



**Report on the fifth expert roundtable:  
Freedom of media in elections and counteracting disinformation**

**29 April 2022**

**Opening Speech**

**Teresa Ribeiro  
OSCE Representative on Freedom of the Media**

Dear colleagues, distinguished delegates of the OSCE participating States, ladies and gentlemen,

It is a pleasure to welcome you to the fifth roundtable in our series of expert meetings dedicated to the topic of disinformation, which today focuses on Elections, the bedrock of democracy one could say.

While in the past we have addressed such relevant issues as media self-regulation and artificial intelligence, disinformation can have a particularly disruptive impact on elections, not only by seeking to alter election results through mind manipulation, but also by delegitimising the electoral process altogether.

Thus, election interference can perhaps best be defined as unjustified and illegitimate ways of influencing voters' free choices prior to and during an election, thereby hindering their ability to exercise their political right to vote, freedom of thought, and freedom to make choices and form opinions.

To this end, disinformation seeks to manipulate and distort the information that citizens receive by presenting the so-called "alternative facts", conspiracy theories and shocking opinions. They are in fact false news and false accusations, often against political candidates, making it difficult for citizens to make informed choices, while also falsifying or manipulating polling data in order to reduce citizens' trust in the electoral process and, crucially, in its outcomes.

We have witnessed this more explicitly in today's digital age, where "fake news" and disinformation, when combined with technology, can spread faster and more widely than before in the online ecosystem, with the aim of confusing voters. Following the 2016 and 2020 US Presidential elections social media platforms subsequently took steps to mitigate the phenomenon, with Twitter

adopting new guidelines in 2020, for instance by labelling and then banning certain accounts that spread disinformation or are in fact fake accounts.

Since then, we have witnessed elections across the entire OSCE region where disinformation, perhaps, has been involved in some way, shape or form, including last weekend in France and just a few weeks ago in Serbia.

In 2020, in co-ordination with the special rapporteurs on freedom of expression of the United Nations and the OAS, we issued a joint declaration shedding light on the issue of disinformation during elections, particularly in the digital age. We expressed specific alarm at the misuse of social media by both State and private actors to subvert election processes, including through the use of propaganda, and denounced the use of disinformation, which can exacerbate and generate election related tensions. The document also provided a set of recommendations and key standards, calling on participating States to refrain from adopting general or ambiguous laws, such as prohibitions on spreading “falsehoods” or “non-objective information.”

Before this, in 2017, we issued another Joint Declaration dedicated to “fake news” and disinformation, in which we expressed concern at how disinformation is often designed and implemented in such a way as to mislead a population. Among its recommendations, we emphasised that media outlets should consider including critical coverage of disinformation and propaganda as part of their news services, particularly during elections, in order to debunk disinformation and provide citizens with reliable, trustworthy information.

Other international bodies, too, have spoken out against the threat of disinformation. Most recently, amid the unfolding Russian invasion of Ukraine, the European Parliament adopted a resolution expressing grave concern at Russia’s persistent efforts to destabilise democratic processes across the EU and the Western Balkans, including through disinformation. This shows the threat posed by foreign states that are able to influence and undermine democracy through digital means.

The resolution further stated that disinformation, during election campaigns, may also disproportionately target female journalists through the use of sexist narratives and derogatory language, leading to their discouragement from taking part in these democratic processes and thereby depriving society of crucial voices and perspectives. We must therefore remain ever vigilant to the threat posed by disinformation, including its impact on marginalized voices and communities.

How then should we respond to the problem and challenges posed by disinformation? And how can we ensure the credibility and integrity of electoral processes?

First, let me recall the guiding principles and the volume of robust international human rights law and UN standards that can guide us moving forward. Take, for instance, the Human Rights Committee General Comment No.25, which explicitly states that “Persons entitled to vote must be free to vote [...] without

undue influence [...] and to form opinions [...] free of [...] manipulative interference of any kind.” In its later Comment No.34, the UN further underscored the crucial role of a free press in communicating information and ideas between citizens and election candidates, without censorship or restraint.

While these standards must continue to guide us in the digital age, one cannot underestimate the impact that new technologies have had in facilitating the spread of disinformation during elections or, more importantly, the need to adopt robust, human rights-centred policies.

All too often, we have seen governments attempt to tackle election disinformation through prior restraint and the blocking of internet sources. Yet, in doing so, they themselves may be inadvertently restricting people’s human rights and freedom of expression, having a chilling effect on public discourse and public engagement.

Instead, it is crucial that any restriction or legal curbs on disinformation pass the strict test of Article 19 of the International Covenant on Civil and Political Rights; in other words, that they be provided by law and be a necessary and proportionate measure in view of the international standards.

States should also consider supporting positive measures, such as the promotion of independent fact-checking mechanisms and public education campaigns during elections, while adopting clear and appropriate laws that prohibit the dissemination of statements that are specifically designed to obstruct individuals’ right to vote, such as the spread of incorrect information about where and when to vote.

Another key component of any response to disinformation is media literacy. As one of the most effective ways of building resilience against disinformation in the long run, media literacy campaigns, particularly prior to elections, can help counter disinformation by empowering citizens with the tools and knowledge to spot false stories and hold media accountable on the quality of the information they share as well as to act responsibly as content providers.

This, however, requires a multi-stakeholder approach, working closely with governments, the media, civil society and other stakeholders to engage in promoting media and digital literacy as well as raising awareness about the harms posed by disinformation during election periods. The OSCE, with its comprehensive approach to security, remains an effective platform on which to engage on this topic, particularly in these dire times that we face.

My office will therefore endeavour to strategically engage with the OSCE participating States, on a bilateral level and in line with the mandate bestowed upon me, to share best practices and provide expert policy recommendations so that we may find adequate and effective ways of protecting the citizens of the OSCE region against the harms of disinformation during elections whilst safeguarding their rights to vote and freedom of expression.

I hope that today's session will provide us with much-needed food-for-thought and implementable recommendations for the way forward.

Thank you all for your attention and I look forward to our fruitful discussions.

### **Panel presentations**

**Vladimir Misev**

**Senior Adviser on New Voting Technologies, OSCE Office for Democratic Institutions and Human Rights (ODIHR)**

ODIHR is the leading European agency in the field of election observation. It deploys thousands of observers to assess whether elections in the OSCE region are conducted in line with OSCE standards and commitments, international standards and national legislation.

The new phenomenon of disinformation campaigns is a particularly important one to address. We are taking co-ordinated efforts to address it and provide additional support to participating States. For this purpose, we have produced guidelines and a policy paper on the topic.

**Yves-Marie Doublet**

**Deputy Director of the financial department of the National Assembly (France)**

This is a sensitive subject. Digital platforms have been praised for making democratic information available, which is particularly useful in countries where the executive controls information. But digital platforms do not mean more democracy when they are used for disseminating false information, stigmatizing and criminalizing others in electoral campaigns, and the dissemination of disinformation through an online platform is harmful, erodes the press and makes the world less informed.

From a legal point of view, the European Court of Human Rights considers freedom of expression to be applicable not only to information or ideas that are favourably received or regarded as inoffensive but also to views that are considered offensive, as well as those that shock or disturb the state or any sector of the population. The dissemination of views must be ensured even if these views may be considered as false.

Regarding these legal frameworks, there are two distinctions, first, between misinformation, which refers to incorrect or wrong information shared without malicious intent, and disinformation, which is a deliberate attempt to make people believe things which are not accurate. Often through the use of automated accounts, manipulated videos or targeted techniques. The second distinction is between disinformation and hate speech. Hate speech mostly relies on discrimination and in some cases the same message may contain disinformation and hate speech. These techniques of disinformation were used

during the last two presidential elections in the US, the Brexit referendum in the UK, and other elections around the world.

To address this phenomenon, we need to understand why these processes are so developed on such a large scale during electoral campaigns, why they are dangerous for election campaigns and democracy, and third to analyse responses to counter such practices.

There are four factors which explain the development of disinformation. First, the impact of social media. We have to bear in mind that the number of daily Facebook users is 1.9 billion, Twitter users amount to 210 million, and up to 1.8 billion daily views are on YouTube.

The second factor is the method. Facebook has created a targeting paradigm, enabling political parties during electoral campaigns to access millions of users and to target them individually by age, gender, electoral district, interest etc. For this purpose, digital media use an algorithm to target those voters and customers – a partnership was formed between digital companies and media businesses, because algorithms may be used to determine the profile of voters and becomes part of their business models. Political campaigns then combine voters' profiles with commercial information in order to match the right type of message for voters, as was the case during the Brexit campaign for instance.

The third factor is the speed of dissemination: between 12 and 14 hours are needed to debunk a rumour that has circulated on Twitter. The impact of false news on the eve of polling day may therefore be devastating.

The fourth factor is the cost. Financing propaganda on social networks does not require much money.

My second question is why are these online techniques dangerous for election campaigns and democracy?

First of all, these techniques hamper the clarity of electoral debate and the compliance with the principle of fairness of elections. These techniques infringe on the right to privacy of voters, because the use of political data is not protected. These techniques are immaterial and therefore opaque, they are quite unknown to users, and they weaken the national framework on electoral law. Rules on electoral law or political finance have been conceived on a national level, because electoral law is part of the sovereignty of the state. But disinformation crosses borders and is not easily stopped by national legislation. Some candidates or political parties may benefit from online platforms, while others might not benefit at all, carrying the danger of an unfair electoral campaign.

What are the possible options to prevent the spread of false information? There are two approaches: self-regulation and statutory legislation.

Self-regulation went through several steps. At the beginning, Facebook, Twitter and Google employed fact-checking and removed accounts. However, Mark

Zuckerberg said that Facebook would not be the arbiter of truth. This policy of self-regulation turned out to be inefficient, because there is a strong imbalance between the amount of “fake news” and the number of fact-checkers, only 15,000 for Facebook, so fact-checkers can only manage a small part of “fake news”. We have observed also that fact-checkers do not always know the language or background of the country from which the disinformation originates.

In a second phase, Facebook removed 265,000 pieces of content for violating its policy. Facebook and Twitter also suspended Trump’s account, but they only did so once he was no longer President, with his suspension subsequently confirmed by the Oversight Board of Facebook.

There are three types of actions, namely legislative, judicial and preventive ones, which address the problem of disinformation in electoral campaigns from different perspectives: transparency, liability and monitoring. Concerning transparency, for instance French legislation in December 2018 sought to counter the risk of citizens being tricked or manipulated in exercising their vote through the mass dissemination of false information during electoral campaigns. An online platform with 5 million visitors has to provide users with true, clear, transparent information. This information must pertain to the identity of those who remunerate this platform in return for promoting information campaigns related to debates regarding the public interest. It must pertain to the amount of remuneration and to users’ private data.

Following the Brexit campaign, the UK asserted the need to identify who is behind online platforms and provided recommendations on spending in digital campaigns, the transparency for digital campaigns and the enforcement of this rule. It is obvious that when you have a ceiling of expenditure and if, at the same time, you have spending on a digital platform, which is conducted from abroad and not recorded within these ceilings, they will not be deterrent. In the US, the Draft Honest Ads Act subjects internet ads to the same rules as TV and radio ads, and allows the public see who bought an online political ad.

Now we move to online liability. Article 10 on freedom of expression of the European Convention on Human Rights admits legitimate and proportionate restrictions. The removal of certain content on a given platform which is charged with hosting inaccurate or misleading information would not be considered a violation of article 10 if the damage is able to affect the outcome of the election and if therefore the content on the platform should be blocked during a campaign.

It would comply, too, with another jurisprudence, which implies that the member states have a positive obligation to protect the right to freedom of expression from attacks, including by private individuals.

French legislation provided for that purpose an interlocutory proceeding to stop, within the timeframe of 48 hours, the spread of false information likely to harm the fairness of election. The proceedings provided by the law are intended for incorrect and misleading allegations or accusations which may alter the

fairness of elections. But they do not relate to opinions or partial inaccuracy or exaggerations which are part of electoral debates. The misleading information must be artificial or computerised, deliberate and spread through mass distribution.

A French court required Twitter last year to submit any documents of the operator related to hate speech within two months.

The French broadcasting authority also has the right to refuse to sign agreements with a foreign country if the activity [of a foreign broadcaster] could seriously harm the life of the nation by disseminating false news or violating media pluralism.

The German Network Enforcement Act, NetzDG, which has a broader scope than electoral campaigns, should be mentioned in this context too.

Monitoring is the third level of action. A taskforce was set up in France to prevent online attacks before the presidential elections. It is in charge of the coordination of the activities of the ministries; this unit is staffed with 60 people and may challenge suspicious cases through the agency for telecommunication, through the national supervision committee of the presidential election, and appeal to the Constitutional Council in charge of supervision of regulation of the election.

A special unit within the Prosecution has been created by the German authorities. A rapid response team was set up in the UK Cabinet Office to monitor the false news.

But monitoring is not just a task designated to governmental monitoring bodies. Citizen fact-checkers could raise disinformation cases before the relevant supervision bodies and regulators of communication services, they promote fact-checking, literacy, and best practices.

I do not underestimate the obstacles raised by the implementation of the relevant law and policy. The criteria to remove unlawful content are sometimes inadequate, because the attacks are often perpetrated by individuals. The time limit for removing unlawful content in France and Germany is very short. When the offences are committed abroad, outside the EU, it would be almost impossible to impose sanctions. The German judiciary has not managed to remove certain messages from the Telegram network based in Dubai. But we need to send a proper signal against those who disseminate disinformation, either through a national legal framework or an international convention.

**Brenda Santamaria**  
**Chief of the Election Observation Section, Department of Electoral Cooperation and Observation of the Organization of American States (OAS)**

We have been discussing in our community of electoral observers the phenomenon of disinformation. Disinformation is technically not a new

phenomenon in elections, but the massive dissemination of disinformation is what is new for elections today. The substantial potential audience that social media has in terms of reaching people makes the biggest difference, because the speed of the flow of this type of information has hugely increased.

We observe elections, freedom of expression and campaigns. We try to cooperate with Member States to improve the quality of their elections and processes, as well as electoral institutions. Because of this new challenge for us and for election management bodies (EMBs), we have introduced new elements in our analysis of election observation missions, and the OAS observes elections in 28 Member States in the Americas.

What we have observed is that the debate about the precise impact of disinformation in election processes is not quite settled. Some studies mention that they have a big impact while others say the opposite. What we do know for now is that it does have an impact on the debate; it contributes to the impoverishment of those debates during elections. This has to do directly with what is going on during elections; it is not only the campaigns that are the target of disinformation. Given this context, we brought an expert on freedom of expression, campaigns and disinformation to understand/analyse what is going on and make recommendations. Our ultimate goal is to produce recommendations to help improve electoral processes.

Some of the findings that I can share with you include: the targets of disinformation are very diverse; it can be political actors, political parties, candidates, election management bodies, authorities or the institution of elections itself. Journalists are being targeted and even election observation missions were targeted in the past, e.g., text messages were circulating accusing the OAS of imparting instructions and the election management body had to clarify that they are just observing the election.

The topics that are used to disinform around the election process often centred on the candidates. In that regard, I share the view of Ms Ribeiro about trying to understand what happened to women during elections, mindful that they are targets of disinformation and face violence. We have a gender expert and an expert on this specific issue, so gender-based violence is an aspect that we are interested in observing.

These types of campaigns also try to undermine the process itself and its credibility. The types of things noted during the voting relate to the issues of who can vote, what type of documents they should bring, etc.

There was a lot of disinformation, especially during the COVID-19 pandemic, when campaigns turned increasingly to social media. This enhanced the power of these tools in the context of the electoral process. The tools that are being used to create disinformation have become more sophisticated over time, using different tools, including AI and manipulation of videos, among others. We are still in the process of the evolution of the phenomenon.



We have identified main strategies to counter disinformation: to detect and expose disinformation, as well as disseminate correct information. This can be done by electoral management bodies, together with fact-checkers, journalists and other institutions. It is important to facilitate access to certain information and to quality information. We also talk about filling the gaps: if you do not present information then someone else will. As Ms Ribeiro said, we need to promote digital literacy, we need to generate skills in our citizenry to be able to identify false information and make them aware of their role in disseminating this false content.

There are some good examples in the region on how EMBs have worked in a multi-stakeholder approach to counter disinformation. For example, the electoral tribunal in Brazil has established agreements with social media companies and the political parties, wherein they engage the parties to better understand the kind of information their campaigns will use/spread and to explain the risks posed by disinformation.

It is important to have a good webpage and dissemination tools, as well as communication campaigns. Mexico has been implementing very good strategies in this regard, while Costa Rica had a good example of a responsible digital citizenry campaign.

States have to take a multi-stakeholder approach. The problem of disinformation is not something that will be solved by one institution. Strengthening capacities for communication, it is not only important to run a good election but also to inform the public about what is going on. Legislation must comply with international standards to respect freedom of information. We work with EMBs in similar to this roundtable events, and we plan on continuing to work with them to strengthen their capacities. We also co-operate with EMBs in order to have a better ecosystem for our electoral process.

**Mikheil Benidze**  
**Chief of Party, Georgia Information Integrity Program (GIIP)**

Though I head the GIIP, I would be speaking from a broader civil society perspective, including from my experience of monitoring social media and disinformation in Georgia. Georgia is an interesting case in terms of disinformation because, while it is not necessarily unique that Georgia's political and electoral discourse to be dominated by disinformation, it is noteworthy because it faces the acute challenges both from foreign and from domestic actors as sources of disinformation campaigns.

Georgia is also interesting as many lessons can be learned from us. While since recently, we are seeing new findings of foreign meddling campaigns in elections and political processes, Georgia is one of the hotbeds where this was tried and tested way before. This especially intensified following Russia's 2008 invasion of Georgia, after which we began witnessing foreign propaganda campaigns that are primarily aimed at undermining Georgia's Euro-Atlantic path, undermining trust in institutions, and sowing fear in society as well as dividing society among value-based discussions by employing propaganda, as well as

xenophobic, nationalistic, and anti-Western narratives to undermine the fabric of society.

What makes Georgia unique is that there is also an added layer of complexity in terms of domestic polarisation along political figures and political party lines. This obviously influences and pollutes the information environment with discrediting campaigns, manipulating content and various attempts to influence voters. Both foreign and domestic campaigns become more active around elections, therefore making the public more vulnerable to undue influence. Social media as a vehicle of disinformation has been particularly potent over recent years, with greater amplification of these processes in the country.

What trends have we seen in terms of tactics, especially during elections? We see the use of social media and traditional media to discredit candidates in elections, to target and silence political opponents. These campaigns are not limited to political actors, as journalists and civil society actors are also being attacked. Anyone with a different opinion can become a target of discrediting campaigns.

These attacks are carried out through anonymous networks. We are also seeing “false media” operations - actors pretending to be media outlets and trying to populate the information space with propaganda. We also see “false support” webpages – operations, which try to deceive and confuse voters by pretending to support a particular political actor but actually spreading information that undermines that very actor.

There are also anonymous support campaigns that mobilise around specific political actors without disclosing their ties, usually done channelled through advertising and promotion of content. What we have also seen is the co-ordination behind these types of operations is what Facebook calls Co-ordinated Inauthentic Behaviour: organized networks pushing these messages around the same time in a co-ordinated manner.

While value-based propaganda narratives are also active during and in-between elections, they usually become specifically active around elections. We see a trend whereby elections have some sort of propaganda theme that targets a specific vulnerability. In 2016, during the parliamentary election in Georgia, there was a debate around banning gay marriages - while there was no legislation pushing for marriage equality, the debate in the election was around the issue, as if it was the main pre-election topic. Then in 2017 local elections, anti-migration debates followed. Similarly, during the 2020 parliamentary elections, anti-Turkish and anti-Azerbaijani narratives dominated pre-election rhetoric. These types of narratives bring additional vulnerabilities to minority groups and those that are already disadvantaged in society. They sometimes also promote violence, as we saw in July 2021, when an “anti-pride rally” was mobilised by a far-right propaganda group. This was a hybrid operation, in which propaganda and disinformation then resulted in physical clashes and violence against journalists and attacks on the offices of the pride movement and other civil society organizations.

What should be done? What are some of the remedies? In terms of legislation, Georgia has fairly liberal freedom of expression legislation. Georgian civil society has been trying to protect this kind of approach and not go down the path of overregulation. In an environment where there is insufficient trust to the judiciary and institutions, there is the risk that any type of legislation can be misused against freedom of expression.

When it comes to EMBs, what we see on the one hand is a lack of capacity to understand and respond to the challenges, especially understanding political advertising online. Or we see attempts to go after disinformation while branding information or criticism from the media and civil society as disinformation. We should not allow EMBs to shape the narrative in this way as it undermines the work of CSOs.

When we talk about media regulators, we also see a lack of political independence. Oftentimes, what we see is that their efforts are not targeted towards overall resilience, but in a narrow political perspective, only singling out media outlets that are considered the opposition, only targeting disinformation in those outlets. While political parties comply with election regulations in official channels, we see proxies of the parties employ inauthentic accounts on social media. In the lead-up to the 2020 parliamentary elections, we saw Facebook take down several networks of accounts linked to the political parties, including pro-Russia ones, and the largest networks being linked to the ruling party, which brings additional vulnerabilities to the situation.

The media in Georgia is very polarized, which reduces its effect in the fight against disinformation. But not all is lost. There are efforts of CSOs to target disinformation – there is active monitoring, focused generally on disinformation, but also specifically during elections. We have very strong fact-checking work and partnerships with Facebook and other tech companies to take down disinformation or reduce its distribution. Ahead of the 2020 Georgian elections, over 50 Georgian CSOs and media outlets successfully advocated with Facebook to introduce transparency requirements on political advertisement in Georgia.

There is a positive example of a self-regulatory body, the Georgian Charter of Journalist Ethics, which addresses complaints to media outlets on accuracy, on whether they follow the standards of accuracy etc. What we as our programme do is try to help these different actors co-ordinate better and support partnerships between CSOs and the media to investigate disinformation actors and uncover new learnings around disinformation. We also support research into the effect and vulnerabilities of disinformation, why people believe in it, and try to target the root causes of the problem, not just the symptoms.

I commend the UN, OSCE and OAS Joint Declaration on Freedom of Expression and Elections in the Digital Age, which addresses the key issues and problems out there, as well as providing strong recommendations. I would add the importance of resilience, which should be built by the strategic communications bodies, who should be independent from political influence, and work not just within the government, but also co-ordinate better and work

with various actors, including tech platforms, CSOs, the media etc. EMBs should understand the role of disinformation and work with CSOs in good faith and implement genuine counter-disinformation efforts. One thing is the legislation itself and then implementing it in the right context. I would also underscore the role of CSOs and their involvement in fighting disinformation, as in the case of Georgia where their efforts have been crucial.

**Jelena Surčulija Milojevic**  
**Assistant Professor, Department of Journalism and Communication Studies, University of Belgrade (Serbia)**

I will look at the differences between misinformation/disinformation, and why we are not using the term “fake news”, giving examples and a legal overview of what is happening in South East Europe. This started long before the disinformation that we know today. One of the reasons why I deal with media law is that the things we could hear/see on TV back in the 1990s was completely different from what we could see in reality.

Media literacy is still very important and perhaps more so for older generations today, in terms of recognising disinformation and what media/source of information to trust/not trust.

Let me raise the question from an academic/policy point of view: Who deals with disinformation? We heard there are so many actors who are dealing with it. There is the Government, but who is the Government and whose Government is it? What do we do with disinformation that travels between states? What is the role of parliaments, prosecution/the courts? We have seen that they are not very proactive in addressing disinformation even when it is weaponized and can pose a real threat. We also have a lot of female journalists who are receiving online threats when carrying out their work. What about regulatory authorities and the media themselves?

There was a “cry for help” by Mark Zuckerberg back in 2019 calling for state regulation. In academia we have two different poles, one thinks that social media should be regulated by governments, and the other thinks they should be self-regulated. Now we see a change in ownership of Twitter – will that shift the policy towards what is allowed/not allowed?

The UK was the first government to call on their ministers and the public not to use the term “fake news” – in 2019 – but instead use mis/disinformation as news cannot be “fake”.

We know of Article 10 of the European Convention on Human Rights (ECHR) on freedom of expression and that it can only be restricted in certain situations, and the restriction must be prescribed by law, have a legitimate aim and be necessary in a democratic society. There is also protocol 1 of the ECHR, Article 3 on the right to free elections, which prescribes that every country has to hold free elections at reasonable intervals by secret ballot, and should ensure the free expression of people in the choice of the legislature.

The Council of Europe has provided recommendations on measures concerning media coverage of election campaigns and manipulation of opinion polls. Often, when polls are conducted, you do not know who arranged them or what methodology was used, this makes it easy to manipulate people and to spread disinformation about poll results before the elections.

Political advertising is one of the ways of spreading false information. Free airtime and presence for political parties/candidates is sometimes not used equally or the information provided is not accurate.

There is also paid political advertising. In the region, in the last 10 years, we have heard complaints about small political parties that lacked sufficient funds and could not access the market.

Regarding news and current affairs programmes, there is a major issue here, whereby TV is still the main source of information for many, especially during elections. If you watch and compare pro-government and independent news you would hear completely opposite stories, which creates confusion among the public and the audience. There is often no reaction from the regulatory authority. Entertainment and other programmes are not specifically regulated during election campaigns in the region.

We have infotainment programmes: a format that mixes entertainment with news programmes, which requires a higher attention about disinformation/misinformation. The same applies to satirical programmes.

There have been examples in Montenegro and Croatia this year. The former often has disinformation originating from Serbian media outlets. The Montenegrin regulatory authority has reacted and has banned TV stations coming from Serbia because of disinformation.

In Croatia, right-wing portals accused the country's main fact-checking media organization of censorship, but it actually revealed false information and received threats as a result.

The regulatory framework for disinformation in Serbia is non-existent. It does not regulate disinformation, it only has a positive obligation that media and journalists are to report truthfully and provide accurate, verified information.

There is still no proper regulatory framework to fight disinformation in South East Europe. Some of the main issues that we should tackle relate to media spreading disinformation and institutions' lack of response. What about online media where we cannot determine who the authors of disinformation are? How to deal with broadcast of opposing information on state-owned/state-controlled media and independent media? How to regulate social networks? What to do about enforcement? We need legal standards together with strong enforcement mechanisms.

**Giuseppe Milazzo**

**Research Associate and Senior Media Analyst of the Osservatorio di Pavia (Italy), consultant of OSCE/ODIHR on media and elections**

The online environment is a fertile ground for spreading and disseminating (election) disinformation, as well as for freedom of expression. It has provided exceptional opportunities for voters to receive information, for candidates to spread information about their electoral programs, and for media to spread information about elections.

Censorship and online surveillance cannot be the answers to address online (election) disinformation, but research and monitoring efforts are needed. The question here is how can States and other sectors of society respond.

Media freedom, pluralism and independence, as well as quality journalism, public awareness and media and digital literacy are antidotes to (election) disinformation. I understand that digital literacy might be perceived as (more) effective in the long run. Our experience with the schools has been promising, due to a generational capacity to understand the internet, on the one hand, and a higher resilience towards disinformation narratives in high schools, on the other.

The True/False paradigm is not conducive to positive solutions. A focus on “dangerous disinformation” causing serious harm and undermining election integrity should perhaps be advisable. Defining the “truth” is not only a complicated philosophical issue, as a practitioner I have found that it is not easy to identify a common agreement on specific cases, but this is not necessarily the core of the debate. The right to freedom of expression also obviously includes the freedom to hold and express a belief or faith.

Long-term processes affect the receptiveness of a society to false narratives, social and cultural factors being the main drivers (cause-effect dilemma). Transparency, due process and privacy protection are key elements to improve the online sphere, to make voters aware of the nature of the messages and regulators more effective in monitoring online campaigns.

Characteristics of the online environment that may inflate disinformation include:

- The potential scale, reach, speed and pervasiveness of disinformation, including low barriers to entry (if any), along with personalized content and targeted micro messaging.
- The permanence of messages, users’ (perception of) anonymity, and the cross-jurisdictional character of the internet.

New technologies make manipulation, fabrication and dissemination of content simple (AI and automated tools) easier. Platforms, in their turn, become a fertile ground for computational propaganda, echo chambers, polarization, and hyper-partisanship.

The ability of political parties/candidates to bypass journalistic mediation, avoid scrutiny and reach audiences directly is paired with a decline of trust in mainstream media. There is inability to easily debunk disinformation once it has gone viral; limited access to platforms; and rise of instant messaging and closed group chat.

Some of these issues are clearly worrying for analysts and policy-makers. We should also recall that many of these characters could be used in a positive way, not just for malicious purposes. Some of them may even be used to counter malicious practices.

Pending issues/challenges:

- There is no clear or consistent definition of disinformation (among practitioners and in international law).
- There is a shortage of specific OSCE commitments or other relevant standards on disinformation and elections.
- There is also a lack of clear evidence about the scale, dissemination or effects of disinformation in elections; the correlation between disinformation and voting behaviour is not proven.

We also see a lack of consensus among practitioners about whether the different kinds of disinformation should be tackled with extreme measures (content restrictions) or soft measures (self-regulation, media literacy, fact-checking initiatives).

The “urgency to solve the problem”, in order to prevent harm, becomes critical with the unintended, or sometimes intended, consequences of the measures adopted to address the disinformation dilemma, including the chilling effects on freedom of expression and privatisation of censorship – delegating private companies to remove (legal) content.

Some aggressive practices are not necessarily false, but aim at causing harm during elections. On the other hand, some false narratives are harmless. Some disinformation practices are also dangerous for their divisive impact, rather than their misleading content.

As election observers, we desperately need more consistent definitions and commitments, as well as more shared views from the research community. An important step we are keeping an eye on these days is the finalization of the EU Digital Service Act (DSA), not only because many OSCE participating States are members of the EU, but also because it is likely to bring a new regulatory approach towards tech companies and platforms.

### *International standards*

The contribution of the 2021 report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,

Irene Khan “Disinformation and Freedom of Opinion and Expression” provides key recommendations on freedom of expression online. Election observers must stick to this framework.

The right to freedom of expression applies to all kinds of information and ideas, including those that may shock, offend or disturb, irrespective of the truth or falsehood of the content. Freedom of expression may be restricted only in accordance with article 19 (3) of the ICCPR. Vague laws that confer excessive discretion [...] are incompatible with article 19 (3) of the ICCPR. The prohibition of false information is not in itself a legitimate aim under international human rights law.

Disinformation is problematic, but so are the responses of States and companies. State regulation of social media should focus on enforcing transparency, due process rights for users and due diligence on human rights by companies.

Companies continue to fail to provide adequate remedies for wrongful actions taken on the basis of disinformation or misinformation. Lack of transparency and access to data continue to be the major failings of companies. Data protection is key to reorienting the advertisement-driven business model of the digital economy, which drives the information disorder and related human rights abuses.

Diverse and reliable information is an obvious antidote to disinformation and misinformation. Media information and digital literacy empowers people and builds their resilience against disinformation and misinformation.

Despite the shortage of specific international standards on election disinformation, we do have quite clear recommendations from international bodies in relation to the right to freedom of expression. These authoritative interpretations are not formally “legally binding” like treaties are, but they still provide us with quite clear guidance on these issues. As election observers, we cannot move away from this framework.

### *Key recommendations*

Any restrictions on speech must be regulated by law and pass the three-part test of legitimacy, necessity and proportionality. The principles of freedom of expression should not enable restrictions on the basis of false content alone. Permissible restrictions include advocacy of hatred that constitutes incitement to discrimination, hostility or violence (as per the ICCPR).

Platforms should be responsible for transparency and non-discrimination of their algorithms, for clearly labelling sponsored content as such, for identifying and disabling fake accounts, for protecting the privacy of users, and for increasing transparency in campaign expenditures.

Civil society fact-checking initiatives have proven effective in countering disinformation narratives, while state-run fact-checkers cannot sufficiently



demonstrate their selection criteria, due process and systematic methodology, which makes them vulnerable to criticism. Media pluralism and media literacy are long-term but effective antidotes to counter the dangerous effects of disinformation.

Micro-targeting based on sensitive information violates human dignity, the right to freedom of (truthful) information, and distorts public discourse – consent by the user should be required. Now technologies and platforms make individuals vulnerable to having their personal data exploited.

### *Disinformation and election observation*

Bearing in mind limited resources, period of observation, and technical expertise on data protection, as well as the mandate of OSCE/ODIHR Election Observation Missions and Observers' Code of Conduct, what can we do?

We can assess several factors including:

- respect of fundamental freedoms, including freedom of expression online;
- legal framework for online campaign, advertising, privacy and data protection;
- freedom and diversity of the online media sphere;
- election campaign of contestants on social networks;
- online campaign advertising;
- role of EMBs and other oversight bodies; and
- response of legacy media to election disinformation.

It is implicit what we should not become or be perceived as institutional fact-checkers. We should not comment on the truthfulness of opinions/value judgments expressed by political contestants. We cannot precisely quantify the scale of disinformation narratives in the information ecosystem and we definitely cannot interfere in any way with election processes.

## **Discussion**

### **Vladimir Misev**

Regarding data protection – advertising and financing of campaigns – disinformation cannot be treated in a vacuum, but must be seen in a wider context, whether talking about foreign or domestic disinformation, and whether same standards and principles can apply to these types of disinformation. As we accumulate knowledge we will be able to provide answers to these questions. Today, a document was published, a Declaration for the Future of the Internet, sponsored by 60 countries, of which many are OSCE participating States, which specifically mentions the issue of disinformation. As more of these kinds of documents are developed, including the Joint Declaration of the special mandates, we will have more ground to tackle these challenges.

*Q. What could have easily been done to address the problem of disinformation?*

**Yves-Marie Doublet**

About the experience of the last presidential elections in France, this year we did not observe foreign countries using digital platforms to influence the electoral campaign/vote. There were two reasons for this: first, the attention has been captured by other targets in other parts of Europe. Second, the pressure of foreign platforms in electoral campaigns has perhaps decreased, as pressure on conspiracy movements through digital movements has increased. We do not have much insight to appreciate this phenomenon, but this is the conclusion of the electoral integrity project, which was launched by Harvard and Sydney universities.

Now it is more efficient to favour more permanent conspiracy theories rather than to interfere every four to five years in the campaigns. It is more efficient in the long-term to keep the “background music” than to just have a “musical performance”. And it is easier to establish a legal framework limited to disinformation related to electoral campaigns, than to set out a general legal framework on disinformation.

**Jelena Surčulija Milojevic**

I wonder if the German way, NetzDG, is the right way, to make platforms accountable to law. Do we need to have our own national legislation in place in order to tackle hate speech? My appeal would be to put more energy into not only norms but also that the regulation includes strong sanctions and empowers institutions to enforce such norms. Free speech has its limits. We need to have access to accurate information.

**Giuseppe Milazzo**

Transparency and data protection are key elements in the fight against disinformation. There are too many cases of unlawful content removal of legal content, and of legislation that is not in line with international standards.

A divided society and weak media system are fertile ground for disinformation to spread. In a strong one, you have the antidotes.

The finalisation of the EU Digital Services Act is important, not only because many OSCE participating States are members of the EU, but also because it is likely to be a new regulatory approach, a new model of tackling the issue with the platforms.

Going back to what Jelena was saying, there was a link between disinformation, COVID-19 and elections, and traditional media, with candidates spreading disinformation during elections in traditional media. The problem is very complex.

**Brenda Santamaria**

A multi-stakeholder approach is the key. As citizens we are responsible, too, it is right to put a lot of responsibility in institutions, EMBs are responsible for managing elections, but they are not the only ones. We have seen how even extreme regulations do not solve problems. Regulation has to be well analyzed on what the pros and cons are of having it and how it will be applied. Who is able to monitor everything during elections? It was easier with traditional media, but with social media it is more challenging.

**Mikheil Benidze**

We are in a much better position now that we are talking about these issues, and specific methodologies and guidelines, including by the OSCE, which now speak to the issue. This will improve over time as it is a new field, but a few years ago, when we were first realising the need to go beyond traditional media and monitor social media with more emphasis on disinformation, there were no methodologies and good practices to learn from. As you know, monitoring social media is challenging as it is not so easy to sample and adopt the same methodologies that work for traditional media.

Second, what is positive is that there is an overall recognition of the problem of Russian disinformation or hostile actor disinformation. This is no longer perceived as paranoia by certain actors, but there is a realisation that this is something serious and does not concern just a specific region. In the context of Georgia, Russian disinformation would not likely undermine society if there were not also this domestic polarisation, divided society. That is where the key vulnerability lies. External factors need to be kept in mind, but there is also a need for internal/domestic resilience. This requires political will and good faith, without trying to manipulate the information environment to one's own end. The key is to realize and recognize how these domestic operations undermine that resilience. As for the regulation, it needs to be tailored to each individual country. In countries with totalitarian past, we will be careful with any regulation of freedom of expression, media freedom and free speech because of past history/legacy.

I would reiterate the need to co-ordinate and work together with different actors, which can contribute to resilience. In this context, it is also important to have consistency and investment from international development actors and donors, when it comes to civil society and quality media. Adversaries who create and spread disinformation do so consistently and with large financial resources.

We need to have strong and consistent investment in civil society and media. In today's commercialized and sensationalist world, it is hard for quality media outlets to maintain professional journalism without such support.