeholders.

30. If possible, IEOMs should try to follow the social media accounts, websites and blogs of candidates and political parties, EMBs and other relevant institutions as well as executive-level public officials. Some IEOMs may also monitor other sectors or topics, for example online harassment against women, to provide a wider view of online discourses. While the online mass media responds to a different set of obligations and responsibilities, it may be relevant to observe their role in the ecosystem. Key elements to be observed include: episodes of information manipulation and interference, hate speech, efforts to suppress voter participation, lack of transparency and misuse of administrative resources and wider actions

[24] *Disinformation and Electoral Integrity A Guidance Document for NDI Elections Programs*, 2019, Washington DC: National Democratic Institute.
[25] Article 19 *International Covenant on Civil and Political Rights*, 1966 (freedom of opinion and expression); Article 20 *ICCPR,* 1966 ; Article 4 *International Convention on the Elimination of Racial Discrimination*, 1965; Council of Europe Committee of Ministers on "Hate Speech," *Recommendation No. R (97)20* of the 30 October 1997.
[26] https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf
[27] Council of Europe Recommendation No. R (97) 20 https://rm.coe.int/1680505d5b

such as black-outs, blocking or other forms of content or behaviour moderation. Positive practices should also be assessed, including those that enhance transparency, voter awareness and mobilisation, offer nonpartisan assessment, facilitate a pluralistic debate and strengthen the overall integrity of the election. It should be noted that full fact-checking is outside an IEOM's scope and credible local organisations are likely to be a valuable source of information for missions.

Formulation of recommendations

31. According to the DoP Guiding Principles and Coordinated Approaches for Follow-Up on International Election Observation Mission Recommendations: "*in order for IEOM* recommendations *to produce the desired effect of contributing to improved electoral processes, IEOM recommendations should be clear, concise and realistic in light of national circumstances and be in accord with relevant international obligations, commitments, principles and best practices for democratic elections*".[28] In this regard, IEOMs should ensure that recommendations for online campaigns duly reflect existing standards and carefully balance the need to protect freedom of expression with the need to promote electoral integrity.

32. While recommendations related to certain issues can be clearly formulated and linked with international principles for democratic elections and human rights standards (i.e., access to the internet, respect of privacy and data protection, transparency of advertising, campaign finance regulations for online campaign ads, responsibility of internet intermediaries), standards for other areas related to online campaigning are still under elaboration (i.e., information manipulation). Recommendations should not be overly prescriptive and IEOMs should be careful when proposing content regulation as it may be used to legitimise online censorship. Recommendations should reflect current trends informing attempts to regulate online campaigning as well as reinforcing existing efforts supported by credible domestic civil society organisations.

33. Key lines of recommendations that could be addressed to electoral stakeholders may include:[29]
    - Enhance the legal framework pertaining to data protection and privacy.
    - Strengthen the legal framework for electoral advertising and its transparency.
    - Promote universal internet access and protection of net-neutrality.
    - Promote regulatory frameworks in accordance with international standards for liability regimes and content moderation with a focus on accountability and transparency.
    - Protect users from online harassment through introduction of appropriate sanctions, including for gender-based political violence.
    - Ensure that cybercrimes are criminalised and prosecuted.
    - Support the development of cooperation agreements and transparency between national authorities (*inter alia* EMBs, data protection and campaign finance

[28] *Guiding Principles and Coordinated Approaches for Follow-Up on Election Observation Mission Recommendations*, 2010, Atlanta: 5th Meeting on the implementation of the Declaration of principles for International Election Observation.
[29] Based on: *Joint Declaration on Freedom of Expression and Elections in the Digital Age*, April 2020, [Geneva / Vienna / Washington]: UN Special Rapporteur on Freedom of Opinion and Expression / OSCE Representative on Freedom of the Media / OAS Special Rapporteur on Freedom of Expression; OAS *Guide to guarantee freedom of expression regarding deliberate disinformation in electoral process*, October 2019, [Washington]: OAS / Inter-American Commission on Human Rights; Pamment, James, EU *Code of Practice on Disinformation: Briefing Note for the New EU Commission*, March 2020, Washington DC: Carnegie Endowment for International Peace; *Protecting electoral integrity in the digital age*, January 2020, [Geneva]: Kofi Annan Foundation; Venice Commission *Joint Report on Digital Technologies and Elections*, June 2019, Venice: Venice Commission / Directorate of information society and action against crime – Council of Europe.

authorities, media regulatory bodies) and technology companies to address threats to the integrity of electoral processes.

- Encourage election stakeholders to increase access to public information and develop awareness-raising, public education, digital literacy and training initiatives against information manipulation.
- Support the creation of fact-checking initiatives and citizen monitoring around digital threats.
- Protect the legitimate use of data gathering tools.
- Support quality journalism and independent traditional and online mass media.
- Elaborate codes of conduct for political parties and election contestants.

Ethical aspects of social media observation

34. The direct observation of online platforms poses a number of ethical issues related to consent, anonymity and privacy-invasive technologies. According to the DoP, "*International election observation missions* must *[…] act in a manner that is consistent with respecting and promoting human rights and fundamental freedoms of the people of the country*."

35. In this regard, IEOMs should consider abiding by a set of principles to ensure that this area of observation complies with data protection and privacy. In particular:
    - IEOMs should follow public accounts/posts only and the data gathered must be carefully secured against leaks or misappropriation. Software and methods used to follow online campaigns should respect ethical and privacy benchmarks when collecting data.
    - In many countries direct messaging channels are widely used to spread information, both true and false, manipulated or not. However, any attempts to access private conversations and these groups are not within the mandate of IEOMs and go against legal and ethical issues related to data protection and privacy rules.
    - IEOM members should refrain from creating or using anonymous accounts for social media observation purposes.
    - IEOMs generally should anonymize data; exceptions should be carefully considered and narrowly applied (for example in relation to political figures). The 'do no harm' principle should be applied, especially in potentially repressive contexts.

Cooperation among DoP partners

36. International election observer groups have varying capacities to monitor the various aspects of online campaigning. Therefore, key aspects to observe differ depending on the priorities of each observation group. Co-operation among DoP partners is important in coordinating online campaign monitoring efforts and improving the collective efficiency and effectiveness. The observation of online campaigns is a new field for IEOMs, and they can benefit from regular and coordinated exchanges of information, approaches and practices both on the field and off the field.

37. Actions that could be adopted in the field may include: information-sharing, exchanging key observation findings and meetings with relevant interlocutors. This cooperation should not compromise the independence of each IEOM.

38. Interested DoP partners may also carry out regular meetings to discuss key developments and trends in online campaign regulations and related methodological updates.

39. DoP partners may also consider engaging with and strengthening their interaction with national networks/organisations that specialise in monitoring online platforms or fact-checking.[30]

Conclusions

40. Like other aspects of international election observation, the assessment of online campaigns requires a solid methodology defining the scope of observation and analytical approach required to ensure accuracy, as well as clear benchmarks for drawing conclusions and recommendations. In order to ensure a consistent approach, it is important that IEOMs be transparent about their scope, methodology and what they can realistically achieve. The observation of certain phenomena may prove difficult (for example in relation to sources of online campaign funding, instances of informational manipulation and interference, including from foreign actors) and findings for other aspects of the online campaign may not be generalisable.

41. Finally, this area of observation is relatively recent and several organisations engaged in election observation are trying to identify how best to address the many challenges it poses. Several members of the DoP have already started developing methodological frameworks to define the scope of observation, the analytical approach, the selection of tools to support possible social media observation activities, as well as clear benchmarks for drawing conclusions and recommendations.

42. For this reason, it is important to attract broad participation from the international election observation community. By fostering their ability to address emerging concerns and identify effective and rights-based recommendations, DoP partners, through discussion and consultation, can help ensure consistency in the approach to this area of electoral observation.

[30] See GNDEM communiqué on collaboration between IEOMs and citizen EOMs.

Annex 1 – International and Regional Standards and Commitments

International Instruments:

International Covenant on Civil and Political Rights (ICCPR), articles 9 and 19:

- **Article 9:** "1. Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law."
- **Article 19:** "2. 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. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order, or of public health or morals."

ICCPR, CCPR, General Comment 34, paragraphs 42 and 43:

- **Para 43:** "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."
- **Para 42:** "The penalization of a media outlet, publishers or journalist solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression."

The Joint Declaration[31] **on Freedom of expression and the Internet, 2011, paragraphs 1(a) and 3(a):**

- **Para 1 (a):** "Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law."
- **Para 3 (a):** Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards."

Joint Declarations related to freedom of expression online:

- **Joint Declaration on Freedom of Expression and Elections in the Digital Age**, 30 April 2020.
- **Challenges to Freedom of Expression in the Next Decade**, 10 July 2019.
- **Joint declaration on freedom of expression and "fake news", disinformation and propaganda**, 3 March 2017.

[31] *Joint Declaration on Freedom of Expression and the Internet*, 2011, [Geneva / Vienna / Washington / Banjul]: UN Special Rapporteur on Freedom of Opinion and Expression / OSCE Representative on Freedom of the Media / OAS Special Rapporteur on Freedom of Expression /ACHPR Special Rapporteur on Freedom of Expression and Access to Information

- **Joint declaration on media independence and diversity in the digital age**, 3 May 2018.
- **Joint Declaration on Freedom of Expression and Countering Violent Extremism**, 3 May 2016.

UN HRC Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/26/30), paragraphs 10-17 (Freedom of expression and communication in electoral processes), 2 July 2014.

UN HRC Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/38/35) 6 April 2018 (*the report focuses on online content regulations*).

1. Right to political participation

ICCPR, CCPR, General Comment 25, paragraph 19: "Voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind."

ICCPR, CCPR, General Comment 25, paragraphs 8, 12 and 25:

- **Para 8:** "Citizens also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves."
- **Para.12:** "Freedom of expression, assembly and association are essential conditions for the effective exercise of the right to vote and must be fully protected."
- **Para 25:** "In order to ensure the full enjoyment of rights protected by article 25, the free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion."

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/74/486), 9 October 2019 (*the entire report is dedicated to issues related to online "hate speech" and respective regulation in international human rights law*).

2. Right to privacy and data protection

ICCPR, article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

ICCPR, CCPR, General Comment 16, paragraph 10: "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and us it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and it so, what personal data is stored in automatic data files and for what purpose."

UN General Assembly Resolution 68/167 "affirms that the same rights that people have offline must also be protected online, including the right to privacy", 18 December 2013.
CCPR's 2011 Guiding Principles on Business and Human Rights.

3. Right to access to information

Access to internet

ICCPR, CCPR, General Comment 34, paragraph 15: "States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."

The Joint Declaration on Freedom of expression and the Internet, 2011, paragraphs 6(a), (b) and (e), and 1(f):

- **Para 6 (a):** "Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections."
- **Para 6 (b):** "Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet."
- **Para 6 (e):** "States are under a positive obligation to facilitate universal access to the Internet. At a minimum, States should:
  a. Put in place regulatory mechanisms – which could include pricing regimes, universal service requirements and licensing agreements – that foster greater access to the Internet, including for the poor and in 'last mile' rural areas.
  b. Provide direct support to facilitate access, including by establishing community-based ICT centres and other public access points.
  c. Promote adequate awareness about both how to use the Internet and the benefits it can bring, especially among the poor, children and the elderly, and isolated rural populations.
  d. Put in place special measures to ensure equitable access to the Internet for the disabled and for disadvantaged persons."
- **Para 1 (f):** "Awareness raising and educational efforts to promote the ability of everyone to engage in autonomous, self-driven and responsible use of the Internet should be fostered."

UN HRC Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paragraphs 19 – 66 (General principles on the right to freedom of opinion and expression and the internet; Restriction of content on the internet; Access to the Internet and the necessary infrastructure), 16 May, 2011

Access to information (published online)

ICCPR, CCPR, General Comment 25, paragraph 11: "Voter education and registration campaigns are necessary to ensure the effective exercise of article 25 rights by an informed community."

ICCPR, CCPR, General Comment 34, paragraph 19: "To give effect to the right of access to information, States parties should proactively put in the public domain Government information of public interest. States parties should make every effort to ensure easy, prompt, effective and practical

access to such information. States parties should also enact the necessary procedures, whereby one may gain access to information, such as by means of freedom of information legislation."

Joint declaration on media independence and diversity in the digital age, **2018, paragraph 1 (a):** "States are under a positive obligation to create a general enabling environment for seeking, receiving and imparting information and ideas (freedom of expression), including through the following measures:

i. ensuring that legislation on the right to access information held by public authorities is in place and being implemented;
ii. promoting universal access to the Internet;
iii. providing appropriate protection for privacy and personal data, including through enabling the anonymous use of digital technologies;
iv. ensuring that legislation providing protection to whistle-blowers is in place and being implemented."

4. Transparency (primarily in relation to campaign finance regulations)

UN Convention Against Corruption (UNCAC), articles 10, 7(3) and 7 (4):

- **Article 7(3):** "Each State Party shall also consider taking appropriate legislative and administrative measures, consistent with the objectives of this Convention and in accordance with the fundamental principles of its domestic law, to enhance transparency in the funding of candidatures for elected public office and, where applicable, the funding of political parties."
- **Article 7(4):** "4. Each State Party shall, in accordance with the fundamental principles of its domestic law, endeavour to adopt, maintain and strengthen systems that promote transparency and prevent conflicts of interest."
- **Article 10:** "Taking into account the need to combat corruption, each State Party shall, in accordance with the fundamental principles of its domestic law, take such measures as may be necessary to enhance transparency in its public administration, including with regard to its organization, functioning and decision- making processes, where appropriate."

ICCPR, CCPR, General Comment 25, paragraph 19: "Reasonable limitations on campaign expenditure may be justified where this is necessary to ensure that the free choice of voters is not undermined, or the democratic process distorted by the disproportionate expenditure on behalf of any candidate or party."

ICCPR, CCPR, General Comment 34, paragraph 41: "Care must be taken to ensure that systems of government subsidy to media outlets and the placing of government advertisements are not employed to the effect of impeding freedom of expression."

5. Equality and freedom from discrimination

ICCPR, articles 20 and 26:

- **Article 20:** "2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."
- **Article 26:** "All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

ICCPR, CCPR, General Comment 25, paragraph 12: "Information and materials about voting should be available in minority languages."

The Joint Declaration on Freedom of expression and the Internet, 2011, paragraphs 5(a): "There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."

6. Right to effective remedy

ICCPR, article 2: "3. Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy."

7. Equality and freedom from discrimination

ICCPR, articles 20 and 26:

- **Article 20:** "2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."
- **Article 26:** "All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

ICCPR, CCPR, General Comment 25, paragraph 12: "Information and materials about voting should be available in minority languages."

The Joint Declaration on Freedom of expression and the Internet, 2011, paragraphs 5(a): "There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."

8. Regional instruments

The American Convention on Human Rights, articles 1, 11, 13, 14, 16, 24 and 25

The Inter-American Democratic Charter, Article 4.

Standards for free, open and inclusive internet, Inter-American Commission for Human Rights, March 2017.

Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, Organization for Security and Cooperation in Europe (1990 OSCE Copenhagen Document).

Convention on Cyber Security and Personal Data, African Union, June 2014.

Declaration of Principles on Freedom of Expression in Africa ACHPR

The Council of Europe Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The Council of Europe Convention on Cybercrime (Budapest Convention).

European Convention for the Protection of Human Rights and Fundamental Freedoms in particular Articles 8, 10, 13 and Article 3 of the First Additional Protocol**.**

Recommendation CM/Rec (2018)2 of the CoE on the roles and responsibilities of internet intermediaries.

Recommendation CM/Rec (2018)1 of the CoE on media pluralism and transparency of media ownership.

Recommendation CM/Rec (2016)5 of the CoE on Internet freedom.

Recommendation CM/Rec (2007)15 of the CoE on measures concerning media coverage of electoral campaigns.

Recommendation Rec (2003)4 of the CoE on common rules against corruption in the funding of political parties and electoral campaigns.

Recommendation No.R (97) 20 of the CoE on "Hate Speech".