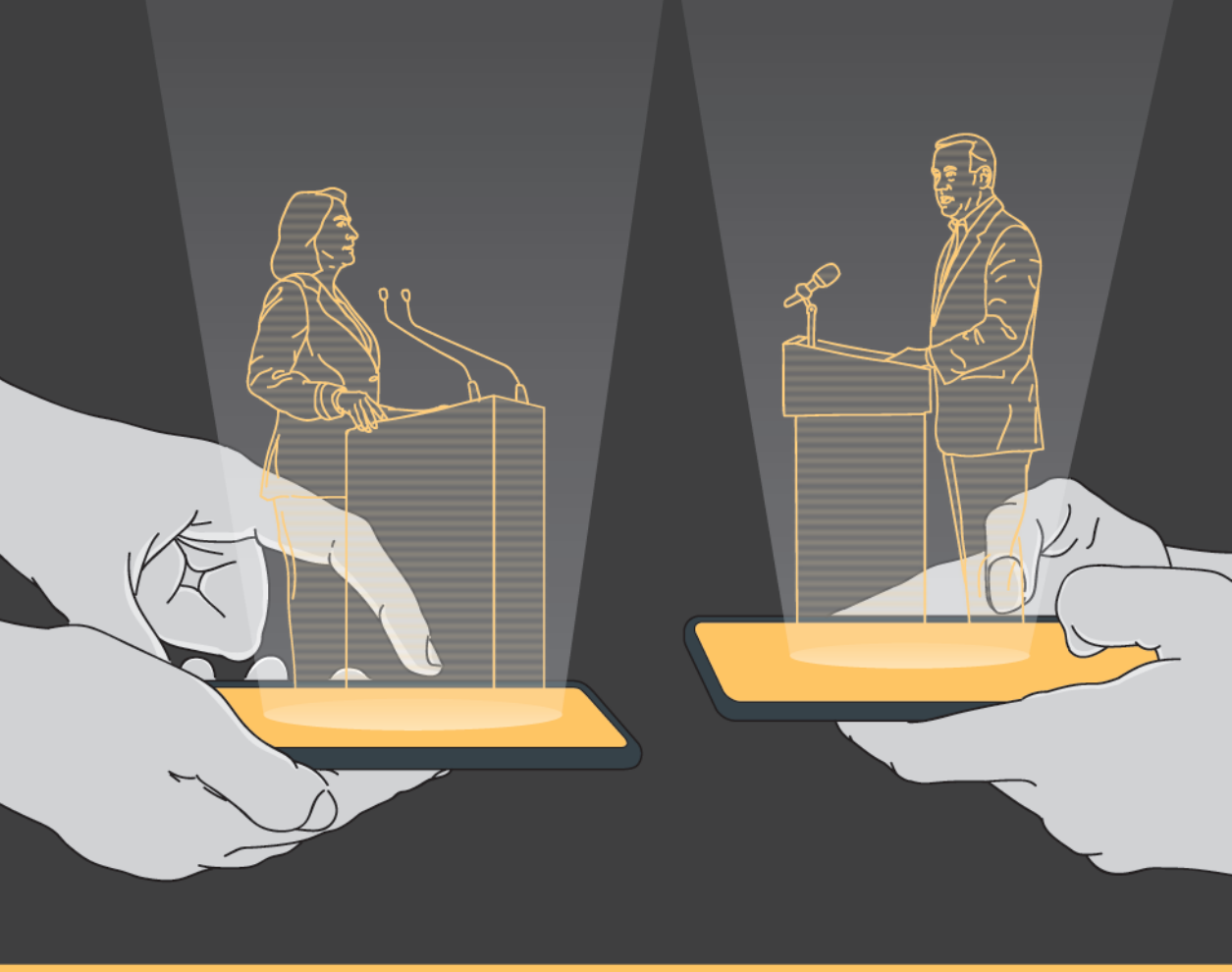


Guidelines for Observation of Election Campaigns on Social Networks

OSCE
ODIHR

Guidelines for Observation of Election Campaigns on Social Networks

30 YEARS OSCE ODIHR

Published by the OSCE Office for Democratic Institutions
and Human Rights (ODIHR)
Ul. Miodowa 10
00-251 Warsaw
Poland

www.osce.org/odihr

© OSCE/ODIHR 2021

All rights reserved. The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction is accompanied by an acknowledgement of the OSCE/ODIHR as the source.

ISBN 978-83-66690-38-7

Designed by Dejan Kuzmanovski

Cover, Chapter 2, Chapter 3, Chapter 4, Chapter 5, Chapter 6, Chapter 7:
OSCE/Dejan Kuzmanovski

Contents

Foreword 5

1. Introduction 7

1.1. The Purpose of the Guidelines 8

1.2. Social Networks and Media 10

2. OSCE Commitments and Other International Obligations, Standards and Principles 14

3. General Features of Election Campaigns on Social Networks 20

3.1 Content and Activity 21

a. Incitement to Hatred, Hostility or Violence 23

b. Intolerant, Aggressive and Negative Rhetoric 26

c. Manipulative Information 27

d. Tackling Manipulative Information 28

3.2 Political and Campaign Advertising 36

a. Responses to Online Advertising 37

3.3 Data Privacy Protection 40

4. ODIHR Approach in Observation and Assessment of Election Campaigning on Social Networks 44

4.1 The Needs Assessment Mission 45

4.2 The Observation Mission 45

4.3 Developing Recommendations 47

5. The Role of the Political Analyst in the Observation and Assessment of Election Campaigning on Social Networks 50

5.1 Assessment of the Legal Framework 52

a. Online Content 52

b. Political and Campaign Advertising 53

c. Data Privacy Protection 54

5.2 Observation and Assessment of Campaign Activities 56

a. Selection of Platforms 58

b. Selection of Accounts 58

c. Collecting Information 61

5.3 Observation and Assessment of Political and Campaign Advertising 63

a. Transparency of Advertising 63
b. Reporting Requirements 64
c. Third-Party Campaigning 65

6. Oversight 68

6.1 Content Oversight 69

6.2 Political and Campaign Advertising Oversight 70

6.3. Data Privacy Protection Oversight 72

7. Challenges and Opportunities for Quantitative Assessment 74

7.1 Methodological Limitations 74

7.2 Data From External Sources 77

A. Web-Listening and Data Scraping Tools 78

B. Big-Tech Companies Access to Data 79

C. Fact-Checkers 80

Annex I – Relevant International Documents 83

Annex II – Glossary of Relevant Terms 88

Foreword

The Internet has facilitated immense public access to information, including during election periods, and provided tools for broad political debate and participation. With the emergence of online social networking sites, election campaigns have entered into a new era of communication. Political discourse has moved away from a one-sided transmission of information toward a multilateral interactive system, in which voters have wider channels to express their opinions. The debate around the impact social networks have on voters and election processes has attracted unprecedented public attention recently. Before getting into the particularities of this debate, it is important to understand that digital campaigning is just another method used by electoral contestants and other election stakeholders to attract support or to communicate with voters. As such, it should be subject to internationally recognized standards and principles for free and fair campaigning.

Social networking sites provide space for voters to enhance their direct participation in campaigns while enabling electoral contestants to better mobilize support. At the same time, the use of social networks, especially during election campaigns, carries a wide array of challenges. Some of these pose threats to the exercise and protection of fundamental freedoms and human rights, as well as the overall integrity of the election process.

Online communication technologies are constantly evolving, the landscape and popularity of different social network platforms shift regularly, within increasingly rigid regulatory environments. The big-tech companies, as owners of social networks, have started to institute changes in the way they operate and deal with online content. Many of these initiatives can potentially bring positive developments, such as increased transparency, prevention of the misuse of private data or protection of particular rights or categories of users from harassment, but often, they may also challenge access to and application of fundamental freedoms. In this context, one of the most worrying developments is the platforms' acquiescence to pressure from some governments to remove legitimate content or user accounts critical of the establishment, often without the possibility of redress. Where the big-tech companies have stood up to defend free speech, they have sometimes come under growing regulatory pressure, including threats of losing market access.

The Organization for Security and Co-operation in Europe (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) has developed a systematic and comprehensive methodology for election observation and assessment of election processes. While the assessment of an election campaign is already a central part of ODIHR's general election observation methodology, these Guidelines aim to deal specifically with campaign conduct on social networks. They provide guidance for ODIHR observers and are a useful tool for other international and citizen observer organizations on important principles and international good practice related to this topic. The Guidelines can also assist the OSCE participating States in their efforts to adequately address the challenges steaming from online campaign activities during the electoral process.[1]

Matteo Mecacci
ODIHR Director

1 ODIHR is committed to regularly reviewing and refining its election observation methodology, in line with relevant taskings by the OSCE participating States (Ministerial Council Decision 19/06).

1. INTRODUCTION

Social networks enable individuals and groups to express their opinions, engage in dialogue and directly communicate with political actors and institutions, as well as becoming active participants in election campaigns.[2] Globally, the use of social networks has further strengthened critical engagement of the electorate and enhanced the emergence and organization of large-scale groups and social movements. Social networks have become instrumental in the advancement in expression and exercise of fundamental freedoms by transforming voters from passive recipients of information to active participants and co-shapers of public debate. Social networks have significantly altered political campaigning, be it with respect to their use by contestants as platforms to present and discuss their policies with the electorate, political advertising tools, or the collection and processing of voters' personal data.

On the other hand, the use of social networks in elections and politics more widely can pose a wide array of challenges and threats. Some of these include the proliferation of manipulative content; states' attempts to restrict access to certain fundamental freedoms online; undue criminalization of content and activities; arbitrary blocking or shutting down of access to networks; and selective presentation, deletion or concealment of content that may effectively lock specific groups of voters into narrow information silos or so-called 'echo chambers.' Other types of challenges are related to the misuse of personal data for advertising and electioneering, foreign interference in elections and political discourse, and the growing use of bots and trolls to set public agendas and shape voters' opinions, as well as mobilize or suppress voter turnout. Such practices, be those promoted by states, big-tech companies, different interest groups or individuals, are detrimental to the democratic electoral process and can diminish public confidence in elections.[3]

Having recognized the dangers posed by some of these challenges and, in particular, the growth of different types of manipulative content, big-tech companies have stepped up their efforts to curb the spread of so called 'disinformation,' and other malpractices that may foster an environment that is not conducive to the conduct of democratic elections. Joint codes for tackling these types of content have been developed, in co-operation with governments or international organizations, in which big-tech companies agreed to flag or remove significant issues of trustworthiness in content, transparency of advertising and data protection. Some of the codes foresee deletion of illegal content or advertisements, and in some countries, users should be informed when they are subject to (micro)targeting.

2 The Guidelines refer uses the term "social networks" as internet platforms that provide for multi-directional interaction through users-generated content. The definition is similar to those used in the 2019 Joint Report of the European Commission for Democracy through Law of Council of Europe (Venice Commission) and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Election; and International IDEA Guidelines for the Development of a Social Media Code of Conduct for Elections.

3 Other main concerns relate to social networks' *decentralized or transnational* nature and resulting limitations on applicability and efficacy of legal and judicial actions and the possibility for effective remedy.

1.1 The Purpose of the Guidelines

These developments, both positive and negative, have given rise to number of questions about the respect for fundamental human rights in the online sphere. While some OSCE participating States have attempted to regulate aspects of the Internet nationally, the practice has shown that meaningful, comprehensive and the most effective responses are those pursued multilaterally through actions that recognize the transboundary nature of social networks. In this respect, the United Nations (UN), the OSCE and other regional organizations, such as the Council of Europe, or the European Union, have introduced initiatives to re-affirm that the protection of human rights and fundamental freedoms should apply as much to the online as to the real world. Thus, access to the Internet and the use of social networks during elections has become a key topic of interest in the context of international and citizen election observation.

While online campaigning is on the raise globally and includes a range of activities and methods, some of which often are used beyond official campaign periods, and which will continue evolving, it is outside of the scope of these Guidelines to cover all of these aspects of online activity in elections. Also, the Guidelines do not attempt to provide a definition, distinction or assessment of different types of manipulative content (dis-, mal-, or misinformation) and do not provide guidance about whether social networks should be held liable for content. In this context it is particularly important to note that there is no one-size-fit-all approach and the OSCE participating states have sovereign rights in regulating the functioning of social platforms and online conduct of their election campaigns, in line with the internationally agreed obligations, standards and principles and their political commitments.

The aim of the Guidelines is to provide a framework, mainly for election observers, to adequately assess the impact of the key aspects of online campaigning on the overall integrity of the election process and election campaign. These aspects include the online activities of electoral contestants, dissemination of specific types of content relevant to the election process, political and campaign advertising, and the protection of private data. The Guidelines have been developed with extra-budgetary support as part of ODIHR's efforts to continually improve its methodology and to increase its capacity to observe certain specialized aspects of elections.

In line with the ODIHR election observation methodology, any assessment of the regulatory framework and practice related to campaigning, including on social networks, should be made on the basis of recognized obligations, standards and principles enshrined in relevant international documents.[4] An assessment should take into consideration the legal framework pertaining to online campaigning, which may be constantly and rapidly changing and expanding. Consequently, any effort to observe and assess

4 Among others, these include the 1948 Universal Declaration of Human Rights (UDHR); the 1966 UN International Covenant on Civil and Political Rights (ICCPR); the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the 1990 OSCE Copenhagen Document.

online electioneering is bound to have limits and the way international election observers approach this topic will continue to evolve.

It is important for the Political Analyst, who has overall responsibility for assessing the election campaign, including on social networks, to be able to contextualize online developments and draw correlations within the overall campaign environment. Given the variety of issues to be observed online, when assessing the election campaign on social networks, the Political Analyst will need to co-operate with other core-team members. The potential fields of overlap and modes of co-operation are elaborated further below.

The Guidelines are structured in the following manner:

- An introduction to campaigning on social networks, including an outline of the differences and overlaps between social networks and traditional media;
- A review of the OSCE commitments and other international obligations, standards and principles relevant to online election campaigns;
- Description of the general features of campaigning on social networks and key areas of regulation and assessment: online content and activities, political advertising and the protection of data privacy;
- ODIHR's approach in observation and assessment of campaigning on social networks;
- The role of the Political Analyst in the observation and assessment of campaigning on social networks;
- Elaboration of the importance of effective oversight in relation to online content, political advertising and data protection; and
- Presentation of some of the opportunities and key methodological limitations for quantitative monitoring.

The Guidelines elaborate on ODIHR's approach for observation and assessment of election campaigns, exclusively on the role of online social networking sites. ODIHR's methodology for overall observation and assessment of election campaigns, including more traditional forms of campaigning is elaborated in the *Handbook for Observation of Election Campaign and Political Environment,* published together with these Guidelines. The Guidelines deal with social networks as distinctively different entities from the traditional media (television and press), their online versions or the specialized news portals (online media), which are assessed against international media-related obligations, standards and commitments and therefore remain within the remit of the Media Analyst during election observation activities.[5] The elements that distinguish social networks from the traditional media are described in the next section.

5 On ODIHR election methodology, see the Election Observation Handbook (Sixth Edition) and for election campaigns see Handbook for Observation of Election Campaign and Political Environment.

Within the OSCE context, no specialized commitments with regard to social networks have been developed and online campaigns must meet the same standards that apply for the overall conduct of the election campaign. Due to the lack of specific commitments and standards and to better grasp the challenges posed from recent developments in the online world, the Guidelines offer definitions and quotations from numerous reports produced by credible international organizations that are relevant for the OSCE participating states. While the field of social networks most certainly will continue its pace of rapid development and it is highly probable that new platforms will emerge, at the time of writing, in the OSCE area the following social networks are most commonly used during election campaigns: *Facebook, Instagram, Twitter, YouTube, Odnoklasniki* and *Vkontakte*. Messaging tools, such as WhatsApp, Messenger, Telegram or others, can play an important role in dissemination of information, in particular during election periods, however they are not subject of these Guidelines mostly due to their closed nature and lack transparency for observation, as well as other concerns related to respect for privacy and data protection of the groups' members.

1.2 Social networks and media

The question about the nature of social networks – whether they should be understood as media, as the frequently used term 'social media' implies, or something different – remains the subject of public and academic debate. It is obvious that social networks serve as a medium of communication and exchange of information. Moreover, they serve a similar purpose - share information, and strive to achieve a similar aim - to inform the public.[6] However, recently there is a growing consensus that social networks are indeed a distinct entity, a sui generis creation, and that there are many aspects that set them apart from traditional and online media outlets. Some of these include:

- **Content:** In the context of traditional and online media, media organisations and professional journalists are the ones that create most of the content, while the production of content on social networks is dispersed, and it is mostly the consumers that can shape and disseminate it.

- **Editorial policy:** An editorial policy is one of the pillars for the functioning and operation of media. In turn, social networks, with the exception of the algorithmic settings created by big-tech companies, lack clear editorial policy standards and debate centres on the level of responsibility that they should bear for the content produced and shared on their platforms.

6 Because of these overlaps between traditional media and social networks, a number of international standards, obligations, principles and political commitments related to the freedom of expression and access to information are applicable to both. ODIHR methodology for media observation can be found in the Handbook on Media Monitoring for Election Observation Missions, which outlines these international standards, obligations, principles and commitments.

- **Engagement:** Social networks are highly diffused information platforms, where everyone can participate in the conversation in real time. Traditional media is hierarchically established, where information generally flows in one direction - from the outlet to the public at large.

- **Multi-mediality:** Social networks allow for the use of different types of content in one space and at the same time: text, photos or graphics, video and audio. Traditional media are usually narrower in the presentation, although online media can also integrate various modes of communication.

- **Time:** Communication on social networks is instant while traditional media generally operate on pre-set schedules. Online media are more flexible, but they too tend to be bound by pre-existing timeframes, and real-time communication remains the exception, rather than the rule.

- **Cost:** Traditional and online media tend to involve significantly higher costs compared to social networks for content production, including material and human resources that necessitate revenue to allow continued operation.

- **Private Data Collection:** Traditional media often use different techniques for measuring their rating or popularity of programmes, such as opinion polls or metric devices, which at times can collect certain amounts of personal data. One of the key aspects of how social networks function (and other Internet-based platforms and online media) is the constant collection of private data from their users. The type, amount, processing, use and trading of users' private data, in particular for election purposes, has become one of the most controversial issues in the functioning of social networks.

Recognizing the changes in the field of mass communication, the **Council of Europe**, an intergovernmental human rights organization, which includes 47 out of the 57 OSCE participating States as members, developed **six criteria** for States' common understanding of the notion of media and whether to grant social networks specific media-related rights and assign certain responsibilities.[7] The Recommendation notes that, "the extent to which criteria are met will permit to recognize whether a new communication service amounts to media or will provide an indication of the bearing of intermediary or auxiliary activity on media services." The Recommendation further states that, "intermediaries [...] can be distinguished from media as they may meet certain of the criteria [...], but they usually do not meet some of the core criteria such as editorial control or purpose. However, they often play an essential role, which can give them considerable power as regards outreach and control or oversight over content. As a result, [they] can easily assume an active role in mass communication editorial processes. Member states should therefore consider them carefully in media-related policy making and should be particularly attentive to their

7 See Committee of Ministers of the Council of Europe Recommendation CM/Rec(2011)7 on a new notion of media.

own positive and negative obligations stemming from Article 10 of the European Convention on Human Rights."

The criteria (in bold text) which are supplemented by a set of indicators (in brackets) are: (i) **Intent to act as media** (self-labelling as media; working methods typical for media; commitment to professional media standards; practical arrangements for mass communication); (ii) **Purpose and underlying objectives of media** (produce, aggregate or disseminate media content; operate applications or platforms designed to facilitate interactive mass communication - for example social networks; animate and provide a space for public debate and political dialogue; shape and influence public opinion; promote values; facilitate scrutiny and increase transparency and accountability; provide education, entertainment, cultural and artistic expression; create jobs; generate income; periodic renewal and update of content); (iii) **Editorial control** (editorial policy; editorial process; moderation; editorial staff); (iv) **Professional standards** (commitment; compliance procedures; complaints procedures; asserting prerogatives, rights or privileges); (v) **Outreach and dissemination** (actual dissemination; mass-communication in aggregate; resources for outreach); and (vi) **Public expectation** (availability; pluralism and diversity; reliability; respect of professional and ethical standards; accountability and transparency).

2.

OSCE COMMITMENTS and OTHER INTERNATIONAL OBLIGATIONS, STANDARDS and PRINCIPLES

To date, no specialized commitments with regard to the use of Internet and social networks in election processes have been developed by the OSCE participating States. However, over the last decade there has been a concerted effort within different international organizations, including the Council of Europe to develop basic principles and standards for use of technologies in elections. Election campaigning on social networks should respect the same conditions as for traditional campaigning and, therefore, meet

the same obligations, commitments and standards that apply to the other methods of campaign. The OSCE commitments - agreed by OSCE participating States in the 1990 Copenhagen Document, and in subsequent OSCE commitments and Ministerial Decisions - define principles for democratic elections, regardless of the method of campaign used. In general, these principles require that the campaign should be conducted in a free and fair environment, with respect for fundamental freedoms and States should provide the necessary conditions for contestants to compete on equal terms.

When assessing the legislation and practice of campaigning on social networks the following obligations, standards, principles and commitments to which the OSCE participating States have signed in different international documents should be considered:

1. Freedom of expression and the right to hold opinions without interference - a fundamental human right, indivisible from any democratic society and in an election context, provides the right for contestants to express their views and for voters to have access to diverse information and make an informed choice.[8] An essential element of this freedom is the right to hold opinions without interference, which means that all citizens, as well as associations, including political parties, must be free to hold their own views and to communicate them freely.[9] Interpretive sources note that, "voters should be able to form opinions independently, free from violence or the threat of violence, compulsion, inducement or manipulative interference of any kind."[10] At the same time, freedom of expression has some limitations. These include, "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." [11]

i. **Access to Information and Internet** – the right to freedom of expression is closely related to the exercise of other rights, such as access to information.[12] Although it is not yet recognized as a human right under international law, the UN Human Rights Council (HRC) has urged states to promote universal Internet access and recognize

8 The UDHR and the ICCPR guarantee the right to freedom of opinion and expression. Their indispensability for every democratic society has been further reiterated in General Comments No. 25 and 34 issued by the UN Human Rights Committee. Numerous other treaties protect the freedom of expression such as the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD); and the Convention on the Rights of Persons with Disabilities (CRPD).

9 See article 19.1 of the ICCPR. Both the 1990 OSCE Copenhagen Document and the 1995 Commonwealth of Independent States (CIS) Convention on Human Rights and Fundamental Freedoms (CHR) in articles 9.1 and 11(1), respectively, recognize that everyone shall have the right to freedom of expression and that this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by a public authority and regardless of frontiers.

10 See the United Nations (UN) Human Rights Committee General Comment No. 25.

11 As prohibited under the ICCPR. Moreover, other prohibitions can be made to (1) the respect of the rights or reputations of others and (2) to protect national security or of public order, or of public health or morals. In all cases, before imposing any restrictions on fundamental rights, including the freedom of expression, the so-called three-part test of legality, necessity and proportionality should be implemented, meaning that any restriction (1) must be clearly established in the law, with the possibility of redress; (2) it must be clearly justifiable for the above mentioned exceptional circumstances; and (3) it must be proportionate to the interests that it intends to protect.

12 See the UN Human Rights Committee General Comment No 34.

human rights in cyberspace.[13] Access to the Internet as a fundamental right has also been promoted in several OSCE and the UN Joint Declarations on freedom of expression and the Internet.[14] At the national level, some OSCE participating States have recognized Internet access as a fundamental right in their national legislation.[15]

ii. **The Principle of Net-neutrality** – essentially related to the right to access the Internet, it requires that all data traffic is treated equally.[16] Net-neutrality means that Internet users should be able to use any applications or access any services of their choice without traffic being managed, prioritized or discriminated by network operators.[17] Under the net-neutrality principle in the context of elections, Internet service providers should not intentionally block, slow down, degrade or discriminate against specific types of online content.

2. Non-Discrimination – requires that all individuals regardless of their "race", color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status are treated equally.[18] In the context of elections and online campaigns, this largely relates to the use of discriminatory language against voters or candidates who belong to specific communities and groups. Moreover, respect for this principle should be assessed against the negative practice of some big-tech companies' algorithms and search engines that systematically discriminate or down-rank content and search results related to specific groups and communities. OSCE participating states have committed in the 1990 Copenhagen Document to ensure conditions in which citizens are permitted, "to seek political or public office, individually or as representatives of political parties or organizations, without discrimination."

---

13 The UN HRC resolutions from 2012 and 2016 on the promotion, protection and enjoyment of the human rights on the Internet affirmed "that the same rights [...] offline must also be protected online, in particular freedom of expression" and call for "adopting national Internet-related public policies that have the objective of universal access and enjoyment of human rights."

14 See the UN, OSCE and Organization of American States (OAS) Joint Declarations on: Freedom of expression and the Internet (2011); Universality and the right to freedom of expression (2014); Freedom of expression and "fake news", disinformation and propaganda (2017); Media independence and diversity in the digital age (2018); Challenges to freedom of expression in the next decade (2019), Freedom of Expression and Elections in the Digital Age (2020) and the Joint Declaration on Politicians and Public Officials and Freedom of Expression (2021).

15 At the moment of writing these Guidelines the list includes: Estonia, Finland, France, Greece and Spain.

16 At the global level, net-neutrality has been advocated for in the 2011 UN, OSCE and OAS Joint Declaration on Freedom of expression and the Internet. The Council of Europe Committee of Ministers stated that the principle of net-neutrality, "reinforces the full exercise and enjoyment of the right to freedom of expression." See also the 2015 EU regulation, the Inter-American Commission on Human Rights, Standards for a Free, Open, and Inclusive Internet, and 2019 Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections. See also the 2017 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

17 See the 2016 OSCE Media Freedom on the Internet Guidebook and the 2010 Council of Europe Declaration of the Committee of Ministers on Network Neutrality.

18 International law posits that everyone be treated as equal before the law and enjoy equal protection of the law. See the ICERD; CRPD; ICCPR and General Comment No. 28; OAS, American Convention on Human Rights (ACHR); Charter of Fundamental Rights of the European Union (EU CFR); Convention on Human Rights and Fundamental Freedoms (CIS CHR).

3. Equality of Opportunities – a level playing field is an essential part of fair competition.[19] Election campaign frameworks, for traditional or online campaigning, should provide opportunity for all contestants and other eligible stakeholders to freely express their views on an equal basis and without undue restrictions. All electoral contestants should have the same opportunities to present their candidacies, should be subject to the same rules governing the use of online space for campaigning and enjoy the same access to social networks. Several OSCE commitments in the 1990 Copenhagen Document specifically call for equal treatment and fair opportunities for competition, including in paragraphs 7.6 and 7.7.[20]

4. The Principle of Transparency – lies at the heart of assessments of political and campaign financing.[21] It is therefore a key element when it comes to observing campaigns, in particular with regard to the disclosure of sources of funding and amounts spent online by electoral contestants, political parties and third-parties. In the context of social networks, the principle of transparency is also relevant in the moderation of online content (for instance how a certain type of content is promoted, down-ranked or removed from specific platform). The implementation of the principle of transparency remains a challenge and can be often curtailed because of the transnational and decentralized nature of social networks and the possibility of network users to remain anonymous, and limited enforcement mechanisms.[22]

5. Data Protection – recently became a fundamental principle in the public discussion about the impact that social networks have on political and electoral developments. Private companies (big-tech platforms, data brokers but also electoral contestants) process large amounts of personal data collected from surveys, public records, online activities, commercial sources and other means. These are often used for targeted campaigning, advertising, direct messaging and assessing voters' preferences. International law

19 See also the ICCPR; CRPD; ACHR; CFR; Convention on Human Rights and Fundamental Freedoms (CIS CHR); General Comment No. 25; Council of Europe 2001 Committee of Ministers' Recommendation on Financing Political Parties 1516(2001), and 2002 Code of Good Practice in Electoral Matters. The article 10 CIS Convention on Standards of Democratic Election, Voting Rights and Freedoms in the Member States of the Commonwealth of Independent States for ensuring fair elections require that, "equal possibilities for every candidate or every political party (coalition) to participate in the election campaign, including the access to mass media and means of telecommunications."

20 In paragraph 7.6 of the 1990 OSCE Copenhagen Document participating States have committed to, "provide political parties and organizations with the necessary legal guarantees to enable them to compete with each other on a basis of equal treatment before the law and by the authorities," and in paragraph 7.7, "to permit political campaigning to be conducted in a fair and free atmosphere in which neither administrative action, violence nor intimidation bars the parties and the candidates from freely presenting their views and qualifications, or prevents the voters from learning and discussing them."

21 The 2003 United Nations Convention against Corruption (UNCAC), states that each State Party shall also consider taking appropriate measures, "to enhance transparency in the funding of candidatures for elected public office." Other international standards are encompassed in the Recommendation (2003)4 of the Council of Europe Committee of Ministers to member States and Recommendation 1516 (2001) of the Parliamentary Assembly of Council of Europe (PACE). See also articles 7 and 12 of the CIS Convention on Standards of Democratic Election, Voting Rights and Freedoms in the Member States of the Commonwealth of Independent States.

22 The lack of transparency has been cited as a main flaw in content moderation and regulation by big-tech companies. See the 2019 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. See also UN, OSCE and OAS 2011 Joint Declaration.

provides for protection from, "arbitrary unlawful interference with [...] privacy, family, home or correspondence," and obliges 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 use it."[23] The protection of this right is also enshrined in many regional instruments, including the 1990 OSCE Copenhagen Document.[24] The right to privacy applies equally online and a number of instruments call for enhanced data protection on the Internet.[25]

6. Freedom of assembly and freedom of association – are protected by the UDHR and the ICCPR, as well as by the 1990 OSCE Copenhagen Document.[26] Other regional bodies, such as the Council of Europe and its European Convention on Human Rights (ECHR) or the CIS also protect or guarantee freedoms of peaceful assembly and association.[27] Digital technologies have brought new opportunities for the enjoyment of these freedoms and vastly expanded the capacities of individuals, political movements and civil society groups to organize and mobilize, to connect with other groups and co-ordinate their activities, and to gather in an online environment without undue physical interference from third parties or governments.[28] Both the UN General Assembly and the UN HRC have stressed States' obligation to protect the freedom of assembly and association online.[29] The UN HRC has acknowledged that although an assembly, "has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online."[30]

---

23 See the ICCPR and the UN Human Rights Committee General Comment No. 16.

24 The 1990 OSCE Copenhagen Document requires States to ensure access to information and protection of privacy.

25 See the UN General Assembly Resolution on the right to privacy in the digital age, the Council of Europe's Convention 108 for the protection of individuals with regard to automatic processing of personal data; Council of Europe Committee of Ministers Recommendation (20012)/4 on the protection of human rights on social networking services and Recommendation (2016)/5 on Internet freedom.

26 In the 1990 OSCE Copenhagen Document, the participating States committed themselves to upholding fundamental freedoms that are central to the conduct of democratic elections including peaceful assembly (paragraph 9.2) and association (paragraph 9.3). Further, paragraph 7.6 provides for the, "right of individuals and groups to associate in their own political parties" and paragraph 7.7 ensures that political campaigns are, "conducted in a free and fair atmosphere," in which neither, "violence nor intimidation bars the parties and the candidates from freely presenting their views and qualifications, or prevents the voters from learning and discussing them or from casting their vote free of fear of retribution."

27 See Article 11 of the ECHR and Article 12 of the 2000 Charter of Fundamental Rights of the European Union (CFR). See also article 12 of the CIS CHR.

28 See the 2019 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the 2018 Encryption and Anonymity Report.

29 See the UN General Assembly Resolution on the promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association; and the UN HRC Resolution on the promotion, protection and enjoyment of human rights on the Internet.

30 See the UN HRC Resolution on the promotion and protection of human rights in the context of peaceful protests.

7. Right to effective remedy – in the context of elections, requires that the States institute rules and procedures to allow voters, contestants and other electoral stakeholders to challenge violations of their election-related rights through an effective dispute resolution system.[31] In the context of the online election campaign, this right requires that the bodies responsible for election dispute resolution should ensure effective and timely remedies for violations of voters, candidates or other electoral stakeholders' rights online, including violations by social networks and big-tech companies, such as moderation and removal of content, data protection or political and campaign advertising matters.

Relevant for the implementation and respect of the above-mentioned freedoms and rights in the context of election campaigning on social networks owned by several big-tech companies, are the **UN Guiding Principles on Business and Human Rights.** The document elaborates on the application of the human rights in the work of transnational corporations and other business enterprises and provides three general sets of principles: (i) existing obligations for member States to respect, protect and fulfil human rights and fundamental freedoms; (ii) the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights; and (iii) the need for rights and obligations to be matched to appropriate and effective remedies when breached. In connection to these principles, the document states that, "laws [should be] aimed at, or have the effect of, requiring business enterprises to respect human rights" and that "business enterprises should respect human rights."[32]

31 See Article 2.3 of the ICCPR; Article 13 of the ECHR; paragraph 5.10 of the 1990 OSCE Copenhagen Document and Article 6 of the CIS CHR.

32 See the 2011 UN Guiding Principles on Business and Human Rights.

3.

GENERAL FEATURES of ELECTION CAMPAIGNS on SOCIAL NETWORKS

Often, campaigning on social networks is only one of the methods used in the overall electoral campaign. The enormous amount of information on social networks and the challenges stemming from their global and decentralized nature, make full-scale monitoring impractical and unfeasible. While ODIHR's approach to observing and assessing online campaigning is elaborated in the next chapter, based on the OSCE participating

States and other intergovernmental organizations approaches to regulate or address campaigning on social networks, this chapter provides outline of the following key features:

1. Online content and activity;
2. Digital political and campaign advertising; and
3. Voters' data protection rules.[33]

3.1 CONTENT AND ACTIVITY

User-generated (or user-created) content is any content, such as text, voice recording, videos, images or mix of all, created by an individual or a group of social network users. Due to its 'organic' nature, big-tech companies and many states and international organizations treat this type of content differently than content created by commercial brands and more recently content created by political parties, electoral contestants, institutions, and civil society organizations. A third-type of content that is distinct of the previous two categories is content created by so-called social network 'influencers'. [34]

Within the OSCE region, there are numerous national and international attempts to regulate online content and activity, including during election periods. In doing so, participating States should take into account the necessary elements for the protection of the right to freedom of expression and other fundamental rights. In addition to its conventional understanding as a right to hold and express different political views, which is of crucial importance for free conduct of election campaigns, the freedom of expression can also include or relate to speech that may be regarded as deeply offensive, and to information or ideas that can offend, shock or disturb.[35]

At times some limitations on the freedom of expression may be imposed, but only in line with international obligations and standards and when the expression includes incitement to violence, hostility, hatred, discrimination or other types of extreme aggressive or intolerant rhetoric, and public disorder.[36] With regard to regulation and restrictions

33 Campaign-related *online content* and any restrictions imposed on it are closely linked to freedom of expression, the right to access to the Internet, non-discrimination, and the principle of transparency and net neutrality; *political and election advertising* is mainly linked to the principles of transparency, equality of opportunity and non-discrimination; and the *data protection* aspect is related to the right to privacy and transparency.

34 A social network 'influencer' in the context of an election is a person or owner of an account, who actively proliferates political content and holds influence over certain voters or categories of voters when it comes to the formation of their opinion and choice. While the phenomenon of 'influencers' is mainly active in the commercial world, it is becoming increasingly relevant in political and election communications on social networks.

35 See General Comment No. 34 and the European Court of Human Rights Explanatory Memorandum on Freedom of Expression and Information.

36 Moreover, as provided in the ICCPR any limitations must fulfil the three-part test of legality, necessity and proportionality.

on the freedom of expression and opinion on the Internet, the UN HRC stated that only content-specific restrictions compatible with the protection and promotion of human rights are permissible, and it excludes generic bans.[37] Within the OSCE region, the practice has shown that participating States aim to regulate or restrict three general categories of content and speech which:

- Contains elements of incitement to hatred or violence;
- Is intolerant, aggressive or offensive; and most recently
- Has a manipulative character with intent to cause harm or often referred as 'disinformation'.[38]

While instances of speech that contains the above elements are present and extend beyond the election periods, they gain in intensity especially during election campaigns. The use of this type of speech might have a negative impact on the voters, either to discourage them to participate in elections, or impact their right to form opinion on different political matters without interference or misinform them on some technical and factual aspects of the election process, thus ultimately diminishing the public trust in the overall political and election process.

Key challenges for the OSCE participating States in the debate for regulation of online content and its impact on fundamental freedoms, most notably the freedom of expression, are related to the *lack of the common definitions and understanding* of basic concepts, such as, incitement, hatred or 'disinformation' as well as about *the role and liability of social networks* (or the big-tech companies as their owners) in dissemination of content. In addition to these concerns some criticism has been also expressed related to inconsistent case-law practices even within the same jurisdictions. It is important to note that the practice has shown that the interpretation on the meaning of these concepts, and impact or the responsibility of social networks is subject to lengthy judicial processes, involving a complexity of actors and decided on a case by case basis.[39]

In the absence of a common understanding, ODIHR observers should refrain from providing definitions, classifications or characterizing particular events or activities observed within these concepts. ODIHR observers should focus their efforts on providing assessment about the impact of these malpractices have on the election process and the assessment should be based on relevant international obligations, standards principles and commitments for democratic elections.

---

37 See General Comment No 34. In a 2011 Report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression acknowledged that "blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal."

38 The OSCE Representative of Freedom of Media (RFoM) is mandated by the OSCE participating States to provide an early warnings and rapid responses to serious non-compliance with regard to free media and freedom of expression. While dealing with media content is not at the core of the mandate of the OSCE RFoM, these issues may be of concern for a number of reasons and therefore the RFoM has issued number of statements and reports. See the OSCE RFoM website.

39 See the European Court of Human Rights hate speech data base.

Following two seminal judgments the European Court of Human Rights developed and now applies five criteria when considering cases on intermediaries liability for user-generated content: (i) the context and content of the impugned comments; (ii) the liability of the authors of the comments; (iii) the measures taken by the website operators and the conduct of the injured party; (iv) the consequences of the comments for the injured party; and (v) the consequences for the applicants. In the case **Delphi AS vs Estonia** the Court found the intermediary in question responsible due to the extreme nature of the user-generated content and ruled that intermediaries should bear liability especially in cases that involve incitement to violence or 'hate speech', emphasizing the professional and commercial character of the news platform. In the case **Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt vs. Hungary,** which involved insults and vulgar comments but did not concern a form of 'hate speech' or direct threats against individuals, the European Court of Human Rights confirmed that news portals, in principle, must assume duties and responsibilities, however, because of the particular nature of the Internet, these duties and responsibilities may differ to some degree from those of a traditional publisher, notably as regards third-party content. Most crucially the Court stated that by establishing objective liability on the side of the Internet websites, merely for allowing unfiltered comments that might be in breach of the law, would require, "excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet," and considered the negative consequences of holding intermediaries liable for third-party comments.[40]

a. Incitement to Hatred, Hostility or Violence

Globally, international treaties prohibit *incitement* to hatred, discrimination, hostility and violence but there is a lack of consensus on the meaning and clear definition on the concept of 'hate speech'.[41] However, at the regional level, organizations such as the Council of Europe have provided definition for this concept.[42] Overall, across the OSCE regions many national laws remain vague and fail to define key terms such as 'hatred' or 'incitement'; overly broad interpretations of what constitutes 'hate speech' can provide possibilities for speech restrictions for illegitimate purposes.[43]

---

40 The Court further noted that, "such liability may have foreseeable negative consequences on the comment environment of an Internet portal […] For the Court, these consequences may have, directly or indirectly, a chilling effect on the freedom of expression on the Internet."

41 See the ICCPR, which requires States to prohibit, "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" and "any propaganda for war."

42 The Council of Europe's Committee of Ministers has stated that the term 'hate speech' covers all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin. See Council of Europe dedicated website on 'hate speech'.

43 A treaty that explicitly addresses forms of expression that can be interpreted as 'hate speech' is the ICERD. According to the ICERD, although there may be some prohibitions, States are not obligated to criminalize 'hate speech'. In 2013, the Committee on the Elimination of Racial Discrimination, the expert body that monitors the ICERD, clarified in its General Comment No.35 that criminalization, "should be reserved for serious cases, to be proven beyond reasonable doubt, while less serious cases should be addressed by means other than criminal law, taking into account, inter alia, the nature and extent of the impact on targeted persons and groups."

The lack of clear definitions causes inconsistent adoption and implementation of regulations in the OSCE region. However, aware of the threats to public life of the spread of these issues, the OSCE participating States, "decided to take strong public positions against hate speech and other manifestations of aggressive nationalism, racism, chauvinism, xenophobia, anti-Semitism and violent extremism, as well as occurrences of discrimination based on religion or belief," and, "recognize the need to combat hate crimes, which can be fueled by racist, xenophobic, and anti-Semitic propaganda on the internet."[44] While the majority of the OSCE participating States have laws that restrict certain forms of speech, "there are extreme variations between the hate speech laws of different countries [and] common criticism of hate crime laws is that they infringe freedom of speech or amount to a penalty for opinions or attitudes rather than actions."[45]

The **UN Strategy and Action Plan on Hate Speech** covers three categories of levels of unlawful and lawful expression.[46] At the *top level*, are "direct and public incitement to genocide" and "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." These are prohibited under international law. At the *intermediate level,* certain forms of 'hate speech' may be prohibited, but only if restrictions are provided by law, pursue a legitimate aim (e.g., respect of the rights of others, or the protection of public order) and are necessary and proportionate. At the *bottom level,* legal restrictions should not be imposed on the dissemination of lawful expressions that are, for example, offensive, shocking or disturbing. (See below Article 19's Hate Speech Pyramid). The Strategy also sets the UN approach and responses to instances of 'hate speech' that should be assessed on the basis of the six criteria set in the **Rabat threshold test.**[47] In implementing the Strategy the UN notes that: a. only incitement to discrimination, hostility or violence that meets *all six* criteria should be criminalized; b. less severe forms of incitement or 'hate speech' (i.e., which do not meet all six criteria) should attract civil or administrative law-based restrictions, or public policy responses; and c. public condemnation of hate speech, accountability for attacks on those exercis¬ing their right to freedom of expression, and the expediting of public policy measures on the promotion of diversity may be especially important in the immediate aftermath of an incident of hate speech or incitement, when tensions are escalating in a society.

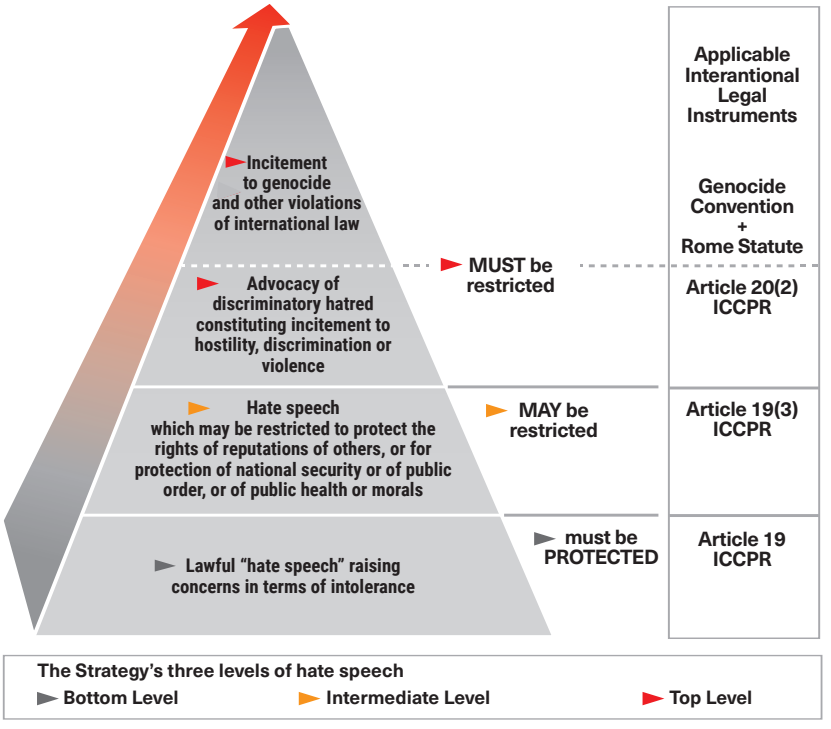
44 See the Ministerial Council Decision 10/06 in Porto and Ministerial Council Decision 04/03 in Maastricht.

45 See the RFoM 2015 Non-Paper of on Propaganda and Freedom of Expression and the 2009 ODIHR Hate Crime Laws, *A Practical Guide*.

46 See the 2020 UN Strategy and Action Plan on Hate Speech.

47 The Rabat Plan of Action, an initiative of the UN Human Rights Office of the High Commissioner, on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence suggests a high threshold for defining restrictions on freedom of expression, incitement to hatred, and for the application of article 20 of the ICCPR. It outlines a six-part threshold test that needs to be fulfilled in order for a statement to amount to a criminal offence: (i) the social and political context, (ii) status of the speaker, (iii) intent to incite the audience against a target group, (iv) content and form of the speech, (v) extent of its dissemination and (vi) likelihood of harm, including imminence.

Article 19's Hate Speech Pyramid[48]



SOURCE: Based on ARTICLE 19, "Hate Speech" Explained: A Toolkit, p19.

With the emergence of social networks, the use of different forms of vulgar, harmful, hostile and even illicit content became highly visible, especially during election periods. According to international law, extreme measures such as blocking policies, Internet shutdowns or criminalization of online political dissent should be applied only in exceptional cases of openly illegal content or discourse not protected by the right to freedom of expression.[49] In all other cases, alternative tools should be deployed such as education, counter-speech and the promotion of pluralism.[50]

Despite many efforts, initiatives and public campaigns for tackling 'hate speech', numerous international organizations report that many individuals, groups and communities remain targets of online hatred and discrimination. Discriminatory practices, incitement to violence and 'hate speech' are not limited to racism and xenophobia, but may also take the form of sexism, anti-Semitism, Islamophobia, misogyny,

48 Article 19 is an international human rights organization working on issues of freedom of expression and access to information. See Article 19 'Hate Speech' Explained: A Toolkit.

49 This includes war propaganda and advocacy of hatred that constitutes incitement to violence, direct and public incitement to genocide and child pornography, provided that the illegality of the content has been determined by a judicial authority.

50 See the 2019 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

homophobia and others.[51] While online platforms allow voters to share information and opinions freely, they also leave the door open to undue comments, including sexist and other discriminatory remarks.[52] Online harassment can lead to the exclusion of certain groups from the political and electoral contest, in particular women candidates, who in some contexts can be the preferred targets of such speech.[53]

b. Intolerant, Aggressive and Negative Rhetoric

In some contexts, election campaigns may become emotionally charged, with contestants or voters using more aggressive rhetoric. In the OSCE region, a number of participating States have adopted and implemented provisions for the online domain that replicate regulations and restrictions designed for conventional ways of campaigning and for traditional media, including criminal defamation laws. In general, criminal defamation laws, as well as their application and abuse by politicians or other public figures, are in violation of international standards.[54] Moreover, sanctions for defamation or insult must be proportional to the violation of the rights or reputation of others. The measures adopted by States should give consideration to any possible effective and adequate voluntary remedies that have been granted by the media and accepted by the individuals concerned.

The European Court of Human Rights, in two landmark judgments, ruled that, "freedom of expression [...] is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population," which are necessary for the existence of, "pluralism, tolerance and broadmindedness without which there is no democratic society." The Court also noted that, "the limits of acceptable criticism [...] are wider with regard to a politician acting in his public capacity", who "inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large."[55] While both judgments were made in the pre-social networks era, the Court recently reaffirmed that, "its jurisprudence [related to] Article 10 is fully applicable to the Internet."[56]

51 See PACE Resolution 2144 (2017) on Ending cyber-discrimination and online hate.

52 See Council of Europe Study DGI (2017)10 Media, Elections and Gender.

53 A 2018 Inter-Parliamentary Union (IPU) – PACE study showed that women members of parliament in Europe are more likely to be targets of online attacks. A 2016 study conducted by the same body established that "social media have become the number one place in which psychological violence – particularly in the form of sexist and misogynistic remarks, humiliating images, mobbing, intimidation and threats – is perpetrated against women parliamentarians."

54 See the OSCE RFoM dedicated website on defamation. The UN Human Rights Committee in General Comment No. 34 has affirmed that all states "should consider the decriminalization of defamation and, in any case, the application of criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty." The UN, OSCE and OAS 2020 Joint Declaration call upon states to repeal criminal defamation and replace it with appropriate civil defamation regulations.

55 See European Court of Human Rights cases of Handyside vs UK (1976) and Lopes Gomes da Silva v. Portugal (2000).

56 See European Court of Human Rights on Freedom of expression and information - Explanatory Memorandum.

c. Manipulative Information

The debate about a common understanding and the development of unified terminology for the issues elaborated above is ongoing but these malpractices have been in the public sphere for quite some time and States have experience in addressing them and as such they are often subjected to sturdy regulatory standards. On the other hand, the phenomenon of online proliferation of manipulative content (most commonly called 'disinformation') which especially gains in intensity during campaign periods presents bigger challenges for regulation and often can have decisive or detrimental impacts on election processes and outcomes.[57] Due to the absence of clear regulatory standards, corresponding to the new challenges steaming from the online world and its global nature and the potential for virality that social networks provide, in some contexts the spread and proliferation of this type of content has become increasingly pronounced and became a source of concern for the overall integrity of the election process.

Different types of manipulative online content, especially **disinformation,** can be harmful to the democratic process and adversely affect the conduct of genuinely democratic elections. As this type of content is often used to mislead voters or undermine public confidence in the electoral process, it inhibits the voters' right to form an opinion without undue interference and weakens their ability to make fully informed decisions. In broader terms, this type of content may also interfere with the right to freedom from unlawful attacks upon honour and reputation, as it often relates to a particular individual, a political or public figure, and is designed to harm her or his reputation, and when directed against particular groups in society, such as migrants or certain national minority groups, and incites hatred, violence or discrimination, it can interfere with the non-discrimination principle, as provided by the ICCPR. At the same time, poor regulation and/or policy responses from either the big-tech firms or authorities can also have detrimental effects on the protection of fundamental rights, in particular the right to freedom of expression. Overly broad restrictions on manipulative content and disinformation can lead to the curtailment of legitimate speech.[58]

The OSCE participating States have committed to ensuring conditions for electoral processes in line with democratic standards and principles, and thus have a responsibility to provide for an election environment devoid of manipulative content and in which voters are free to form their opinions without undue interference. Accordingly, the participating

57 While there is no universally accepted definition on information of manipulative content, some organizations attempted to make distinction between different types of information disorder such as: (1) *Disinformation:* knowingly sharing false or misleading information with the intent to harm; (2) *Misinformation:* false or misleading information, but without the intent of causing harm; (3) *Malinformation:* genuine information shared with the intent to cause harm. These Guidelines focus on the assessment of the impact of different types of manipulative content on the integrity of the election process and conduct of election campaigns and do not attempt to provide terminological clarification and distinction between these concepts.

58 The 2017 UN, OSCE and OAS Joint Declaration emphasizes that some forms of manipulative content may harm individual reputation and privacy, or incite violence, discrimination or hostility against identifiable groups in society. However, the Declaration concludes that "general prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information,' are incompatible with international standards for restrictions on freedom of expression [...] and should be abolished." Moreover, the 2020 Joint Declaration on elections in the digital age argues against Internet blocking and shutdowns, as well as against overly broad or ambiguous laws on disinformation.

States bear responsibility and are obliged to tackle the phenomenon of disinformation. The decentralized, dispersed and extraterritorial nature of social networks, the difficulties of identifying perpetrators due to user anonymity, and often ineffective judicial responses owing to the absence of jurisdictional authority, have prompted many governments to address this phenomenon through multilateral efforts and co-operation that also engages non-state actors such as civil society, media and the big-tech firms.

The 2021 **Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression** examines the threats to human rights, democratic institutions and electoral processes that disinformation poses. The report acknowledges the complexities and challenges posed by disinformation in the digital age, and finds that the responses by States and companies have been problematic, inadequate and detrimental to human rights. The report calls for multi-dimensional and multi-stakeholder responses that are well grounded in the international human rights framework and urges big-tech companies to review their business model and States to recalibrate their responses to disinformation, enhancing the role of free, independent and diverse media, investing in media and digital literacy, empowering individuals and rebuilding public trust. Specifically to elections, the report recognizes that disinformation campaigns have been used, "in highly visible ways to undermine the right to free and fair elections [and] that have sought to influence elections." The report concludes that due to the disinformation phenomenon, "it is easy – but dangerous – to lose sight of the value that digital technology offers to democracy, sustainable development and human rights, or the vital importance of the right to freedom of opinion and expression in that equation. That is why attempts to combat disinformation by undermining human rights are short-sighted and counterproductive. The right to freedom of opinion and expression is not part of the problem, it is the objective and the means for combating disinformation." [59]

d. Tackling Manipulative Information

i. State Responses

In addition to the lack of clarity and agreement on the definition of what constitutes manipulative information, which reduces the effectiveness of responses, one of the key challenges that most of the OSCE participating States face is how to address and regulate manipulative content in a way that respects human rights and fundamental freedoms and the principles of legality, necessity and proportionality.[60] A human rights-based approach requires targeting not only disinformation directly, but also the adverse impact caused by it. Adequate, long-term policies for improving digital literacy and awareness-raising campaigns for electoral stakeholders should be put in place, rather than exclusively relying on legislative or regulatory solutions that might negatively affect fundamental rights, including the freedom of expression.

59 See the 2021 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

60 See the 2020 UN HRC Resolution 44/12 on Freedom of opinion and expression.

While the OSCE participating States have a positive obligation to provide a level playing field for all contestants and to give effect to voters' rights, as enshrined in international and regional instruments, there is no one-size-fits-all solution to the challenges posed by manipulative content.[61]

Globally, **four state-driven approaches to tackle disinformation and manipulative content can be observed**, including among the OSCE participating States:

(i) Application of relevant provisions of existing civil, criminal, administrative, and other laws regulating the media, elections, and anti-defamation, even though these laws, enacted in the pre-Internet era, do not always reflect current technological developments;

(ii) Enactment of new legislation that imposes sanctions on social networks that spread false news, usually imposing fines and ordering the removal of information identified as false;

(iii) Co-operation with election authorities and online platforms to secure a well-informed electorate, either by identifying and blocking fake news, providing fact-checking resources for the general public, or through the mass publication of "real" news during election season and beyond; and

(iv) Employing broader and long-term policies for educating citizens about the dangers of fake news.[62]

Throughout the OSCE region, several States have adopted laws imposing intermediary liability for user-generated content; an approach criticized by relevant human rights organizations as not fully in line with international standards, which calls on States to avoid delegating responsibility to companies as adjudicators of content. Assigning this kind of liability and responsibility to private companies empowers them with corporate judgment over human rights values, often to the detriment of the users' enjoyment of freedoms.[63] Other OSCE participating States have adopted non-regulatory measures, including the development of professional codes, establishment of media councils, appointment of public broadcasters or the creation of specialized units to counter information disorder, as well as self-regulation efforts by media companies and media literacy programmes.[64]

61 According to article 2 of the ICCPR, States are the primary duty bearers with obligations to respect, protect and fulfil human rights and have a positive obligation to give effect to these rights. In the context of disinformation, the States have a duty to refrain from interfering with the right to form opinions and an obligation to ensure that others, including businesses, do not interfere with it, and to proactively put information of public interest in the public domain, as well as promoting plural and diverse sources of information, including media freedom.

62 See the Library of Congress 2019 Report Initiatives to Counter Fake News in Selected Countries.

63 See the UN HRC Contribution of parliaments to the work of the HRC and its universal periodic review. See also both, the 2017 and 2020 UN, OSCE and OAS Joint Declarations that reiterate that intermediaries should never be held liable for disseminated content, unless they specifically intervene in that content or fail to implement a legally binding order to remove it and have the technical capacity to do so. Moreover, both declarations call upon big-tech companies to use a human rights-based approach to content regulation and to implement the UN Guiding Principles on Business and Human Rights.

64 For a detailed overview of national case studies, see the OSCE 2019 report on disinformation.

ii. Big-Tech Companies

Private companies should implement a human rights approach to content moderation and regulation, however, it is important to note they do not have the same human rights obligations as States. In response to increased public pressure and following numerous controversies related to both massive and widespread information of manipulative content, at times leading to hostility and violence, and the misuse of private data, including for political and campaign purposes, which might have had a decisive effect on election outcomes, several big-tech companies adopted a set of measures to tackle these challenges.[65] Furthermore, as previously noted, some States adopted regulations that placed a direct obligation and responsibility on big-tech companies as liable intermediaries for user-generated content. However, the attempts of private entities' to avoid liability and financial sanctions can sometimes lead to the removal of lawful and legitimate content with no opportunity for redress.

While it can be a positive development, self-regulation is generally carried out on a voluntary basis. In addition to the concerns about big-tech companies acting as adjudicators of content, other issues relate to the platforms' reliance on automation to flag or remove content and insufficient transparency about the standards and processes for restricting content. The use of artificial intelligence software for removing content lacks contextual evaluation and poses distinct risks of actions that are inconsistent with human rights law. As a general rule, any policies restricting content should be clear, objective, easily accessible and understandable, and users should be promptly notified in case of any action taken against their content.[66]

Big-tech companies have a range of options other than deletion or removal of websites and accounts. The measures can include:

- Content deletion;
- Restricting its virality;
- Labelling its origin;
- Suspending the relevant user or organization sponsoring the content;
- Developing ratings to highlight a person's use of prohibited content;
- Temporarily restricting content while a team conducts a review;
- Precluding users from monetizing their content;
- Creating friction in the sharing of content;

65 The changes introduced by some big-tech companies were made mostly to address public concerns, including those coming from intergovernmental organizations, such as the EU. In addition to content moderation rules, new policies included additional safeguards for the protection of users' private data and transparency measures for political advertising. The adopted set of measures was made in line with the big-tech commitments to the EU Code of Practice on Disinformation (discussed later in the Guidelines). While some progress has been noted within the EU context, "the reports show that further efforts must be deployed in other areas to improve the reliability of the online ecosystem and the protection of users." Moreover, one of the key criticisms towards big-tech companies relates to the fact that, irrespective of their global presence and outreach, the policies for data protection, content moderation and transparent political and campaign advertising are uneven across different countries, including those from the OSCE region.

66 See the UN, OSCE and OAS 2017 Joint Declaration.

- Affixing warnings and labels to content;
- Providing individuals with greater capacity to block other users;
- Minimizing the amplification of content;
- Interfering with bots and co-ordinated inauthentic behaviour;
- Adopting geolocation restrictions; and
- Promoting counter-messaging.[67]

iii. International Community Efforts

Several UN institutions and agencies have devoted substantial attention to the phenomenon of dissemination of manipulative content. Specifically addressing the impact of disinformation on elections, the UN Secretary General in its 2019 report to the UN General Assembly, stated that the use of the Internet in the context of elections, "as both enablers of participation and tools for spreading disinformation and hate speech, raised complex issues [...] The paralyzing suspicion that any information or discourse can be manipulated – and the resulting erosion of trust – lies at the heart of the Internet's challenge to democracy. The importance of, among other measures, building societies' resilience against the spread of false or hateful content, increasing transparency in public discourse and pursuing multi-stakeholder dialogue to find answers to those policy challenges, is underlined." Moreover, in addition to this and the already referenced statements and reports by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the United Nations Educational, Scientific and Cultural Organization (UNESCO) has issued several publications related to the broader issue of information disorder and its impact on election processes.[68]

Within the OSCE context, the OSCE RFoM issued several documents on freedom of expression issues on the Internet.[69] Further, in co-operation with the UN and the OAS freedom of expression rapporteurs, the OSCE RFoM has issued several joint declarations related to information disorder, including the 2020 Joint Declaration on Freedom of Expression and Elections in the Digital Age and the 2021 Joint Declaration on Politicians and Public Officials and Freedom of Expression.[70]

The 2020 **Joint Declaration** recognized, "the essential role that freedom of expression and information, free, independent and diverse media and a free and accessible Internet play in ensuring free and fair elections" and that different types of information of

67 See the 2019 Report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

68 See the 2018 Handbook for Journalism Education and Training, the 2019 Elections and Media in Digital Times and the 2020 Broadband Commission research report Balancing Act: Countering Digital Disinformation while Respecting Freedom of Expression.

69 See the OSCE RFoM 2013 Social Media Guidebook, the 2016 Media Freedom on the Internet: An OSCE Guidebook and the 2019 Review of International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media.

70 See the UN, OSCE and OAS 2020 Joint Declaration and the 2021 Joint Declaration.

manipulative content "can exacerbate and even generate election related tensions." It calls, "on parties and candidates to avoid intentionally using these types of statements to enhance their electoral prospects and recognizing the important role played by independent election regulators in addressing these forms of speech and promoting access to information," and expresses concerns over some States practices, such as, "passing laws which [...] unduly limit freedom of expression." The Joint Declaration provides a set of recommendations to States and non-state actors, including big-tech companies aimed at protecting freedom of expression on the Internet."

The 2021 **Joint Declaration** acknowledges, "that politicians and public officials play an important role in shaping the media agenda, public debate and opinion," and expresses, "concern at the growing incidence of online and offline 'hate speech', disinformation and dangerous rhetoric against and scapegoating of the media, human rights defenders and groups at risk of discrimination, including by politicians and public officials, which chills freedom of expression, thereby reducing the diversity of information and ideas in society and misleading citizens." Further, the 2021 Joint Declaration denounces, "the increase in public communications by some politicians and public officials which are intolerant and divisive, deny established facts, attack journalists and human rights defenders for exercising their right to freedom of expression, and seek to undermine democratic institutions," and reiterates, "States have a positive obligation to create an enabling environment for freedom of expression and the right to information." Similar to the previous declaration, to protect freedom of expression the 2021 Joint Declaration provides a number of recommendations to States and non-state stakeholders, as well as for political parties, politicians and senior public officials.

Numerous other intergovernmental institutions, as well as international civil society networks and organizations within the OSCE area, have called for a multi-stakeholder approach and shared responsibility of all interested parties to establish efficient mechanisms of transnational co-operation to tackle manipulative content. These regional initiatives are of fundamental importance in tackling this type of information, including during election periods, because its creation and dissemination extends beyond national borders and jurisdictions. These joint response efforts are also particularly relevant because they aim to address the challenges steaming from the spread of manipulative content that intends to cause public harm, influence democratic processes or election outcomes.

While most of these initiatives deal with manipulative content in a broader manner and its negative impact on the overall societal and democratic developments, some have recognized and addressed the specific influence this type of content has on election processes. Efforts for tackling manipulative content have more wide-ranging approaches, which include not only suggestions or recommendations for content creation, moderation, spread and other activity-related aspects, but also for data privacy protection and transparency in political and campaign advertising. Therefore, most of the initiatives cited here that are present in the OSCE area are relevant for the subsequent sections on political advertising and data protection.

Several Council of Europe institutions have also addressed the issue of dissemination of manipulative content during and outside of election periods and the role that social networks have in preventing its spread. In 2020, the Committee of Ministers adopted a Recommendation on the human rights impact of algorithmic systems and in 2018 a Recommendation on the roles and responsibilities of Internet intermediaries.[71] PACE advocated inclusion of media literacy in school curricula, support for awareness-raising projects and targeted training to promote the critical use of social networks, online media, and support for professional journalist training.[72] Specifically for election processes, in 2020, the Venice Commission adopted Principles for a fundamental rights-compliant use of digital technologies.[73]

The **Principles** emphasize the, "need for a human rights-compliant approach; human rights and fundamental freedoms must be translated into the digital environment." The document notes that the Internet, "affects the ways people communicate, conduct their behaviour and form their opinions, [and] transformed the way public opinion can be formed but also provided the means for distorting reality to an extent unknown before [...] The misuse of digital technology to manipulate facts, to spread disinformation in a strategic, coordinated fashion, to conduct surveillance by collecting information from (and about) citizens, and engaging political stakeholder groups, has affected people's trust in democratic institutions and the rule of law." These challenges, "threaten the democratic process in general, and have to be analysed with caution when it comes to electoral campaigns [and] problems arise when technology stops being a competitive advantage and turns into a threat to the integrity of elections, restricting the right to free elections." It recognizes that "digital technologies impact in different ways, both positive and negative, the different types of democracy [and] all the stages of electoral processes [and] the significant increase in the number of actors in the campaign, independent from the parties."

The document lists **eight principles** addressing broader aspects of the use of new technologies in electoral processes, such as data privacy and cybersecurity, as well as election campaigns on social networks:

Principle 1 - The principles of freedom of expression, implying a robust public debate must be translated into the digital environment, in particular during electoral periods.

71 See Recommendation CM/Rec(2020)/1 and Recommendation CM/Rec(2018)/2, which acknowledge the curatorial and editorial roles of various platforms and call on States to assign to them corresponding responsibilities. The CM/Rec(2018)/2 recommends States to ensure that laws and regulations applicable to intermediaries effectively safeguard the human rights and fundamental freedoms of users and that Internet intermediaries have a similar responsibility to conform to international human rights standards. It further notes that transparency, inclusivity, oversight and effective remedies are key to human rights-compliant content moderation on platforms. See also the 2019 Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, which emphasizes, "the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness and integrity of elections offline as well as online in line with established principles."

72 See 2017 PACE Resolution on online media and journalism: challenges and accountability.

73 See the 2020 Principles for a fundamental rights-compliant use of digital technologies in electoral processes.

Principle 2 - During electoral campaigns, a competent impartial EMB or judicial body should be empowered to require private companies to remove clearly defined third-party content from the Internet, based on electoral laws and in line with international standards.

Principle 3 - During electoral periods, the open Internet and net-neutrality need to be protected.

Principle 4 - Personal data need to be effectively protected, particularly during the crucial period of elections.

Principle 5 - Electoral integrity must be preserved through periodically reviewed rules and regulations on political advertising and on the responsibility of Internet intermediaries.

Principle 6 - Electoral integrity should be guaranteed by adapting specific international regulations to the new technological context and by developing institutional capacities to fight cyber-threats.

Principle 7 - The international co-operation framework and public-private co-operation should be strengthened.

Principle 8 - The adoption of self-regulatory mechanisms should be promoted.

The EU high-level group of experts was launched in 2018 to advise on policy initiatives to counter disinformation.[74] The EU strategy did not foresee regulatory intervention, but rather focused on a multi-dimensional approach, involving a self-regulatory Code of Practice, fact-checking, use of artificial intelligence and media literacy.[75] The initiatives outlined in the Code of Practice, the Action Plan against disinformation, and the subsequent monitoring of the implementation of big-tech commitments to the Code, have a specific focus on protecting the integrity of the European Parliament elections.[76]

The EU considers the threat coming from large-scale disinformation campaigns as a, "major challenge for Europe, require[ing] a co-ordinated response from the EU countries, the EU institutions, social networks, news media and the EU citizens." In response to these threats, the EU Commission has developed a number of initiatives to tackle disinformation, such as:

- the Code of Practice on Disinformation, laying out a set of worldwide self-regulatory standards;

74 All 27 EU members are OSCE participating States. See Final Report of the High Level Expert Group. See also Resolution 2016/2030(INI) on EU strategic communication to counteract propaganda.

75 See 2018 Communication on tackling online disinformation: a European approach. The self-regulatory 2018 Code of Practice on Disinformation included *Facebook*, *Google* and *Twitter* and in May 2019 Microsoft also joined and in June 2020 *TikTok* became 16th signatory of the Code. The new Code of Practice expected to be launched in 2021 intends to strengthen the co-operation framework and evolve towards a co-regulatory instrument as outlined in the EU Digital Services Act.

76 See the EU Commission Assessment of the Code of Practice on Disinformation, which outlines the key findings of the EU Commission assessment of the implementation and effectiveness of the Code, including those specifically made to protect the integrity of the European Parliament Elections. See also the 2019 EU Commission Election Report in complementing the specific transparency commitments on online political advertising.

- the European Digital Media Observatory, a European hub for fact-checkers, academics and other relevant stakeholders to support policy-makers;
- the Action Plan on Disinformation strengthens the EU capability and co-operation in the fight against disinformation;
- the European Democracy Action Plan develops guidelines for obligations and accountability of online platforms in the fight against disinformation;
- the Communication on "tackling online disinformation: a European approach" is a collection of tools to tackle the spread of disinformation and ensure the protection of the EU values;
- the COVID-19 Monitoring and Reporting Programme, carried out by signatories of the Code of Practice acts as a transparency measure to ensure accountability in tackling disinformation; and
- the European Cooperation Network on Elections is a network of representatives of Member States' authorities with competence in electoral matters that provides for practical exchanges on topics relevant to ensuring free and fair elections, including data protection, cyber-security, transparency and awareness raising. [77]

In 2019 the OAS has published a Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts which, "establishes a conceptual framework to address the phenomenon of the dissemination of deliberate misinformation and includes recommendations addressed to [OAS member] States and other actors that can positively impact the combat of misinformation." The Guide systematizes inter-American human rights standards that should guide state responses and presents a number of recommendations for different election stakeholders, including OAS member states and various state institutions, big-tech companies, political parties, media and journalists, fact-checkers, advertising companies that trade users' data and universities and research centres.[78]

iv. Civil Society Initiatives

Civil society initiatives have played an important role in empowering and informing voters, increasing public awareness and preventing the spread of different types of manipulative content. Many civil society organizations operate as part of larger networks that also monitor online content in general or during election periods. Several OSCE participating States have institutionalized fact-checking networks in co-operation with journalists, civil society, big-tech companies and the academic community to identify and debunk viral misinformation and thus combat 'fake-news'.[79]

77 See the EU Commission websites on Disinformation and on European Cooperation Network on Elections.

78 See the 2019 OAS Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts.

79 See the Council of Europe Information Disorder Report 2017, which lists some fact-checking initiatives.

3.2 POLITICAL AND CAMPAIGN ADVERTISING

Political and campaign advertising is the backbone of any democratic and competitive election.[80] In order to reach out and seek voter support, contestants must be free to campaign, including through online paid advertisements. When it comes to regulating political and campaign advertising, several key principles must be heeded:

- All fundamental rights must be respected, including the right to the freedoms of expression and to form and hold opinions;
- Safeguarding equality of opportunities and maintaining a fair electoral process requires ensuring a level playing field and protecting it from capture by particular interests;
- Regulation must ensure transparency and enhance accountability to allow voters to make informed choices; and
- Voters' privacy rights must be respected at all times, an aspect that became particularly relevant with the emergence of online advertising.

Generally, rules that govern political advertising online should match or mirror the regulation of traditional forms of campaigning. To ensure transparency and equitable opportunities, frameworks for political advertising should contain donation limits, including in-kind contributions, and spending on ads on social networks should be subject to the overall expenditure caps, reporting and disclosure requirements, while oversight and sanctioning mechanisms should also extend to advertising on social networks. As in the non-digital world, online political advertising should be subject to a labelling requirement that, among others, should establish clear rules for the identification of its sponsors.

Third-party and 'political issue' campaigning has become increasingly relevant online. The online environment may be particularly conducive to third-party activism because of the decentralized nature of online communication and the ease with which large sectors of the electorate can be reached at a relatively low cost. Third-party or 'political issue' campaigning should be subject to the same transparency and accountability principles as traditional forms of campaigning.

A significant matter in this debate is the often-blurred line between information produced as 'organic content' and advertising. While the former is protected under freedom of expression and should not be regulated except in extraordinarily justified cases, the latter may and, in accordance with international standards, should be subject to transparency rules. Although approaches to political and campaign advertising vary, most OSCE participating States define it with reference to the question of whether or not the material or messages were paid-for, their volume, reach and frequency (i.e., systematic

80 For comprehensive ODIHR methodology on party and campaign financing, see ODIHR's Handbook for the Observation of Campaign Finance and the Guidelines on Political Party Regulation.

distribution), as well as their intended aim and whether they are intended to bolster or diminish support for given political options.

However in some cases, election stakeholders may choose to use social networks to spread what may seem like 'organic content' messages of support for or criticism of contestants. When this takes place in an organized manner, it may give rise to questions about whether such efforts should be treated as dissemination of 'organic content' or advertising. While this is not unique to social networks, it is often more pronounced there given the opportunities for amplification, wider reach and ease with which posts can be disseminated.

In light of the wide range of technical possibilities offered by the Internet and social networks, various stakeholders may be able to reach specific groups of voters with 'organic' or paid content thanks to personal data gathered on users by the big-tech firms or other actors, including companies specialized in data brokering.[81] While these so-called (micro)targeting techniques do not necessarily violate international standards, there are increasing regulatory attempts to ensure that voters are informed if what they see online is paid-for and that they are being specifically singled out, including why and by whom. Similarly, the so-called 'boosting' of content, which artificially increases its public reach at cost, blurs the line between the provision of information and campaigning. There are also growing concerns that algorithms may privilege specific categories of content, thus ultimately distorting the level playing field in election campaigns. The data protection aspect is closely related to political and campaign advertising, as well as to overall content creation, amplification and dissemination, especially in connection with the so-called disinformation campaigns, elaborated later in the Guidelines.

a. Responses to Online Advertising

In recent years, concerns have been voiced by many stakeholders that online political and campaign advertising is serving to distort the level-playing field and facilitate undue advantage for some electoral contestants. These concerns have increased the need for fully transparent and accountable online political advertising, including as pertains to its cost and sponsorship, limits on donations and the role of third-party or 'political issue' campaigning on social networks. Different paid campaigning techniques, including the (micro)targeting of voters, are increasingly subject to regulation by national or supranational actors, as well as to monitoring by civil society organizations.

81 Campaign and political (micro)targeting usually consists of collecting personal data, using that data to identify groups of voters that share common interests or views and are likely susceptible to a certain message, and sending specifically designed or tailored messages to these groups.

i. State Responses

Many OSCE participating States addressed the growing prevalence of online campaigning by enhancing transparency with respect to campaign finance. In doing so, they have either implicitly relied on existing frameworks that govern traditional advertising or devised new regulations specific to the online domain.

As noted above, regulatory models in OSCE participating States vary significantly. While some have general bans or limit political advertising in broadcast media and extend such restrictions to online campaigning, others have prohibitions that apply only partially to the Internet. In line with good practice, a growing number of OSCE participating States where online campaigning is permitted, require that ads are explicitly labelled as such, similar to outdoor campaign materials or commercials in traditional media. Contestants are also obliged to report their online expenses in an analogous manner to their offline spending. To further enhance transparency, in some States newly introduced legislation mandates platforms to publish advertising rates before the start of the campaign and/or report or make transparent disaggregated income from selling political ads.

To address third-party and 'political issue' campaigning, some OSCE participating States introduced more expansive regulation, requiring the disclosure of information about sponsors of all politically relevant ads. In other States, existing rules were expanded to all content pertaining 'to a debate of general interest', thus ensuring that they capture a breadth of political outreach. Overall, practice has shown that it is precisely in the area of third-party and 'political issue' campaigning, as well as the targeting of voters on social networks that the application of rules developed for campaigning in traditional media is least effective. A number of countries have increasingly recognized these deficits, and there is a growing body of regulation aimed specifically at the online domain, with the goal of injecting transparency into political advertising.

ii. Big-Tech Companies

Having come under increased pressure from users and in light of growing scrutiny by governments, some big-tech companies have started to introduce measures aimed at bolstering transparency in online political and campaign advertising and some platforms have withdrawn from political advertising. While platforms have begun to confirm the identity of donors and advertisers and disclose the amounts they contributed, many shortcomings, such as the verification of sponsors through an imperfect system of self-categorization, remain. Importantly, some newly introduced measures addressed aspects of paid political content, but they did not illuminate the opaque practices of (micro)targeting and content 'boosting' and, currently, the big-tech have an uneven approach across different

markets. Moreover, some platforms are also less open when it comes to disclosing information on third-party or 'political issue' campaigning.[82]

Facebook was first to establish an advertisements library. Although this contributed to the overall transparency in political advertising, measures are implemented unevenly across different countries. Moreover, downloading data from *Facebook's* interface has been unwieldy for some users. Different libraries aggregate data in dissimilar 'units' (e.g., different blocks of time) that frequently do not correspond to campaign finance reporting timeframes and, in many cases, the amounts paid are listed in wide 'bands' (e.g., EUR 500-4,999) thus not allowing for reasonable estimates of the overall expenses. *Google* also launched a global ad library for its platforms, and the rollout of transparency measures was similarly uneven. Moreover, the company did not institute the same level of transparency for third-party or 'political issue' ads, which further limited the effectiveness of these measures. Positively, on (micro)targeting, *Google* introduced measures to limit the ability of non-commercial advertisers to obtain data on specific categories of users and disallowed advertisers from making verifiably false claims. The *Google* ad library includes banned ads, thus positively enhancing transparency. In 2019, *Twitter* decided to no longer permit political advertising on its platform.

iii. International Community Efforts

Although regulation of election campaigns is the purview of individual OSCE participating States, international actors have recognized the importance of transparency in political advertising and, in certain respects, took the lead in addressing some of the challenges outlined above. As elaborated in the previous section, most intergovernmental organizations' initiatives that addressed aspects related to tackling manipulative content and data protection also included measures for enhanced transparency in party and election funding.

The EU is at the forefront of international efforts to address challenges stemming from political and campaign advertising on the Internet. The EU Digital Services Act Package and European Democracy Action Plan focus, among other things, on aspects related to political advertising online.[83] The package of measures to secure free and fair elections for the European Parliament provides recommendations to the Member States and political parties to ensure greater transparency in political communication. **The Council of Europe** has framed the debate on political advertising in terms of fundamental rights, recognizing an inherent link to the freedom of expression. The European Court of Human Rights adopted broad interpretation of the ECHR

82 Election observers, the academic community and other stakeholders expressed criticism towards the efficacy of big-tech companies in the implementation of transparency measures in relation to a lack of standardized data and proper labeling of advertisements and sponsors, limited search functionality and interfaces of ad libraries as well as towards the inconsistent or incompatible time periods in which data was published compared to election campaign periods in which contestants often are required to disclose their financial activities.

83 See the EU Digital Services Act Package and European Democracy Action Plan.

on political advertising, which includes paid advertisements on matters of public interest, including those promoted by civil society and campaign groups. The Court considers that under the ECHR, publishing information "with a view to influence voters" must be treated as an exercise of freedom of expression, regardless of whether it was paid for or not. [84]

iv. Civil Society Initiatives

In many OSCE participating States, civil society organizations are increasingly active in advocating for regulation and greater transparency of political advertising online, including during election campaign periods. Having long-term activities and being more familiar with the country-specific contexts, citizen observer groups are especially important in providing contextual information, highlighting third-party and 'political issue' campaigning and noting instances of (micro)targeting of voters. Beyond advocacy, civil society initiatives are increasingly engaged in monitoring political advertising on social networks, and are particularly well-placed to assess whether reporting requirements and oversight measures are correctly implemented and effective overall. International networking among domestic civil society organizations has also served to increase the capacity of some groups and helped maximize the results of their work despite limited resources.

3.3 DATA PRIVACY PROTECTION

Until recently private data regimes were not a core interest of international observers. Traditionally, aspects of personal and data privacy protection in elections were mostly discussed in the context of voter registration.[85] However, with the emergence of social networks the protection of voters private data become particularly relevant. The protection of the right to data privacy is enshrined in many regional instruments, including the OSCE Copenhagen Document.[86] In most OSCE participating States, contestants are able to access the voter list to verify it is accurate, up-to-date and complete, and in some States the voter lists are used for campaigning and creating election strategies. Nevertheless, the use and exploitation of voter data for campaigning purposes remains a controversial topic.

84 The European Court of Human Rights delivered what some have described as divergent rulings in two cases involving bans on political advertising on broadcast media, underlining the limited certainty as to how proportionate limitations on free speech in political advertising could be set, and highlighting the essential role of country-specific contexts. The rulings also indicated that while free speech is privileged under the ECHR, in certain circumstances the Court may accept that some restrictions are consistent with the aim of protecting freedom of expression. See 2009 TV Vest and Rogaland Pensioners Party vs Norway and 2013 Animal Defenders International vs the United Kingdom.

85 Personal data often are defined as information that relates to an identified or identifiable individual.

86 The 1990 OSCE Copenhagen Document requires States to ensure access to information and protection of privacy.

In line with international standards, the conditions under which voter data may be obtained and the purpose of its use should be spelled out in the law and further regulated in secondary legislation. The absence of clear regulation and procedures for handling data can potentially expose voters to unsolicited communication, be it in the form of free campaigning or paid political advertising. The abuse of voter data can negatively affect the integrity of the process by providing contestants with information on voters' preferences and may give undue advantage to some contestants. In more extreme cases, such instances can make voters vulnerable to pressure, intimidation or manipulation.

When subscribing to social networks, most often routinely by accepting the terms of use provided by social networks, voters expose and make available to different private companies, such as big-techs, data brokers or political and state actors, a wide range of their personal data, which are used of variety of business and political purposes. As such personal data has become increasingly commoditized, they are often used for political and election campaigns. Given the sensitivities involved, data collection, storage, processing and use should be subject to stringent regulation and oversight. In general, the key standards for personal data protection require lawfulness, transparency, fairness, limitation on the purpose of the use of data, data minimization, accuracy, storage limitation, adequate security safeguards and accountability of those that are given access to voters' data.

Personal data in the context of election campaigns are also used for so-called **'profiling' and for targeted campaigning and advertising.** 'Profiling' and targeted advertising may not necessarily be an issue if voters are aware that they are subject to tailored adverts but becomes a problem when it is used to manipulate voters, such as segregating certain categories of voters for political campaigning. For instance, undecided voters can be addressed via tailored political messages to their personal attitudes or refused access to particular information, goods or services.

Many OSCE participating States have or increasingly are introducing privacy and data protection regimes, applicable in the context of election campaigning, including by contestants and third-parties. Provisions should ensure that voter privacy is meaningfully protected, with regulations clearly spelling out who and on what terms may access voter data. Moreover, political parties and candidates should have their own policies ensuring that private data is treated in compliance with international standards. Regulators should be independent and sufficiently resourced to conduct their work, while also having the capacity and be endowed with enforcement/sanctioning powers to fulfil their role efficiently.[87]

While the big-tech firms are well-placed to collect troves of sensitive data about their users, it is widely recognized that strict rules must define what kind of information they may gather and how it should be handled. It is important that users themselves are informed about what data is aggregated and who can access it. They should always have the right to give or withdraw their consent when it comes to the collection, storage and

87 Most often, the legislation for data protection provides voters with the right to be informed, the right of access, the right of rectification, the right of erasure, right to restrict processing and the right to object.

processing of their data. By the same token, access to data for legitimate purposes on terms that comply with international standards should be equal for all contestants.

One of the first international initiatives, in response to the emerging information technologies and the need for protection of personal data is the **Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108).** [88] The Convention 108 applies to all data processing carried out by the private and public sectors and protects individuals against abuse that may accompany the processing of personal data, including trans-border data flows. Also relevant for some parts of the OSCE region, are the EU initiatives that, to date, are the most detailed and comprehensive regulation and protection of private data. The relevant EU initiatives include the **General Data Protection Regulation (GDPR) framework, European Data Protection Board, and the voluntary EU Code of Practice on Disinformation.** The GDPR establishes strict rules based on individual consent for the collection and processing of personal data. It also places limitations on the use of (micro)targeting. The document lists a number of concerns related to online (micro)targeting, including the recognition that it creates possibilities for communication in "non-transparent ways" and may involve the processing of personal data "unlawfully in the electoral context."[89] A number of civil society organizations have also addressed aspects of the use of personal data for election and campaign purposes. Some of these initiatives have global reach and their initiatives have influenced different governments and intergovernmental organizations to adopt legislation and regulations for data protection, including for election contexts.[90]

88 The 1981 Council of Europe Convention 108 is the only legally binding international instrument in the data protection. See also the Council of Europe dedicated website on data protection. The 2018 modernized Convention 108 (also known as Convention 108+) reaffirmed the principles enshrined in the original Convention 108 and introduced additional safeguards for data protection, "to be applied to the new realities of the on-line world."

89 See EU 2016 General Data Protection Regulation (GDPR), European Data Protection Board, Code of Practice on Disinformation and the EU Agency for Fundamental Rights 2018 Handbook on European data protection law.

90 See the Privacy International 2019 Technology, data and elections: A 'checklist' on the election cycle.

4.
ODIHR's APPROACH to OBSERVATION and ASSESSMENT of ELECTION CAMPAIGNING on SOCIAL NETWORKS

This part of the Guidelines elaborates on the connection of the key elements of campaigning on social networks to the general election campaign and ODIHR's approach to observation and assessment of these aspects.

ODIHR observes campaigning on social networks in a manner similar to the observation of the general campaign. ODIHR observers look at the legal framework related to campaigning in general and specifically on social networks, the online activities of the electoral contestants and the involvement of other relevant stakeholders, and the financial and advertising aspects of the electoral campaign. Due to its limited resources and relatively short periods for observation, ODIHR observers assess only the legal and institutional framework related to data privacy protection issues. ODIHR observers are not in a position to fully monitor, evaluate or numerically determine the level of campaign activity and engagement of contestants on social networks, or the accuracy of the reported funds used for advertising on social networks. While campaign finance activities and data protection related aspects do not always coincide with the period of an observation activity, ODIHR observers can still collect sufficient information based on direct observations and meetings with interlocutors to make a well-informed assessment.

4.1 THE NEEDS ASSESSMENT MISSION

Needs assessment missions (NAMs) are deployed by ODIHR to assess the needs for an election observation activity in an OSCE participating State. The NAM's aim is to learn about election stakeholders' confidence in the electoral process, status of election preparations, developments in the legal framework and contestants' plans for campaigning, in terms of strategies and campaign topics. In this context, it is of fundamental importance for the NAM to provide outline of the regulatory framework for campaigning on social networks and to obtain understanding on the use of social networks for political purposes and on the contestants' intention to use them for campaigning. Based on the assessment of these aspects the NAM should recommend adequate composition of the core-team that will reflect the needs of the participating State and the observation activity. In contexts where the campaign merits specific attention, the NAM can recommend deployment of two Political Analysts.

4.2 THE OBSERVATION MISSION

In the context of ODIHR election-related activities, the Political Analyst has the overall responsibility for assessing election campaign, including on social networks. However, several core team members have specific roles in assessing different aspects of the election campaign and when conducting the assessment, the Political Analyst should co-operate with the Media, Legal, or Campaign Finance Analysts and with the Long-Term Observers Co-ordinator. The role of the Political Analyst in the assessment of campaign on social networks is further explained in the next section of the Guidelines.

While social networks should be treated as something that is both unique and distinct from online media, the latter are clearly close to and subject to similar standards and often regulatory requirements as the traditional media. Because online media continue to share many key features with traditional media, the assessment of their role in elections

is best left to Media Analysts, who work with their well-established yet 'living' methodology for qualitative and quantitative observation and analysis. Social networks, on the other hand, mix different types of content, including organic 'posts' and advertising, and are more diffuse, they are better placed in the purview of the Political Analysts who are well equipped to assess the strategies that electoral contestants pursue both offline and on the Internet, and can make better sense of other stakeholders' activities on the platforms, including those whose neutrality is paramount for ensuring respect for the level playing field. At the same time, given the often intermeshed nature of online campaigns on the one hand, and the role of traditional or online media and the phenomenon of 'reposting' of media content on social networks on the other, Political and Media Analysts must work together to obtain the best results.

The Political Analyst will engage closely with several other members of the core-team to observe and assess campaigning on social networks. Because a genuinely democratic campaign is one in which contestants compete on a level playing field and meet existing transparency requirements concerning their campaign income and expenditure, it is important that online campaigning activities, including on social networks, be properly examined with respect to an effective system of reporting and oversight. Given the sometimes blurred line between paid materials and 'systematic' endorsements of contestants through artificial amplification techniques or manual 'reposting' of content on social networks, drawing a clear division between 'advertising' and the provision of (information) 'content' can be challenging. Similarly, 'third party' and/or 'political issue' campaigning are especially prevalent on social networks. It is, therefore, important that on missions with a dedicated Campaign Finance Analyst, the latter work closely with the Political Analyst on aspects pertaining to the financing of online campaigns.

Lastly, in order to address aspects of privacy and data protection when it comes to campaigning on social networks, the Political Analyst must also work side-by-side with the Legal and Election Analysts in the core-team. Together, they will establish whether, and if so, what kind of rules are in place to help protect the privacy of voters. Beyond assessing whether the legal framework for handling private data meets international standards, they should jointly assess the effectiveness of the institutional oversight for protection of private data, as discussed later in the Guidelines.

4.3 DEVELOPING RECOMMENDATIONS

ODIHR observers can provide recommendations for different aspects of the election campaign, including for campaigning on social networks. These recommendations can address the legal framework or its implementation, the conduct of the campaign, the online activity and behavior of electoral contestants and other stakeholders, including paid campaigning, institutional oversight and responses to campaign violations, and the involvement of other actors in the campaign, such as third-parties and big-tech companies.

Given the relatively new, dynamic and ever-evolving field, as well as the complexity of actors involved in this type of campaigning, ODIHR observers should have a diligent and balanced approach when providing recommendations, taking into consideration all relevant aspects and stakeholders. In all cases, recommendations should be supported by concrete findings detailed in the report and references to undertaken commitments, international obligations, standards and good practice.

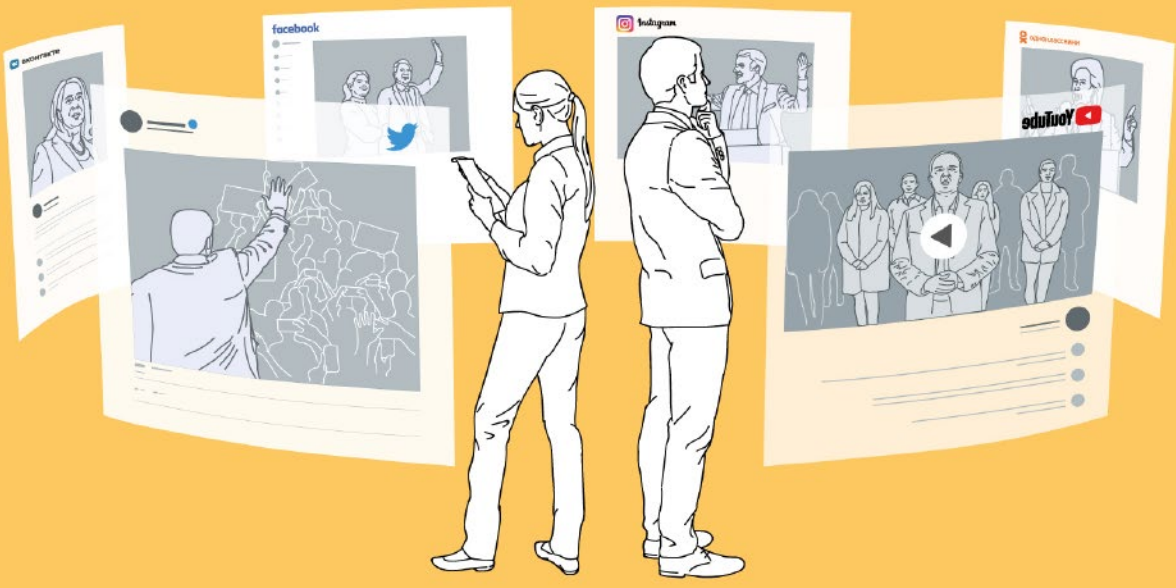
ODIHR campaign-related recommendations are aimed to help participating States in their efforts to provide a free and fair campaign environment with equitable conditions for campaigning for all contestants. While it is difficult to foresee specific issues that might arise during the observation and to provide concrete examples, as well as the fact that election observation is developing in this area, the following suggested points should be taken into consideration as a starting point:

- Respect for fundamental freedoms, including the freedom of expression online and possible limitations to any fundamental freedom can be imposed only in line with relevant international documents;
- Promotion of universal access to Internet and net-neutrality;
- Implementation of the anti-discrimination principle in all aspects of the campaign on social networks;
- Implementation of the principle of transparency, in particular related to advertising on social networks and content moderation by big-tech companies;
- Providing a campaign environment in which election contestants will have equal opportunities to campaign;
- Introducing effective measures for promotion and protection of different underrepresented groups in political life and in elections;
- Designing a comprehensive and effective framework for addressing challenges posed by the spread of manipulative content;
- Promotion of public information and awareness campaigns for building confidence among voters in electoral processes;

- Designing a robust regulatory framework for advertising and private data protection on social networks;
- Strengthening the institutional framework and capacities for oversight of campaign finance and data protection; and
- Providing timely and effective remedy and dissuasive sanctions for campaign-related violations on social networks.[91]

As with providing recommendations on other aspects of the electoral process, ODIHR observers should provide recommendations for the conduct of the election campaign on social networks that are accurate, concrete, implementable and targeted. This means that recommendations address the main shortcomings of the campaign and seek to remedy their underlying causes (accurate); are specific about the end result to be achieved, as well as possible means of arriving at this result (concrete and implementable); and are clear to which stakeholder they are addressed (targeted).

91 The 2020 UN, OSCE and OAS Joint Declaration on Freedom of Expression and Elections in the Digital Age provides a set of recommendations to state and non-state actors on different aspects of the general principles for online campaigning that can be utilized by analysts in the process of drafting recommendations. Importantly, the document should be used for reference and each ODIHR recommendation should be specific for the respective participating State and for the given elections.



5.
THE ROLE of the POLITICAL ANALYST in the OBSERVATION and ASSESSMENT of ELECTION CAMPAIGNING on SOCIAL NETWORKS

This section provides practical guidance for election observers about how to assess and follow campaigns on social networks, and on which aspects the observation should focus. It is essential to note that this topic is relatively new and continues to evolve, which might change approaches for assessments in the future.

As noted above, the Political Analyst is the core-team member with responsibility for assessing the conduct of the election campaign, including on social networks. As with the other aspects of the election process, the assessment of campaigns on social networks should be made against international obligations, commitments, standards and principles, as well as national legislation, and be based on the analysis of the legal framework, meetings with interlocutors and Long-Term Observers (LTO) reports, as well as conclusions drawn from direct observation. Such an approach allows for the triangulation of findings. The wide range of interlocutors that the Political Analyst ordinarily meets during the course of a mission should include new actors, such as organizations that monitor social networks and representatives of social platforms. [92] Although the importance and level of online campaign activity is increasing, many political actors across the OSCE region treat social networks as an additional space for outreach, rather than a substitute for traditional campaigning. As a consequence, Political Analysts should adopt a holistic approach to their observation and assessment of the overall election campaign.

One of the major challenges that Political Analysts face in this area is the massive number of accounts, actors, profiles, pages and posts available online, and determining which of these should be observed. Moreover, each actor can create numerous anonymous, automated or fake accounts employing a myriad of strategies to reach the electorate. Individuals or organizations can campaign on behalf of or against a specific contestant, for instance by buying sponsored content, amplifying campaign messages and deploying 'bots' to help widen their reach. While conducting an assessment, it is important for the Political Analyst to bear in mind that actors without formal links to the contestants' official campaigns can also become active, such as third-parties and 'influencers'. The complexity of working with large volumes of data is further compounded by the velocity with which posts appear and the difficulty of determining their veracity. Finally, enforcement of rules can be especially trying and difficult for assessment because of the Internet's extraterritoriality.

Transparent Observation: ODIHR maintains a high level of transparency in its election-related missions and should publicly announce at the outset its intention to follow online activities of different electoral stakeholders. The mission opening press conference is a good opportunity for such an announcement.

92 The Political Analyst will need to closely co-operate with the Legal Analyst to effectively assess matters that pertain directly to the legal framework and those related to the broader application of fundamental freedoms and human rights, he or she should also work closely with the Media Analyst to assess the campaign on social networks, especially when selecting the sample for observation and on issues related to the freedom of expression.

5.1 ASSESSMENT OF THE LEGAL FRAMEWORK

As a first task, the Political Analyst will need to review and assess the legal framework pertaining to:

1. Provisions related to online campaigning and content regulations;
2. Provisions related to political and campaign advertising; and
3. Together with the Legal Analyst, the privacy and data protection regime relevant to campaigning on social networks.

a. Online Content

A comprehensive assessment of online campaign regulations includes a review of the overall legal framework related to civil and political rights that are prerequisite for genuine competition. In accordance with the ODIHR election observation methodology, the right to freedom of expression and its application are ordinarily dealt with in the assessment of the overall legal framework and regulations related to freedom of media. As a consequence, the Political Analyst should co-operate closely with the Legal and Media Analysts when examining whether the existing legal framework conforms to international standards and ensures access to fundamental freedoms online. The Political Analyst should also determine if the legal framework provides for unimpeded access to social networks and if it contains sufficient guaranties for an online environment free from violence, harassment and intimidation for both voters and contestants.[93]

The Political Analyst should establish if general campaign regulations extend to the online campaign, or whether specific regulations apply. Moreover, the Political Analyst should assess whether regulations provide for the conduct of democratic and competitive election campaigns. To achieve this, the Political Analyst will need to examine if provisions are in place to ensure equal conditions and treatment of electoral contestants, and whether they are being implemented. The Political Analyst should also assess whether any undue limitations on contestants' ability to freely conduct their campaigns exist in the law or in practice. Equally, provisions on the misuse of administrative resources online should be evaluated.

The Political Analyst should review national legislation and regulations for compliance with international obligations, standards and OSCE commitments regarding the distribution of harmful content and speech inciting to hatred and violence, as well as other types of negative rhetoric, manipulative content and disinformation. The Political Analyst should assess whether they have the potential to affect voter ability to make an

93 In addition to the general and election legal frameworks that most often regulate the conduct of election campaigns, specifically for online campaigning, Legal and Political Analysts should consider if there is anti-terrorism, cyber-crime and harassment or anti-disinformation and anti-false news legislation, as well as some specific regulations related to blocking and filtering online content, including intermediary liability regimes.

informed choice and whether the state and/or other actors have taken appropriate action to tackle manipulative content in line with international obligations, standards and principles and OSCE commitments.

Guiding Questions:

- ✓ Does the existing legal framework conform to international standards and ensure access to fundamental freedoms, including freedom of expression?
- ✓ Are there specific laws or regulations governing the conduct of the election campaign online?
- ✓ Do legal provisions ensure diversity, plurality and competitiveness of the campaign?
- ✓ Do all electoral contestants enjoy equal conditions in their access to and while using social networks?
- ✓ Do any contestants face undue limitations or obstacles with regard to the content of their platforms or campaign messages?
- ✓ Have any instances of violence, harassment or intimidation online been observed against a specific group or contestant?
- ✓ Are women or national minority contestants and voters disadvantaged when it comes to exercising their right to exercise fundamental freedoms?
- ✓ Does the existing legal framework offer measures against dangerous or harmful speech, including incitement to hatred?
- ✓ Are social networks held legally liable for content posted on their platforms?
- ✓ Are the criteria for removal clear, consistent and provided for by law? What sanctions are in place for non-compliance? Are there any remedies available?
- ✓ Are there any legal provisions regarding campaign silence online?
- ✓ Are there any regulations regarding publication of opinion/exit polls online?

b. Political and Campaign Advertising

The Political Analyst, in co-operation with the Legal Analyst (or the Campaign Finance Analyst, if deployed), will need to establish whether political and campaign advertising on social networks is regulated and whether campaign finance provisions, such as expenditure limits, reporting requirements, oversight mechanisms and sanctions, are applicable online. Analysts must ascertain whether reporting requirements and other regulations genuinely provide sufficient data for voters to become more informed about the contestants' campaign spending on social networks before they cast their ballot. The absence of regulation and enforcement mechanisms for political advertising on social networks decreases the overall transparency of political and campaign financing.

Regulatory efforts to increase transparency of online political advertising often include a labelling requirement for all campaign materials, as well as disclosure and reporting regulations concerning the expenses, prohibitions on donations from public entities and

foreigners among other restrictions. It is necessary that the Political Analyst assesses both the rules and their uniform implementation. The Political Analyst should also attempt to examine the transparency measures that have been put in place by social network platforms in some OSCE participating States and the level to which they contribute to the overall robustness of the campaign finance framework. It is important to remember that any applicable restrictions on campaigning must be necessary, proportionate and implemented in accordance with the law, which should include precise definitions of offences. Analysts should also establish if the law regulates third-party and 'political issue' campaigning.

Guiding Questions:

- ✓ Is there a regulatory framework in place governing paid political advertising online?
- ✓ Does the legal framework provide for sufficient transparency in online advertising?
- ✓ Does the legal framework provide adequate safeguards and sufficiently mandate transparency for campaign advertising on social networks?
- ✓ Are contestants required to disclose information on expenditures and are campaign finance reports sufficiently detailed to include expenditures on online advertising?
- ✓ Does the legislation regulate online campaigning by third-parties and 'political issue' campaigning? If so how are they enforced?
- ✓ Are there any regulations prohibiting misuse of administrative resources online?
- ✓ Does the legal framework sufficiently regulate the practice of third-party campaigning online?

c. Data Privacy Protection

The Political Analyst, together with the Legal and Election Analyst, should assess whether the right to privacy is legally protected online and in traditional campaigning, as well as in voter-registration and voter-management aspects. Further examination should be made with regard to international obligations that require States to ensure that individual privacy is respected and personal data are used lawfully, only for authorized purposes, and that individuals concerned have both explicitly given their consent, and can withdraw it at any time. The Political Analyst should also inquire during meetings with political parties and candidates if they have policies in place to ensure that private data is handled in ways that comply with international standards. Finally, where voter data is available, the Political Analyst should assess how different actors obtained it, whether voters have consented to its use and whether political parties, candidates and third-parties are able to access information on equal terms.

Legislation should regulate the acquisition, storage, processing and use of data and ensure effective oversight by a competent and independent authority. The mission assessment should include consideration of whether there are specific regulations for the

protection of voter data, as well an examination of the powers of the competent oversight authority (elaborated later in the Guidelines). Data may not be shared with anyone unauthorized to receive, store, process or use it. International standards prescribe that voters be informed about the extent to which their data can be accessed and are being used by state or private actors. In light of an increasing prevalence of (micro)targeting of voters online, there is an emerging agreement that voters should not only be able to identify political ads through labelling or imprint data, but that they also be informed when and why they are being targeted.

Guiding Questions:

- ✓ Is there a data-protection regime in place?
- ✓ Does the legislation adequately safeguard voters' personal data?
- ✓ Does the legislation provide for clear regulations under which electoral contestants can use data from social networks users?
- ✓ Does the legislation provide for effective remedies for misuse of voters private data?
- ✓ Is the practice of (voter) targeting regulated in the law and are rules implemented in practice?
- ✓ Is the privacy and data protection regime applicable in the context of election campaigning?
- ✓ Does it encompass contestants and third-parties?
- ✓ Do political parties and candidates have policies in place to ensure respect for privacy and data protection?
- ✓ Are eligible stakeholders able to access voter data on equal terms?

5.2 OBSERVATION AND ASSESSMENT OF CAMPAIGN ACTIVITIES

In addition to analysis of the legal framework, the Political Analyst should assess the activities and conduct of contestants and other stakeholders' on social networks during the campaign period. As a first step, the Political Analyst will need to map social networks that are relevant to the electoral process, select a limited number of users accounts and establish the extent and purposes for which they are employed in the campaign. The selected accounts should be observed by the mission-created accounts to assess the role played by the election participants, other relevant political actors, such as public institutions or officials, as well as third-parties, including most prominent 'influencers'. The Political Analyst should be able to draw parallels between the field conduct of the campaign and the campaign on social networks, noting the similarities but also specifying any perceptible differences.

For conducting an assessment and observation of campaigning on social networks, the Political Analyst will be supported by at least one national assistant with specific responsibilities and assignments for this task. As in the case of the national assistant who supports the Political Analyst in the observation of traditional campaigning, it is important to remember that national staff, who are direct stakeholders in the election, may face challenges retaining full neutrality or being perceived as neutral, especially when faced with divisive political issues. All mission members are required to abide by the Code of Conduct, but as a function of their exposure to political actors, the Political Analyst and their assistants should take particular care to safeguard impartiality and integrity of the observation activity.

The Political Analyst in the observation and assessment of the online campaign should consider the following aspects:

- **Methods and Strategies:** The Political Analyst will need to establish which platforms, methods, and activities electoral stakeholders engage with when campaigning online. When observing, he or she should consider whether the activity is user-generated or reproduced, for instance by sharing content or links to media articles, whether it focuses on voter mobilization or possibly discourages participation in elections, as well as what type of material is being shared (text, images, videos or a combination thereof). Moreover, observation should include aspects such as whether there is outreach to specific groups of voters, such as young and first-time voters, women, national minorities or persons with disabilities, and, if possible, a determination as to whether the candidates pursue an individualized campaign style or follow a party-centered approach that echoes a central campaign message.

- **Key Campaign Topics:** The Political Analyst should also determine and follow which topics are discussed on social networks and to what extent they mirror those presented in the media and at campaign events. This is important to determine whether the online campaign provides voters with sufficient substance to make an informed choice, and to uncover if there may be aspects of wider public or election-related interest that are or not addressed online or are discussed in online

debates but absent from traditional campaigning. The Political Analyst should establish which are the most salient topics and assess, to the extent possible, which subjects and posts appear to generate the greatest resonance.[94]

- **Tone and Rhetoric:** As with the traditional campaign, the Political Analyst should assess the overall tone, and the style and type of rhetoric used by election stakeholders on social networks. Instances of incitement to violence or hostility, inflammatory rhetoric, dangerous and harmful speech, as well as the use of manipulative content should be noted, including whether it features comments on technical or political aspects of the electoral process or discredits other contestants. The assessment should also establish whether the tone and language used online differs from that found at campaign rallies and other public appearances.

- **Paid Campaign:** The Political Analyst should assess the use of paid advertisements by contestants or other stakeholders, including both those in favour of or against a specific candidate. Following the transparency policies instituted by the big-tech companies in some countries, the financial activities of the political parties, candidates and other election stakeholders are included in the so-called ads libraries or the paid content is labeled as such. He or she should determine if they are sufficiently transparent to allow viewers to identify their sponsors. The observation and assessment of paid content and activity is elaborated further below.

The selection of 'what' and 'who' to follow on social networks needs to be based on resources that are at the disposal of the Political Analyst. Limited time and staff available during the mission on the one hand, and the wealth of material available on the Internet on the other, means Analysts need to concentrate their efforts on manageable samples. Any analysis and assessment should follow the fundamental principles of ODIHR election observation methodology and rely on a systematic, consistent and reliable approach based on direct observations. The Political Analyst's focus should therefore fall on a strictly defined time period, often from when the Political Analyst is able to get the observation of online campaigning up and running through the duration of the campaign or the general election period, and a clearly defined sample. Rather than analyzing individual posts or reporting quantitatively, it is important to capture the main trends across various platforms and produce a qualitative assessment reflecting campaign strategies, tone, language and topics, and to assess compliance and enforcement of campaign regulations, as well as noting any potential breaches, including misuse of administrative resources.

94 As noted above, due to the decentralized nature of social networks and content that is user-generated, which allows voters to co-shape agendas in the online domain, in some cases the range of topics discussed online is wider than those presented in traditional media, which are subject of editorial policies and stricter regulation. The Political and Media Analysts should determine jointly if some topics of public interest are censored from the political discourse, identify the reasons why this may be the case, and depending on the context, reflect this in the Campaign Environment or Media sections of the mission report.

a. Selection of Platforms

The Political Analyst will need to identify which social networks are most widely used during the election process.[95] The decision about which platforms to be followed should be context-specific and take into account other relevant international or domestic organization reports, meetings with interlocutors, and not exclusively on the number of users or followers and reach of accounts. The selection of platforms should also reflect the outreach, including average user age, language and ethnic diversity. In most OSCE participating *States, Facebook* and *YouTube* are the most common social networks used for political communication and campaign advertising, while *Twitter* is generally utilized by politicians and opinion makers to craft political narratives. Instagram is often employed to feature campaign messages, event stills and soundbites from speeches, but also daily posts and written narratives. Depending on the country or region, the Political Analyst might find that other social networks are more relevant, such as *VKontakte*, and *Odnoklasniki*.

Guiding Questions:

- ✓ Which platforms are most widely used by voters, election contestants and other political actors and stakeholders?
- ✓ Which platforms are most popular for political content and news?
- ✓ How do political actors use different platforms during the campaign?
- ✓ Are there any platforms known for the use of disinformation?
- ✓ Are there any platforms on which specific groups of voters are more or less likely to be active (or excluded) such as national or language minorities and young voters?

b. Selection of Accounts

After the selection of platforms, the Political Analyst will have to decide on the range of accounts to follow. To this end, a list of user-accounts of relevant parties, candidates, 'influencers' and state institutions should be drawn based on several different platforms. Importantly, because popular actors in the digital realm can change rapidly, the Political Analyst should maintain a certain degree of flexibility and include new accounts that rise to prominence in the course of the campaign. As with the process of selecting platforms, the accounts sample should be as widely representative as possible and reflect the country's political, socio-economic, regional, ethnic and language diversity. Such a selection should aim to reveal general trends that characterize the online campaign environment and offer a solid basis for assessment.

If in a given context there is only limited online activity and mission resources allow, in order to broaden findings, it can be beneficial for parliamentary and local elections to

95 There are several analytic and metric sources for Internet traffic that can be of help for the Political Analyst when selecting which platforms should be observed in a specific country. Some of these include: www.similarweb.com; www.alexa.com; and www.statista.com.

identify key candidates and political actors, beyond those most prominent at the national level, at the local and regional level and include their accounts in the observation. It may be useful to assess the campaign tools they use and inquire whether their strategies and messages are similar to those at the national level or display unique trends. The LTOs can be particularly useful in identifying these regional stakeholders. However, it is important to remember that while the LTOs can elucidate certain regional developments on social networks, data collection and assessment should be completed by the Political Analyst.

To be consistent with the key principles of the ODIHR election observation methodology, including the veracity of findings, the Political Analyst should only include in the sample and label correctly authentic user accounts. There may be multiple social network accounts that use the same or similar names of different electoral stakeholders – if their authenticity is disputable, they should not be simply assumed to belong to the alleged stakeholders. If there are 'fake' accounts that attract significant public attention, they can be included in the analysis and assessed separately, especially with a view to the spread of harmful or manipulative content. The principles of the Code of Conduct for ODIHR observers need to be adhered to and impartiality must be maintained at all times when observing social networks. While the accounts of politicians, parties and other actors are being followed, mission members must refrain from sharing, commenting or any other activity that might compromise the integrity of the election-related activity.

i. Electoral Contestants

In addition to the electorate, candidates and political parties are key stakeholders in electoral contests. The Political Analyst should naturally follow their profiles and accounts. For parliamentary or local elections where following all candidates is not possible, to maintain impartiality and objectivity, the selected accounts should offer a representative sample of contestants across the political spectrum, including those who support the government, the opposition, candidates nominated by formations represented in parliament, and those without parliamentary seats, as well as parties or candidates that represent different national or religious minorities. It is also important to follow accounts that belong to those representing women candidates, persons with disabilities and other vulnerable groups. In case the number of candidates is high, the Political Analyst needs to draw up a narrower list and decide to follow contestants with particularly high visibility.[96] However, such a pre-selection should be proportional and not made to the detriment of contestants that represent smaller political entities or minority groups.

96 During parliamentary or local elections, the selection of accounts can be an especially challenging task given the number of candidates. In some cases, the Political Analyst may limit observation to the accounts of the leading nominating parties and their leaders, as well as candidates who are exceptionally active online.

ii. State Institutions and other Political Actors

In addition to direct participants in the election, the Political Analyst should consider following the online activities of other political stakeholders, including parties that did not field any candidates or state, local or other public institutions relevant to the electoral process and campaign. The selection should be similarly context-specific and can include the election management body (EMB), the government, prime-minister or the president's accounts. Moreover, some ministries, judicial authorities or the ombudsperson can be included in observation. The Political Analyst will need to examine whether any of these actors may be using social networks for campaigning purposes. It is especially important to observe whether administrative resources are being misused for online campaigning, or alternatively, to assess whether 'content' featuring on these institutions' pages may be implicitly giving undue advantage to some contestants. It is therefore important, to the extent possible, to also follow the online activities of high-ranking local or regional public officials, including governors or mayors, and to develop a good understanding of their role, if any, in the campaign.

iii. Other Stakeholders

To obtain a comprehensive overview of the online campaign, it is important for the Political Analyst to consider following a wider spectrum of election stakeholders. This does not need to entail a fixed, predetermined set of actors, and the Political Analyst should maintain a certain degree of flexibility. Any selection will depend on the country-specific context – the actors may include civil society organizations, activists and 'influencers', as well as any other third-parties engaged in the campaign. Overall, the Political Analyst should strive to determine the context and motives for the involvement of third-parties, and if possible, to establish if their activities are or should be subject to campaign finance regulations. In this context, the observation may include opinion makers, journalists, academics, religious bodies or their high-ranking representatives and trade-unions, as well as organizations representing youth, gender or national minorities.

A comprehensive list of actors and accounts can be established with the support of national assistants, who should have a good understanding of the political and electoral environment. The selection may also be made in consultation with the Media Analyst. The process can also draw on information gathered during meetings with interlocutors and discussions with media or political experts. When contextualizing and interpreting the gathered data, it is also advisable for the Political Analyst to meet with civil society organizations, domestic monitoring groups and local organizations that focus on social networks.

c. Collecting Information

Information from public posts found on selected accounts should be systematically collected and methodologically organized. For this purpose, the Political Analyst should develop a database to maintain a record of different elements of their observation. The timeframe for observation should include the campaign period, often from when the Political Analyst is able to get the observation of online campaigning up and running through the duration of the campaign or the general election period or after the candidates had been nominated.

Based on the data collected from social networks, the Political Analyst should be able to determine the similarities between the online and traditional forms of campaigning and to point to any significant differences. The database should also provide sufficient information for the Political Analyst to draw conclusions about the methods and strategies used for campaigning on social networks, including the nature of content (free 'organic' or paid, user-generated or shared, for or against voter participation, etc.) and type (text, images, videos or a combination thereof). Moreover, the analysis should include aspects related to outreach to specific groups of voters, such as youth, first-time voters, women or national minorities. If the scope and timeframe of the mission allows, it might be useful to assess whether campaign strategies have changed during the campaign, for instance in the aftermath of a significant event.

To develop a good understanding of outreach strategies, the Political Analyst should pay attention to the volume and scale of activities, which may include the number of posts, paid advertisements, users' comments and reactions. While rigorous enumeration of these details is not expected and the Political Analyst should rather strive for a qualitative assessment, some basic numerical trends could be established. These can include broad references to the frequency of posts by contestants, and reactions and comments from their followers. The activities of other political actors, state or public institutions, but also third-parties, can be analyzed qualitatively. Incidents related to the misuse of administrative resources, 'hate speech', negative rhetoric or other manipulative content should be separately analyzed, on a case-by-case basis, and supported with more detailed descriptions.[97]

If the time and other resources permit, the Political Analyst could go beyond the above-mentioned actor-based approach and conduct keyword searches, including terms that are thought or expected to be important topics in the campaign. To facilitate this, the Political Analyst must identify relevant phrases, slogans and hashtags (e.g., #referendum2018) that are being or are likely to be used to designate content that is election or campaign related.

97 Observations of online incidents, including those related to 'hate speech', incitement to violence, or other manipulative content should be properly recorded, possibly with screenshots, and archived.

As noted earlier, the Political Analyst should pay particular attention to the treatment and rhetoric used towards different underrepresented groups. For instance, cyber violence against women is increasingly present during campaign periods.[98] It can be manifested through harassment, bullying, mobbing, posting of explicit visual material, posting and sharing violent content, death threats, and use of sexual or insulting comments and derogatory/altered images or videos (deep-fake). Due to the possibility of users anonymity and social networks decentralized nature, these acts of violence can easily cross national borders and have effects that are difficult to tackle or redress. Political Analysts should closely observe the presence of this in the campaign, towards contestants but also women voters and supporters and assess their impact on the conduct of the election campaign, as well as the institutional and societal responses to these negative practices.[99] Moreover, the Political Analyst can take note and report on some positive measures and initiatives taken by States, political parties and electoral contests, civil society or social networks that aim to address and tackle online violence against women. In addition to awareness raising campaigns for prevention of violence against women, mostly done in co-operation with civil society and international organizations, some initiatives by social networks include: enforcing so-called 'Community Standards' related to protection of women; introduction of additional privacy and security mechanisms; and development of automated technology for detecting and removing content that includes this kind of violence.

98 See the 2017 UN Women and UNDP Guide for Preventing Violence Against Women in Elections. The Guide states that, "violence against women in political life, including in and beyond elections, is any act of, or threat of, gender-based violence, resulting in physical, sexual, psychological harm or suffering to women, that prevents them from exercising and realizing their political rights, whether in public or private spaces, including the right to vote and hold public office, to vote in secret and to freely campaign, to associate and assemble, and to enjoy freedom of opinion and expression. Such violence can be perpetrated by a family member, community member and/or by the State."

99 See OSCE Ministerial Council Decision on Preventing and Combating Violence Against Women No. 4/18, which calls on participating States to, "encourage all relevant actors [...] to contribute to preventing and combating all forms of violence against women, including those engaged in professional activities with public exposure and/or in the interest of society." See also Council of Europe Committee of Ministers Recommendation (2019)1 on preventing and combating sexism.

5.3 OBSERVATION AND ASSESSMENT OF POLITICAL AND CAMPAIGN ADVERTISING

Several aspects of campaign advertising on social networks merit particular attention, such as:

1. Respect for the principle of transparency, including the amount of publicly available data on advertising on social networks by electoral contestants, political parties and big-tech companies;
2. Reporting requirements by contestants or other stakeholders on their online advertising activities; and
3. Involvement of different actors in the campaign, including third-parties, that do not purport to be connected to the contestants.

a. Transparency of Advertising

Following an assessment of the legal framework, the Political Analyst or the Campaign Finance Analyst, if deployed should assess the implementation of transparency-enhancing provisions during election campaigns on social networks in practice. Namely, they should establish whether campaign content is clearly labeled to indicate who is promoting the advertisement and if information concerning the revenue incurred by the big-tech companies from political and election campaigns is publicly available. Moreover, with a view to the level playing field, the Political Analyst should assess if electoral contestants have equal access to campaign on social networks on a non-discriminatory basis and equitable opportunities to campaign (e.g., if there are differences in advertising prices).[100]

In the face of growing concerns about malicious use of social networks in election campaigns, the big-tech firms have started to introduce more transparency to political advertising. The measures include limitations on who can place political ads, the submission of advertisers to more stringent verification procedures and public disclosure of their identities. Most visibly, some big-tech companies started to label paid political ads and made aggregated information about them more easily accessible online. In some OSCE participating States, platforms' ad libraries have become an increasingly important resource for interested actors, such as media election observers and civil society. Importantly, Political Analysts should endeavour to determine if the platforms have ensured appropriate separation between political ads and other forms of sponsored political and election-related content.

100 In line with international standards and commitments, to have equitable opportunities to campaign electoral contestants should be given equivalent rates when using traditional forms of campaigning, such as billboards, posters and display of other printed material and when campaigning in the broadcasting media. However, for online campaigning most of the big-tech companies are using advertising 'auctioning' or a bidding system that often results in different rates for electoral contestants.

To support its overall assessment, the Political Analyst may use aggregation tools provided by the platforms, such as ad libraries, to identify which political parties or candidates are most active, enjoy the most attention or have spent the highest amount of money on social networks. The ad libraries may also help the Political Analyst to better ascertain the tone of the campaign, and seek out elements of negative campaigning or aspects deemed to violate the law or international standards, including incitement and harmful speech. The Political Analyst should aim to verify whether information that is reflected in the ad libraries corresponds to the amounts that contestants report to the oversight authority. Some of the available tools are elaborated further below.

Due to the large amount of online paid content and (micro)targeting techniques used by big-tech companies and other entities, the Political Analyst might not be in a position to observe and assess all of the ads produced by electoral contestants or third-parties. Moreover, what the different platforms include in their ad libraries varies from one OSCE participating State to another. For instance, in some countries only ads placed by registered contestants are listed, while in others third-party and 'political issue' ads are also featured. Many platforms are collecting and making available some data on the (micro) targeting' of voters or 'boosting' of content, which may be akin to advertising.

Guiding Questions:

- ✓ Is political and campaign advertising clearly labeled?
- ✓ Do electoral contestants have equal opportunities to campaign, i.e., are prices for advertising are equal for all contestants?
- ✓ Are prices publicly available?
- ✓ Are there any (micro)targeting techniques used by big-tech companies, electoral contestants and other stakeholders and are voters are informed?
- ✓ How efficient are efforts of the big-tech companies in addressing malpractice in the area of political and/or campaign advertising on social networks?
- ✓ Are transparency-enhancing tools, such as ad libraries created by the big-tech, helping the overall transparency of political and campaign financing?

b. Reporting Requirements

Reporting and disclosure of campaign finances are important measures to ensure accountability and transparency, including on social networks.[101] In most OSCE participating States, election contestants are obliged to disclose their campaign expenses. It is important that, among others, parties and candidates also account for their advertising

101 ODIHR Handbook for the Observation of Campaign Finance notes that campaign finance reporting is the key policy instrument for ensuring that electoral contestants comply with campaign finance legislation in a systematic and comprehensive manner. Such legislation will generally prescribe the information political parties and candidates must submit about their campaign contributions and expenditures, and when and how those reports must be submitted. This information helps the oversight body to assess whether the parties and candidates have complied with the law.

on social networks. This means that their campaign finance reports should be sufficiently detailed to reflect spending on online campaigning. The mission should assess whether the figures included in the reports match the approximate number, frequency and geographic reach of campaign advertisements as observed during the mission and as reported by the contestants and third-parties in social networks' libraries, if available. The mission should also assess whether expenses are transparently reflected in the contestants' campaign finance reports, and establish how detailed and timely these reports are.

The Political Analyst should carefully assess the balance between public disclosure and protection of personal data. Generally, information that must be disclosed should enable the public to identify a donor, the amount of the contribution and when it was made. Election contestants' financial reports should include in-kind contributions for online campaigning; the Political Analyst should assess how such donations are valued and whether transparency standards apply equally to all contestants.

Guiding Questions:

- ✓ Are electoral contestants and third-parties involved in the campaign required to report on their online campaign activities?
- ✓ Are these reports published in a timely manner?
- ✓ Are legal provisions implemented in a consistent and effective way?
- ✓ Have the big-tech companies implemented some measures for increased transparency, such as creation of ads libraries?
- ✓ Are social networking platforms fulfilling their reporting requirements?
- ✓ What kind of data and information on campaign and political advertising during the campaign period can be drawn from the platforms?
- ✓ Do the amounts reported by contestants and third-parties involved in the campaign to the oversight authorities match those published by social networks platforms?

c. Third-Party Campaigning

Assessing third-party involvement and 'political issue' advertising on social networks can be challenging. As in the traditional forms of campaigning, electoral agitation is not in the exclusive purview of political parties and candidates. Groups and individuals can actively promote contestants directly or by profiling issues that resonate well with the electorate and may be linked to specific political options or candidates.

Third-party and 'political issue' advertising can be positive in election campaigning, signaling wider societal engagement in politics and elections. Interest groups and civil society organizations can mobilize to become more active, facilitating a more pluralistic and inclusive process. In some contexts, non-contestants may also be able to voice their

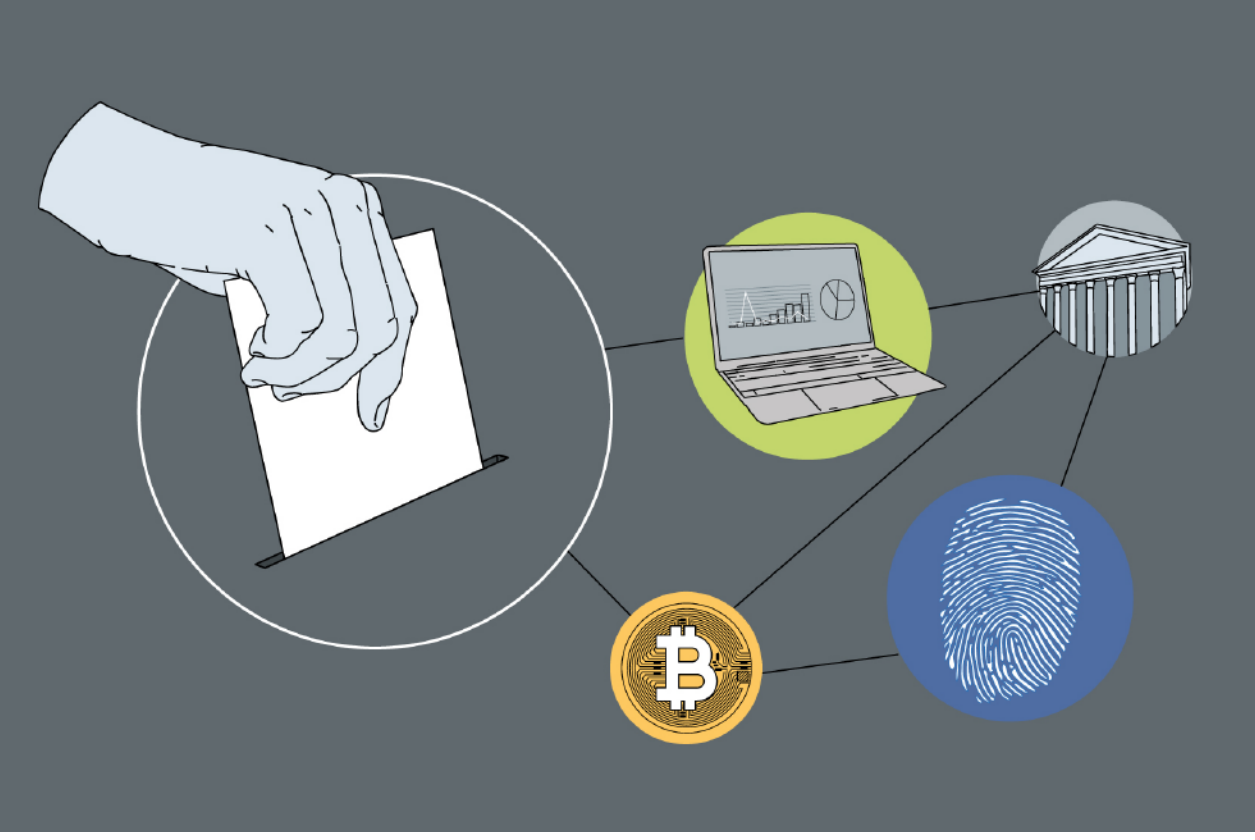
messages, including not only to advocate voter participation, but to also call for boycotts of elections they deem to be illegitimate.

The downside of third-party campaigns in the online context is that actors can use less transparent methods to support candidacies or enhance the messages of specific contestants. When not sufficiently regulated, third-party or 'political issue' ads may allow campaigners to bypass spending limits. It is important for the Political Analyst to establish whether third-party and 'political issue' campaigning are regulated in a manner analogous to that of registered contestants: whether transparency is provided for in the law and ensured in practice, including with regard to donor and donation disclosure, spending amounts and respect for limits, as well as reporting, oversight and possible sanctions.

Finally, the Political Analyst should also seek to identify any cases of hidden third-party or 'political issue' campaigning, which are often linked to negative campaigning and manipulative content (e.g., about candidates) or more general attempts to delegitimize the process. This can be especially dangerous when rather than being clearly labelled, third-party sponsored content is made to appear organic and may therefore bypass campaign finance regulations. While this can be challenging, the Political Analyst should endeavor to determine and report how widespread this kind of behaviour is on social networks. Finally, the Political Analyst should consider the different forms that agitation may take, including endorsements by key 'influencers', and assess whether the authorities are taking steps to ensure that such cases respect the level playing field and are accounted for.

Guiding Questions:

- ✓ Is third-party advertising prevalent on social networks?
- ✓ Are any specific contestants that are benefitting from it?
- ✓ Do platforms make an effort to curb harmful activities in the area of third-party advertising?
- ✓ Are these measures effective and consistent?
- ✓ Does the legal framework satisfactorily regulate the practice of third-party campaigning online, including with a view to campaign finance?
- ✓ Are third-party campaigners required to report to the oversight authorities for their campaign activities?
- ✓ Do social network platforms publish in a transparent and user-friendly manner financial contributions from third-parties?
- ✓ Is the content produced by third-parties clearly marked?



6.
OVERSIGHT

Debates about oversight, effective remedy and sanctions in the area of campaigning on social networks are being shaped alongside the process of emerging regulation of online political content and campaigning. As regulations most often pertain to campaign advertising, campaign finance, opinion polling and campaign silence rules, the oversight responsibility tends to fall on the same institution that has regulatory powers in these areas offline (e.g., the media regulator, EMB or any agency in charge of campaign finance oversight). The Political Analyst should examine the way in which the legal framework governs key aspects of the regulators' work, including their competences and capacities.

In some contexts, the bodies responsible for traditional and online media regulation and oversight have been mandated with powers to oversee social networks. The Political Analyst should co-ordinate with the Media Analyst when meeting with these institutions. They should also assess whether the oversight bodies are politically independent, and yet sufficiently accountable, whether they make decisions in a timely and transparent manner, and whether stakeholders are able to lodge complaints, appeal and seek timely redress with regard to the latter.

With regard to other topics, especially manipulative content or disinformation on social networks, the debate about rightful oversight measures and sanctions remains controversial, as it pits important principles against one another and exacerbates the tension between the voters' right to make an informed choice (free of manipulation of any kind) on the one hand, and the politicians, advertisers and other online actors' freedom of expression on the other.

It is important to note that while the formal oversight power inevitably rests with the regulator or specific supervisory authority, domestic stakeholders, including civil society organizations and media, play an important role holding electoral contestants and other stakeholders accountable. Civil society and citizens observers' statements and media reports can, in some contexts, have a critical impact on public perception of the integrity of elections. Where they have the necessary tools and resources, these actors can provide accurate assessments of key aspects of online campaigning, including with a view to compliance with campaign finance regulations.

6.1 CONTENT OVERSIGHT

At the heart of the debate about content regulation lies the question already identified at the outset, namely whether social networks should be treated like any other (traditional) media and be accountable for what features on their platforms, or rather as mere purveyors of information generated by users, who bear the ultimate responsibility.[102] The ensuing dilemma revolves around the discussion about whether states should regulate and oversee content, which could potentially lead them to restrict online speech, or whether freedom of expression is absolute and the platforms should be left to self-regulate and ultimately adhere to a higher standard of conduct without government intervention.

Having recognized the breadth and depth of responsibility that comes with self-regulation, some of the big-tech companies have introduced internal oversight initiatives.[103] Efforts to regulate the overall functioning of social networks, in some OSCE participating States, have been accompanied by efforts to also regulate online content, thus raising the effectiveness of oversight.[104]

102 It is important to note that even in the latter case, social networks algorithms determine the prioritization of content, i.e., are ultimately involved in at least co-deciding who sees what and when.

103 For example, in 2020 Facebook established an Oversight Board, a body that makes content moderation decisions on its platform – in particular those about appeals for blocked or removed content. In 2021, Twitter launched its own, "community-drive approach to help address misleading information," however, only available for the United States market.

104 In the EU context, the Audiovisual Media Services Directive was adopted in 2018 to establish a regulatory framework for audiovisual content for traditional TV broadcasts and on-demand services, thus constituting an important foray into content regulation of video-sharing platforms. Independent of the EU framework, some OSCE participating States have introduced legislation and mandated bodies responsible for the oversight of traditional media to also oversee and regulate content shared on social networks. Such actions, if implemented arbitrarily and selectively in specific parts of society and without credible methodology, may run counter to the respect for fundamental freedoms and international obligations, standards and commitments for democratic elections.

While oversight can be relatively easily instituted in areas where restrictions on rights and freedoms are clearly established under international law and unambiguously reflected in national law (e.g., as regards incitement to violence, protection of minors or other specific groups of citizens and voters), other less clearly defined aspects, such as defamation, libel and different types of manipulative content, pose a more serious challenge. The regulation of these facets is not only not fully supported by international instruments, but often runs counter to human rights and fundamental freedoms such as the right to freedom of expression and the right to impart and receive information.

Pointing to shortcomings of effective self-regulation by social networks, some governments have sought to curb the spread of 'fake-news' by holding the platforms liable for content, including through fines. Some OSCE participating States have also started to establish agencies tasked with monitoring the online flow of information with the aim of identifying different types of manipulative content and requiring the platforms to remove it. In the absence of specific international standards and weak or ambiguous domestic legislation, the EMBs and other bodies have generally shied away from policing content, in some cases also to the detriment of the principle of transparency, which lies at the heart of the fight against malicious campaign-related practices.

The Political Analyst should be aware that in some OSCE participating States, strides to regulate content may be, in actuality, guided by the aim of inhibiting speech or may lead to stifling speech. Illegitimate censorship of content could inadvertently curb free expression and have a chilling effect on political discourse in general. Restrictive regulations and policing of online speech in a democratic society may set a dangerous precedent and encourage non-democratic regimes to expand censorship. As debates on content regulation and oversight rage, technological developments are also progressing at a rapid pace. Increasingly, the prevalence of manipulative content in campaigns and its growing spread can be especially harmful to women and candidates representing different minority or vulnerable groups, and underlines the urgency of dealing with this phenomenon. The Political Analyst should take note of attempts to regulate content and carefully weigh them against principles, such as the right to freedom of expression and opinion formation without undue interference.

6.2 POLITICAL AND CAMPAIGN ADVERTISING OVERSIGHT

The oversight of campaign advertising normally rests with the institution that oversees political and campaign finance offline, which may be the EMB, judiciary, state audit institution, broadcasting regulator or another specialized body or committee. This institution should have same or similar competences in the field of online campaigning. It is important for the Political Analyst to assess whether the institution is independent and performs its tasks in a neutral manner, possesses the knowhow, technical capacity and resources necessary to meaningfully fulfil the oversight role.

Moreover, the Political Analyst should strive to understand whether the oversight authority effectively monitors paid activities of electoral contestants and other stakeholders and if it has powers to launch investigations and impose sanctions for unreported costs and advertising activity. The oversight authorities should establish and maintain regular contacts with representatives of social networks to ensure effective monitoring and implementation of the regulations and if necessary to impose effective and timely sanctions.

Campaign-related financial reports of the contestants and other electoral stakeholders should be sufficiently detailed and presented in a readable manner for voters to be able to grasp clear understanding of the costs related to campaign activities and published in a timely manner. It is a good practice that interim reports are submitted during the election campaign and prior election day so the voters can make informed choices. Likewise, final reports after election day should be due within a sufficient period for electoral contestants and other stakeholders to close their campaign related financial transactions. The reports should remain available for a longer period after elections and could be published on the oversight body's, contestants' and other electoral stakeholders' websites and on social networks for the costs related to online campaigning.

Other campaign regulations can play a role in the online environment, include provisions for campaign silence before and on election day. In some cases, such measures include requirements that advertisements be taken down before voting starts. The EMB is often charged with oversight, but other actors may also be engaged, including municipal authorities. The Political Analyst should establish whether clear rules exist, identify which bodies have oversight power and assess whether they are able and willing to exercise it effectively.

ODIHR's **Handbook for the Observation of Campaign Finance** provides the most comprehensive guidance for OSCE election observers to assess campaign advertising, including the oversight responsibilities of the participating States. In line with commitments and international good practice, States should provide for independent oversight and observation of campaign finance. That responsibility should be given to an independent, professional regulatory body, mandated to provide guidance to electoral stakeholders, check campaign finance reports and investigate potential breaches. It be endowed with sanctioning power in order to promote the effective imple-mentation of the law and ensure the accountability of all stakeholders.

6.3 DATA PRIVACY PROTECTION OVERSIGHT

In online campaigning, the amount of personal data available and the methods used differ from traditional advertising methods and might have a greater impact on fundamental freedoms and voters' rights. As outlined in the previous sections, international instruments provide for safeguards for the acquisition, storage, processing and use of data. States are obliged to secure data against destruction, accidental loss, theft and any other form of unauthorized access, alteration or dissemination.[105] The legal framework should specify explicitly the conditions for obtaining information about voters and the purposes for which it is sought. It should further establish whether data may be made available to electoral contestants for campaigning purposes. Importantly, it should also identify the institution endowed with oversight responsibility and enumerate sanctions for the misuse of private data.

While the EMBs or population register authorities are likely to be charged with the management and supervision of voter lists, other more specialized agencies are often responsible for oversight of compliance with existing laws in the area of data protection. The Political Analyst will assess together with the Election or Legal Analyst, the statutes and performance of data protection institutions, including their independence during the campaign, as they do with the Media Analyst when examining the work of media-regulatory bodies (if they are competent in area of social network oversight). They should establish whether the authority makes decisions in a transparent manner and whether these decisions are subject to judicial review. They should also scrutinize the body's enforcement powers, including its ability to forward cases for investigation to other institutions or directly fine violators.

All election stakeholders and private data brokerage companies should be subject of independent oversight. The oversight often includes parties', contestants' and other companies' compliance with the data protection regime and the level of transparency in handling private data. For this purpose, it is a good practice that oversight authorities monitor whether:

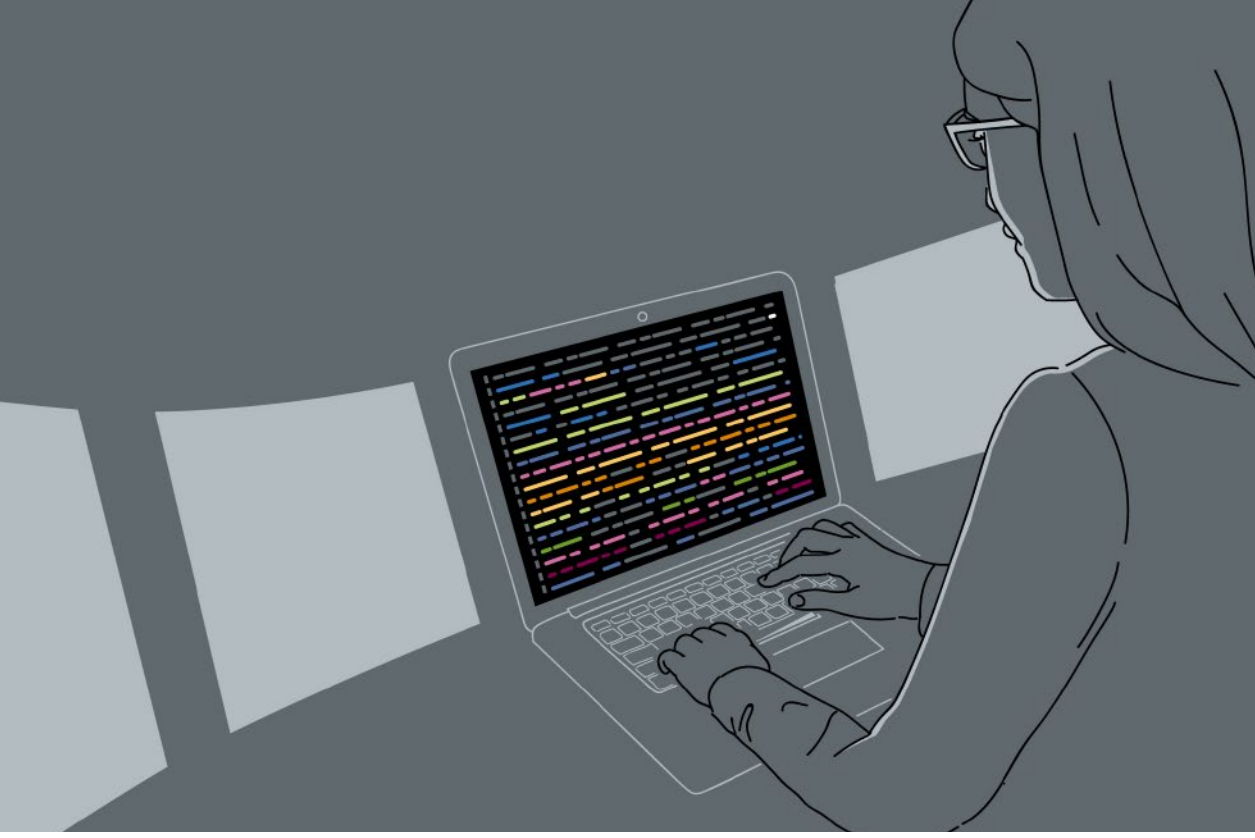
- All data controllers and processors are providing the public with clear information about how their data is and will be used;
- Voters are informed when intrusive profiling, such as combining information from different sources is conducted to find out more about their voting preferences;
- Public accountability is demonstrated, showing how parties meet their obligations and protect voters rights;

105 See the 1981 Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), especially articles 3, 5 and 7. See also the 2001 Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-border Data Flows.

- All data processors, including third-party suppliers, comply with the key transparency, security and accountability requirements of data protection; and
- Data processers regularly review the lawfulness of different types of processing of personal data to ensure the most appropriate basis is used.

Guiding Questions:

- ✓ Is there a privacy and data protection regime in place?
- ✓ Is it applicable and enforced in the context of elections, especially as pertains to campaigning by contestants and third-parties?
- ✓ Which state bodies have oversight and regulatory/sanctioning power in the area of data protection?
- ✓ Are they deemed to be politically independent and neutral in their actions?
- ✓ Does the privacy and data protection authority have the capacity, resources and will to fulfil its role in practice?
- ✓ Does the privacy and data protection authority have the necessary enforcement powers to be effective, including the ability to fine?
- ✓ Is decision-making by the privacy and data protection authority transparent and subject to judicial review?
- ✓ Do political parties and/or candidates have policies in place to ensure that they handle personal data in accordance with the law and/or international standards?
- ✓ Are all actors able to access data on equal terms?
- ✓ Do any contestants (micro)target voters during the campaign?
- ✓ Is (micro)targeting addressed in the legislation?
- ✓ How do actors obtain voter data, and have the latter consented to its use?
- ✓ Can they withdraw their consent?



7.
CHALLENGES and OPPORTUNITIES for QUANTITATIVE ASSESSMENT

7.1 METHODOLOGICAL LIMITATIONS

Although the methodology for assessment of campaigning on social networks is in its infancy and will continue to evolve alongside future technological developments, ODIHR election missions have been following different stakeholders' online campaigns to varying degrees for several years. It is important to note that there is not one universal or one-size-fits-all approach and there are different methodologies implemented by a number of observer organizations in the assessment of campaigning on social networks, some of which base their conclusions on more substantive quantitative and statistical measurements. However, the task of drawing conclusions based on quantitative

analysis is uncharted and presents a number of noteworthy challenges and limitations. The sample choice and methodological basis for quantitative assessment of campaigning on social networks are riddled with complexity that can, under some circumstances, defy systematic monitoring efforts during election activities constrained by time and other resource limitations.

The first set of challenges relates to scope, or the very high number of different platforms, profiles and posts that constitute the body of material for analysis. The *selection of platforms* must take into account their popularity among different demographic groups, so as to capture the widest possible range – even if users are more likely to be younger voters overall, thus making selection bias likely. Another problem is related to identifying representative *samples of profiles for monitoring*. The choice is complicated by the fact that their popularity can be transient, thus trending profiles that attract a lot of attention today may become irrelevant the next day. Another challenge is the *anonymity and veracity of accounts* as it is often more difficult to ascertain whether a profile belongs to the given person or is computer-generated. Lastly, the *volume of posts* that are generated on social networks can be infinite. The speed with which new posts appear, spread and are replaced by the next trending item can be extremely high and practically impossible to record without appropriate software.[106]

Working with large amounts of material requires employing digital tools and sophisticated methods of selecting more workable samples. However, this kind of sampling entails methodological risks, such as inherent biases in the digital tools and issues of external validity or generalization of results. Given the heterogeneity of information available online, it is exceedingly difficult to draw conclusions and make assessments solely on the basis of highly aggregated data and 'engagement' metrics, which can be difficult to interpret and whose magnitudes can be misleading. Moreover, sampling does not necessarily reduce data to amounts manageable without the need to resort to automated tools to gather and process it, which leads to other problems, such as automated exclusion of relevant content.

The second set of challenges is of a technical nature. While basic quantitative analysis of manually selected samples may be feasible and can be included in the assessment, covering a wider terrain requires the use of external digital tools to collect and analyze data from different platforms. Because accuracy of data collected from same platforms through different tools often varies, the consistency of analysis and the quality of findings can lack uniformity.[107] The tools may have to be 'tweaked' to fit local realities and account for both the methods and style of political communication that are popular in a given context. Finally, many applications handle textual data, but might be less helpful

106 Posts disappear regularly, either based on the platform's archiving policy or because they are removed, for instance on grounds of having violated community standards. Moreover, it may not always be possible to ascertain if posts are organic or computer-generated.

107 The optimal use of these instruments also demands deeper knowledge of the local context in order to facilitate the collection and analysis of information about meaningful, but sometimes less visible phenomena, such as the proverbial 'dog whistle' communication between politicians and their constituents, which may not be easily comprehensible to outside observers.

with other types of content, such as videos and images, whose omission could undermine the representativeness of results.

Beyond scope and technical matters, another type of challenge for quantifying findings and analyzing campaigning online is the inherent complexity of social networks. Unlike traditional media monitoring, which establishes relative measures, such as the share and tone of coverage, quantitative analysis of social networks offers a much wider range of metrics, including the frequency of postings, trending issues, analysis of networks, inauthentic accounts, the number of paid advertisements, the reach of public engagement and much more. Used in conjunction with a qualitative assessment, this data can illuminate different trends, including issues related to the malicious use of social networks, such as 'hate speech', incitement, disinformation, the misuse of administrative resources, computer generated propaganda, inauthentic or manipulative content amplification, and/or hidden (micro)targeting. However, without clear reference points, such as the approximate prevalence of a given phenomenon as a share of the total, these findings will not always allow the Political Analyst to dependably establish their actual significance in a given election campaign.

Lastly, research on social networks' impact on the formation of voters' opinions and behavior continues to emerge, and is challenged by competing findings. The overall significance, influence and circulation of a series of malicious posts or trending stories, including those that may be picked up by traditional media, is difficult to measure. Transparency, or bringing to light the ways in which factual information is manipulated or voters are (micro)targeted deserves attention and mission assessment on its background and potential effects, but quantitative analysis will not necessarily add value to findings that may already emerge from contextual observation and assessment based on qualitative methods.

The Political Analyst should generally approach the task of quantitative measurement from a critical perspective and with a keen awareness of what is achievable with limited resources during the time at hand. The Political Analyst should also be mindful of expectations that quantitative methods raise. While enumeration can be valuable, it should ultimately not form the primary basis for assessment. Different aspects that feature in online campaigns – including forms of information manipulation or 'hate speech'– continue to be marred by definitional shortcomings, which can skew findings and make them incomparable and often unreliable. And while new tools are constantly being developed to help improve measurement, technologies and modes of digital communication are also advancing at a rapid pace. Accordingly, quantitative approaches may sometimes lag behind these technological developments and be less helpful in illuminating more novel forms of manipulation, thus putting the credibility of the overall assessment at risk.

7.2 DATA FROM EXTERNAL SOURCES

The backbone of the ODIHR methodology is direct observation, triangulated with information obtained from interlocutors and with other data identified during the course of observation. Political Analysts often come across information collected and analyses carried out by other observer groups. Such input can be valuable for the mission's more general awareness about a particular topic. Most important, while external sources may serve as useful background, they should never be used as the sole basis for the election missions' findings and reporting. In keeping with general demands of independence and neutrality, the Political Analyst should only ever cite information or conclusions reached by other reputable organizations. This normally applies to all aspects of observation, including areas in which mission capacities are limited.

With the development of digital technologies and their increased use in election campaigns, there is a growing number of actors that collect and analyze data related to the role that social networks play in political communication. These include profit enterprises, such as the big-tech firms and data brokering companies, research centers and not-for-profit actors such as civil society organizations, some of which may be connected to citizen observer groups. The Political Analyst should be familiar with the leading entities and, whenever possible during the course of election activity, meet with select stakeholders to contextualize findings, clarify methodologies and collect additional details.

The Political Analysts should pay close attention to both commercial and non-profit initiatives that produce analytical tools by 'scraping' data from social networking platforms. Some of these products include readymade instruments, which if used in a diligent manner may support findings and help the Political Analyst to gain a more informed understanding about the role of social networks in the election campaign. Also, there are fact-checking organizations that specialize in detecting, calling out and correcting falsehoods online, and they are especially active during election periods. Finally, social network platforms themselves can be important interlocutors as they often publicly release data that can sometimes enrich the mission's observation and analysis efforts.

The specific nature and complexity of social networks, combined with the mission's limited time and resources, may make it necessary for observers analyzing online campaigning to use data from external sources to a greater extent than is normally the case in the context of international election observation or assessment. The Political Analyst must be especially vigilant in establishing the neutrality, authenticity and credibility of information and should always seek to verify data, whether it is manually or automatically generated through external tools. The Political Analyst must always triangulate findings; sometimes it may be advisable not to quote external conclusions directly, except in cases where they constitute an important component of the more general background. It is important to note that external assessments and analyses are often conducted based on findings accumulated over a span of time that does not align with election mission's timeframe or the election campaign period. While this

can have less significance with regard to understanding the general political background and context, use of these findings specifically related to the election campaign may be limited and must be treated with caution.

a. Web-Listening and Data Scraping Tools

'Web listening' or data scraping tools can generally provide good insight of overall trends in the political context and campaign environment. If Political Analysts possess the necessary skills, they can use some of these tools to support their overall campaign assessments. In doing so, they should perform manual searches and code data to establish basic quantitative findings and draw their own conclusions based on these elements.

There are several ways to obtain data from social networks. The most common method is using the platforms' own Application Programming Interfaces (APIs).[108] Another way is to resort to a custom-designed or off-the-shelf 'data scraping' tool. At present, there are many instruments available, including more basic ones with limited capabilities and those that are more complex; free programs and those that operate on the basis of a paid-subscription; as well as those that were developed to work with multiple platforms, and others that specialize in a single application.[109] While many of these tools were originally designed for commercial purposes, some can be adapted to process political or campaign-related content. This is a quickly evolving landscape, with many instruments rapidly becoming obsolete, while new ones are regularly created to take their place.

While many tools can be used to obtain data from different social networks, currently, there is no single instrument that can scrape data from all networks. Several of the programs can also be used on platforms such as *VKontakte, Odnoklassniki* and instant messaging services like *WeChat* and *SnapChat*; however, the level of permissible access to them varies. Because of encryption, data cannot be obtained from messaging services such as *WhatsApp, Telegram, Signal* or *Viber*. Moreover, because communication in closed groups is ultimately private, as a general rule, the Political Analyst must not attempt to obtain such data under any circumstances.

In general, to measure the sentiment of political debate on social networks, manual verification is advisable and often necessary.[110] When using some of these instruments, it is important to keep in mind that civic and political culture, different types of discourse, and the usage of context-specific slang may affect results. Political Analysts should, thus, be cautious when selecting key words and hashtags for searches.

---

108 Means by which data from one web tool or application can be exchanged with or received by another.

109 Users of these Guidelines should be mindful of the fast-pace developments in this extremely dynamic field as some of the tools may become redundant and obsolete in a short time, while new tools may emerge. At the time of writing some of the available tools include: *CrowdTangle, BuzzSumo, TalkWalker, NapoleonCat, Social Bakers, Brandwatch, Twitonomy, SentiOne, Fact-a-lyzer, Versus, Google Trends Facebook Ad Library, BotOrNot*.

110 When working with advanced tools, the Political Analyst should, as a matter of general practice, seek to select samples of data to verify whether the system correctly identified a given phenomenon and compare any emerging trends with qualitatively generated findings.

b. Big-Tech Companies Access to Data

Big-tech companies have come to increasingly recognize their crucial role in protecting the integrity of elections. Their engagement has been uneven overall, among different platforms and within single platforms in different countries. When it comes to technical parameters for retrieving metadata by researchers or observers, the big-tech have narrowed such possibilities over time but created some tools for data collection. Some of the efforts and tools introduced by the largest social networks in the OSCE region to increase transparency on their platforms are outlined below:

- *Facebook* continues to be the main platform for campaigning in many OSCE participating States. Concerned about potential data misuse, the company restricted access to its API in 2018 and it is no longer possible to get information in a way that respects the user agreement. Users must submit requests to *Facebook* well in advance and without assurance of success. While some applicants are given permission via *CrowdTangle*, others are offered more limited access via the API. Despite these difficulties, *Facebook* currently grants cost-free access to its data, which does not require programming skills. The company has also sought to increase transparency through its Ad Library and by issuing Transparency Reports, which now include quarterly Community Standards Enforcement Reports that detail actions taken to prevent content that violates user policies, including on *Instagram*.

- The availability of data from *Google* has also been uneven overall and has changed over time. In the past, accessing *YouTube's* API was relatively straightforward, but users had to possess some programming competency. The company has offered documentation and resources to use its service, including code in different programming languages to access the API. This has now become more difficult to obtain, with applicants having to make in-person requests that must reference domestic legislation that explicitly mandates firms to provide access. Since 2010, *Google* has published regular transparency reports, which have become more detailed overtime, and now cover the full range of its platforms.

- *Twitter* has been generally perceived as the most transparent platform and accessible for the research and academic community. Its API has been freely accessible to researchers and data is available across all of the company's markets. *Twitter* proactively releases information on the removal of fake accounts, in some cases announcing takedowns.

Overall, self-reporting by the big-tech companies does not match specific election cycles and is incompatible with the needs of ODIHR election observation or assessment activities. An uneven level of data access across different OSCE countries complicates data analysis. This is especially problematic shortly before elections when reliability of data streams matters most. The practice has shown that platforms have been more open with their data where appropriate legislation is in place to mandate access. Moreover, different platforms offer distinct 'time blocks' of historical data and while some allow

scraping going back years, others are more limited.[111] Finally, one of the key developments in political communication is the shift away from public discussions on social networks towards conversations in closed networks and direct messaging applications, which at the moment lie outside the reach of election observers.[112]

Both the quantity of data and uneven level of access to data create constraints for consistent high-quality reporting relevant for observation and assessment. These challenges underline the importance of keeping a sharp focus on what is achievable within a mission context and resources. The Political Analyst's assessment of campaigning on social networks must clearly state which platform and accounts it pertains to. If used in the assessment, information on how data was obtained and the methods employed to analyze it should be included. Findings must be verified manually by checking select samples of automatically generated material. It is also good practice to follow the insights and findings of other credible organizations, with great caution and diligently, to ensure that general impressions align and understand the reasons and consider possible explanations when they do not.

c. Fact-Checkers

The proliferation of manipulative content that followed the ascendance of social networks, has also given rise to organized efforts to identify, debunk and correct falsehoods trending online. The spread of so-called 'fake-news' online has provided impetus for the development of new techniques to address this problem. Often in co-operation with media and big-tech companies, scores of organizations known as fact-checkers have emerged to mimic what has long been associated with traditional media's practice of *ante hoc* internal correction of factual errors. In the context of social networks, this is now often performed using data mining software, and *post hoc*, (i.e., after) falsehoods have already reached the public domain.

Fact-checking organizations seek to determine the accuracy and correct published information, including news reports and politicians' statements. They are often civic or media initiatives, but also social influencers, and may have links with traditional media outlets. In co-operation with big-tech firms, fact-checker 'tags' have started to appear on some platforms to designate verified content and help improve the veracity of claims

111 For instance, posts on Twitter disappear after a little over a week, thus making regular and timely recording of information necessary. Moreover, social network firms often remove problematic posts, which creates a two-fold problem: an expunged post can be neither properly analyzed nor its effects gauged when its online presence was particularly short-lived.

112 Closed groups present a considerable and currently insurmountable challenge for international election observation. Because they are not in the public domain, observers cannot gain access without becoming party to the group, which they should never do in order to guard their neutrality. Moreover, observers' presence inside a group could affect the behavior of its members. Because transparency is paramount, the Political Analyst should under no circumstances attempt to become party to a group under an alias or through another individual or group.

promulgated online.[113] Many fact-checker groups operate transnationally and benefit from regular exchanges of information.[114] Support given to fact-checking networks that arose from concerns about the spread of falsehoods for electoral purposes has helped to fuel their rapid growth.[115]

The Political Analyst is not in the position to adjudicate the veracity of claims or determine the quality of fact-checking initiatives, but should acquaint him or herself with the landscape and take notice of the presence and activities of leading fact-checking organizations. Time permitting, the Political Analyst could join the Media Analyst and meet with the most prominent groups to establish whether fact-checkers face any impediments in their work and further assess the quality of their relationships with other actors, including electoral contestants, traditional media and the EMB. They could also ascertain any links between fact-checking groups and the big-tech companies, including to probe how responsive the companies are to reports flagged by fact-checkers.

Guiding Questions:

- ✓ Are any domestic organizations monitoring social networks during elections?
- ✓ What are their aims and overall conclusions?
- ✓ What are the key findings or themes that emerge from their observations of any previous or ongoing campaigns on social networks?
- ✓ Are there any reputable national initiatives that monitor campaigning on social networks using automated tools and what are their findings?
- ✓ How easily accessible is data from the big-tech companies in the respective OSCE participating State?
- ✓ Have domestic monitoring organizations reported any issues regarding the availability of data or its consistency?
- ✓ Are fact-checking groups present and engaged in exposing falsehoods during the campaign period?
- ✓ Are they genuinely non-partisan? Are there any concerns about the quality of their work?
- ✓ Is there any relationship between fact-checkers and state or election management bodies?

113 For instance, *Facebook* has teamed up with several organizations to fact-check and label content while *Google* has claimed that it tweaked its algorithms to prioritize fact-checked returns. *Facebook* alleged that this partnership has reduced the prevalence of 'fake-news' by some 80 per cent. *Twitter* developed tools to help users flag content that aims to suppress voter turnout, which the company removes from its platform when reports are substantiated.

114 One of the leading international networking efforts is the International Fact-Checking Network (IFCN), which is a global compact aimed at fostering the development of common working methods to institutionalize the sharing of best practices. Some of the networks are supported by international actors, including organizations such as the EU, which also helped establish the independent European network of fact-checkers.

115 The number of fact-checking initiatives has increased exponentially in recent years. Alongside the emergence of genuine attempts to address the problem of 'untruths', there has also been a spike in the number of 'fake fact-checkers' that seek to affirm falsehoods that are spread online.

- ✓ Do the platforms co-operate with local fact-checkers?
- ✓ How responsive are they to their reports?
- ✓ Is there co-operation between fact-checking organizations and mainstream media?
- ✓ Do social networks provide users with technological solutions to detect manipulative and harmful content (e.g., flagging)?

Annex 1: RELEVANT INTERNATIONAL DOCUMENTS

OSCE

The 1990 OSCE Copenhagen Document

Paragraph (5.1):free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives;

Paragraph (7.5): respect the right of citizens to seek political or public office, individually or as representatives of political parties or organizations, without discrimination;

Paragraph (7.6): respect the right of individuals and groups to establish, in full freedom, their own political parties or other political organizations and provide such political parties and organizations with the necessary legal guarantees to enable them to compete with each other on a basis of equal treatment before the law and by the authorities;

Paragraph (7.7): ensure that law and public policy work to permit political campaigning to be conducted in a fair and free atmosphere in which neither administrative action, violence nor intimidation bars the parties and the candidates from freely presenting their views and qualifications, or prevents the voters from learning and discussing them or from casting their vote free of fear of retribution;

Paragraph (9.1): everyone will have the right to freedom of expression including the right to communication. This right will include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The exercise of this right may be subject only to such restrictions as are prescribed by law and are consistent with international standards. In particular, no limitation will be imposed on access to, and use of, means of reproducing documents of any kind, while respecting, however, rights relating to intellectual property, including copyright;

Paragraph (9.2): everyone will have the right of peaceful assembly and demonstration. Any restrictions which may be placed on the exercise of these rights will be prescribed by law and consistent with international standards;

Paragraph (9.3): the right of associatiowill be guaranteed. […]

Paragraph (10.1): respect the right of everyone, individually or in association with others, to seek, receive and impart freely views and information on human rights and fundamental freedoms, including the rights to disseminate and publish such views and information;

UNITED NATIONS

International Covenant on Civil and Political Rights (ICCPR)

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 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.

Article 19: 1. Everyone shall have the right to hold opinions without interference. 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.

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.

Human Rights Committee - 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.

Human Rights Committee - General Comment 25

Paragraph 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.

Paragraph 11: Voter education and registration campaigns are necessary to ensure the effective exercise of article 25 rights by an informed community.

Paragraph 12: Freedom of expression, assembly and association are essential conditions for the effective exercise of the right to vote and must be fully protected. Positive measures should be taken to overcome specific difficulties, such as illiteracy, language barriers, poverty, or impediments to freedom of movement which prevent persons entitled to vote from exercising their rights effectively. Information and materials about voting should be available in minority languages.

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. 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.

Paragraph 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.

Human Rights Committee - 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.

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.

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.

Paragraph 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.

Paragraph 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.

International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)

Convention on the Rights of Persons with Disabilities (CRPD)

UN Convention Against Corruption (UNCAC)

OTHER REGIONAL INSTRUMENTS

The European Convention for the Protection of Human Rights and Fundamental Freedoms

Commonwealth of Independent States Convention on Human Rights and Fundamental Freedoms

The American Convention on Human Rights

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

The Treaty on European Union

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

European Union General Data Protection Regulation

JOINT DECLARATIONS, GUIDING PRINCIPLES AND REPORTS

The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information Joint Declarations on:

- Freedom of expression and the Internet, 2011
- Freedom of Expression and Countering Violent Extremism, 2016
- Freedom of expression and "fake news", disinformation and propaganda, 2017
- Media independence and diversity in the digital age, 2018
- Challenges to Freedom of Expression in the Next Decade, 2019
- Freedom of Expression and Elections in the Digital Age, 2020

UN Guiding Principles on Business and Human Rights (HR/PUB/11/04), 2011

UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/17/27), 2011
(On key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet)

UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/26/30), 2014
(On the right to freedom of expression in electoral contexts)

UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/35/22), 2017
(On the role of digital access providers)

UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/38/35), 2018
(On online content regulation)

UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression presented to the UN General Assembly (A/74/486), 2019
(On hate speech)

UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/47/25), 2021
(On Disinformation and freedom of opinion and expression)

Annex 2: GLOSSARY OF RELEVANT TERMS

Algorithm - a fixed series of steps that a computer performs in order to solve a problem or complete a task.

Application programming interface (API) - a means by which data from one web tool or application can be exchanged with, or received by another.

Artificial intelligence (AI) - computer programs 'trained' to solve problems that 'learn' from data parsed through them, adapting methods and responses in a way that will maximize accuracy. (See Machine Learning)

Automation - the process of designing a 'machine' to complete a task with little or no human direction.

Big-data - large sets of unstructured or structured data.

Big-tech companies – private entities that provide information communication technology services and own social network platforms.

Bots - social network accounts operated entirely by computer programs and designed to generate posts and/or engage with content on a particular platform.

Botnet - a collection or network of bots that act in co-ordination.

Crowdsourcing - soliciting ideas or content from a group of people, typically in an online setting.

Computational propaganda - use of algorithms, automation, and human curation to purposefully distribute misleading information and other types of manipulative content over social networks.

Co-ordinated inauthentic behavior (CIB) - groups of accounts working together to mislead others about who they are or what they are doing in the online environment.

Cyborg - it refers either to a bot-assisted human or to a human-assisted bot.

Data mining - the process of monitoring large volumes of data by combining tools from statistics and artificial intelligence to recognize useful patterns.

Dark ads - advertisements that are only visible to the publisher and their target audience.

Dashboard – an interface that often provides at-a-glance graphical views of key performance indicators (KPIs) relevant to a particular objective. It visually tracks, analyses and displays key indicators, metrics and key data points to monitor a specific process.

Debunking - the process of showing that an item (e.g., text, image or video) is less relevant, less accurate, or less true than it has been made to appear.

Deep fakes - fabricated items spread on social networks produced using AI by synthesizing different elements of existing video or audio files, in which, for example, an individual appears to speak words and perform actions that did not happen in reality.

Disinformation - false information that is deliberately created or disseminated with the express purpose to cause harm.

Doxing - the act of publishing private or identifying information about an individual online, without his or her permission. This information can include full names, addresses, phone numbers, photos and more.

Echo-chamber - a virtual space, context or situation where certain ideas, beliefs or data points are reinforced through repetition of a closed groups of accounts that does not allow for the free input of alternative or competing ideas and concepts.

Encryption - the process of encoding data so that it can be interpreted only by intended recipients.

Engagement rate – a metric used to describe the amount of online interaction (e.g., 'likes', 'shares', 'comments') a piece of content receives.

Facebook reach - the number of unique users who have seen content from a Facebook page. Facebook provides two different reach metrics: 1) total reach: the number of unique users who saw any content associated with a Facebook page during the last seven days; 2) post reach: the number of unique users who have seen a particular Facebook post in their 'News Feed'. These two categories can be broken down to: 1) Organic reach: the number of unique users who saw content for free; and 2) Paid reach: the number of unique users who saw content because of purchased visibility for it, either by boosting it or buying an ad.

Fact-checking - the process of determining the truthfulness and accuracy of official, published information such as politicians' statements and news reports.

Fake followers - anonymous or imposter social network accounts created to portray false impressions of popularity about another account.

Filter bubble – a process when websites and social platforms make use of algorithms to selectively assume the information a user would want to see, and then give information to the user according to this assumption. Websites make these assumptions based on the information related to the user, such as former click behaviour, browsing history, search history and location.

Geotargeting - a feature that allows users to share their content with geographically defined audiences. Instead of sending a generic message for the whole world to see, the messaging and language of a content are refined to better connect with people in specific cities, countries, and regions.

Hashtag - a word or phrase preceded by a "#" (i.e., #elections) as a way to annotate a message or to categorize information and make it easily searchable for users.

Information disorder - conceptual framework for examining misleading or manipulative types of content, such as propaganda, lies, conspiracies, rumors, hoaxes, hyper-partisan content, falsehoods or manipulated media. It comprises three different types: mis-, dis- and mal-information.

Influencer - a social network user with a significant audience who can drive awareness about a trend, topic, company, or product.

Instant Messaging (IM) - a form of direct and real-time text-based, voice or video communication between two or more people.

Manufactured amplification – reach or spread of information that is boosted through artificial means and can include human or automated manipulation of search engine results and trending lists, as well as promotion of certain links or hashtags on social networks.

Machine learning - a type of AI in which computers use huge amounts of data to learn how to perform tasks through experience and past operations rather than being programmed to do them.

Meme - captioned photos spread online.

(Micro)targeting - a technique that uses people's data — demographic, about what they like, who they're connected to, what they've purchased, and more — to segment them into small groups for content promotion.

Net neutrality - the idea, principle, or requirement that Internet service providers should or must treat all Internet data as the same, regardless of its kind, source, or destination.
Organic content – free, not sponsored content from human accounts, content produced on social networks without paid promotion.

Organic reach - the number of unique users who view content without paid promotion.

Paid reach - the number of users who have viewed published paid content. Paid reach generally extends to a much larger network than organic reach—messages can potentially be read by people outside of a concrete contact list.

Reach - a data metric that determines the maximum potential audience for any given message determined by a calculation that includes number of followers, shares and impressions.

Response rate – an engagement metric assessing the level of an account's interaction with its social audience, calculated as a result of the ratio between the mentions that a user has replied to in a given time period and the total number of mentions the account has received.

Scraping - the process of extracting analytical data from a website or a social networking platform.

Trending topic - the most discussed topics and hashtags on a social network.

Trolling - the act of deliberately posting offensive or inflammatory content to an online community with the intent of provoking readers or disrupting conversation.

Troll farm - a group of individuals engaging in trolling or bot-like promotion of narratives in a co-ordinated fashion.

User-Generated Content (UGC) - text, voice recording, videos, photos, quotes, etc. that is created by individual or group of social network users.

Online social networking sites have moved election campaigns into a new era of communication, in which voters have wider channels to express their opinions. While social networking sites provide space for voters to enhance their direct participation in campaigns and enable electoral contestants to better mobilize support, the use of social networks, especially during election campaigns, carries a wide array of challenges. Some of these pose threats to the exercise and protection of fundamental freedoms and human rights, as well as the overall integrity of the election process.

The aim of these Guidelines is to provide a framework, mainly for ODIHR election observers, to adequately assess the impact of the key aspects of online campaigning on the integrity of the election process and democratic conduct of election campaigns. These aspects include the online activities of electoral contestants, dissemination of specific types of content relevant to the election process, political and campaign advertising, and the protection of private data.

Office for Democratic Institutions and Human Rights
OSCE ODIHR