COMPACT CSA Project

Symposium
Disinformation in the European Elections 2019:
The role of social media & technology trends

21 October 2019, Brussel, Belgium

At the Permanent Representation of the Slovak Republic to the EU
Organised by the European DIGITAL SME Alliance as the local partner with support from COMPACT project partners

Report

Introduction

The conference focused on the extent to which the measures proposed by the European Commission in advance of the elections have been successful. The discussions addressed what else could be done to make sure the electoral system, social media legislation and online political advertisement fit the digital century. Also, preliminary findings from the COMPACT project were presented, such as the mapping of technological, regulatory and policy developments in social media and convergence. The symposium brought together policymakers, academics, NGOs and other stakeholders to discuss how to make social media and our democratic discourses more resilient to extremism and disinformation, especially in light of elections.

During the introduction of the symposium, **Ambassador Tomáš Kozák** welcomed the guests, stating that the outcomes of discussion of the event will help to formulate future policy recommendations.

The 30th anniversary of the Velvet Revolution represents an important milestone in the history of Slovakia, before that period, the whole society was deprived of information and freedom, people were craving to get informed on what was going on in the world. Nowadays, the situation has changed dramatically, in the era of social media, society is overwhelmed by information, meaning that it is not always easy to select what is right and what is wrong. This disinformation emergency in reflected in the spread of information in Twitter in the context of the election panorama: the probability of disinformation to be shared amongst users is 70% higher when dealing with a fake news, secondly, fake news reaches the audience 6 times faster than the real news, and finally, fake news with a notion of scandal picket faster than real news. Enough to say, the society of information faces major threats.

In the Slovakian context, the 2013 International Security Agency Report highlighted that hybrid threats and disinformation are the major security threats that impact society. In parallel, GlobSec conducted a report about the major worries of citizens, placing "migration as a threat" and "EU dictate" as the top disinformation topics in campaigns and slogans in Slovakia. As previously mentioned, in Slovakia disinformation and hybrid threats are identified as the major key issues in security threat. As a response, the MFA department for strategic communication, charged to address and respond to the threat of fake news by spreading positive ones, other activities of the department include the #WeAreTheEU campaign which travels visiting schools and answering questions by students.

Regarding the EU context, over the last couple of years, disinformation has gained a more prominent role in the agenda of the European Commission and decision-makers. Over numerous discussions, disinformation has been classified as a strategic challenge, it is seen a side-effect of the digital revolution. There is a general conception that the internet trolls and third actors are the ones to blame for disinformation, but it is also the representatives of government and policymakers who are at fault for not apprehending the issue as a crucial one in the top of the interests of the agenda. [for not setting it as a top risk on the agenda]

The EU has developed an action plan, but the implementation has unfortunately not been regarded as a top priority by policymakers. The responsible unit in the EEAS is highly understaffed and calls to member states have remained unresponsive to the call. However, there are also a lot of positive initiatives that work well, such as the Centre of Excellent on hybrid threats in Helsinki. Slovakia has taken step to take part in this centre of excellence (25th member).

The Ambassador Tomáš Kozák closed the introduction with a few recommendations from his side. Firstly, there is a need for a better mapping to know which actor is doing what, and overall, better-staffed actors are needed to respond to disinformation. Secondly, create partnerships, especially between Balkan countries, which are the most heavily affected countries by disinformation. In that sense, hybrid and disinformation must be put as a standing point in the Agenda. Lastly, there is a need for a collective change of mindset, in the words of the Ambassador, “those who spread disinformation use sophisticated techniques and so should we”.

COMPACT SYMPOSIUM
Disinformation in EU elections: The role of social media and technology trends

First Panel

What lessons can be learnt from disinformation in the European Elections? How effective has the voluntary code of practice been, do we need to do more? This session examined how effective the voluntary code of practice has been and if there is an urge to do more. The panellists approached the good lessons to be learnt about what can be done in terms of addressing the phenomenon of disinformation and its effects on public opinion.

Discussants:

- Chair: **Paolo Cesarini,** Head of Unit, Media Convergence and Social Media at DG CNECT, European Commission
- **Alexandre Alaphilippe**, Executive Director, EU DisinfoLab
- **Ľuboš Kukliš**, Chair of ERGA and Executive Director at The Office of the Slovak Council for Broadcasting and Retransmission (CBR)
- **Raphael Kergueno**, Policy Officer, Transparency International

First panel (from left): Lubos Kuklis, Paolo Cesarini, Alexandre Alaphilippe, Raphael Kergueno.

Dr. Cesarini introduced the topic of discussion and the context of the panel. There has been a stepping up in the dialogue with private actors, particularly with online platforms. Disinformation is a multi-faceted problem, threats come from both the outside and the inside of the EU, shaping the creation of public opinion. There has been a shift from external to internal threats and vice versa, meaning that it is now difficult to make a clear and neat distinction between both the origins and the actors that are behind the orchestration of campaigns of disinformation. Hence, there is a need of having the civil society fully on board in order to tackle disinformation into a wider and societal approach.

The EC has created a platform to address three crucial issues: a) <u>transparency of advertising</u> that revolves around topics of social interest by labelling sponsored content, to take robust actions against actors that manipulate the space with different techniques (fake accounts, coordinated groups deployment that create distortion), b) <u>sponsored content,</u> c) <u>scrutinizing of</u>

ads, strengthening systems of ad-scrutinizing in order to avoid advertising revenues that are being exploited to use information in a clickbait disinformation manner whose sole purpose is to collect clicks and make money. Finally, Mr Cesarini highlighted the need for more accountability and to protect user's privacy.

Dr. Alaphilippe focused on the investigations that have been made to address disinformation campaigns and operations, as well as some recommendations to fight disinformation.

Disinformation is a multi-form phenomenon; it doesn't always have the same shape or form. What happened in 2016 in the US election is very different from nowadays, in that sense, there has been a shift from the expectations of foreign interference on social platforms disrupting elections to national.

By looking at trends in the EU elections campaigns, some facts about the prevalence of disinformation can be noticed. These movements are very structured online and are able to put their recommendations on top of the suggestions when looking for information on Google. This is reinforced by the fact that mass human behaviour can change the way disinformation is displayed online and can change how said information is accessed. The fact that information is based on personal recommendations, the more a user clicks on disinformation news, the more these are going to be recommended. This is because there is an interest from the platform to distribute content prone to be consumed. All the content-related platforms are connected, and the algorithm is working to attract viewers and get their interest. In that sense, Clickbait is powerful to attract people and voters, especially at times where you don't know what's happening.

Following that line, the intention of bad foreign actors is in many cases to establish an atmosphere where no one believes anything, nothing is checked or verified**,** the absence of a trusted voice, the inability of certain groups of the population to distinguish between the real and the unreal world online. In Mr Alaphilippe words, *"Once you don't believe in anything else, you rely on what you see on the internet".* Further, an emotional debate can be easily turned into the weaponization of disinformation and to fuel hate. Finally, there is a competitive advantage between fake-providers and journalists, the time for a journalist or a fact-checker to write an article is ten times greater than writing about disinformation.

Alaphilippe concluded the discussion by stating it is not much about content regulation, but about content distribution, in other words, the role and impact of algorithms and IA in recommendations.

Dr. Kukliš stated that although the approach of the European Commission has a crucial role, the Code of Practice does not state clear objectives. Until the revised Audiovisual Media Services Directive (AVMSD), there were no competencies for the NRA.

During the process of monitoring, some issues about the context of disinformation campaigns in the EU elections have been brought up to the table. Experts address two necessities. Firstly, there is a need to get researchers on board to understand the problem, especially now that there is an audiovisual directive at the table that has to be implemented by all member states. Secondly, transparency is crucial in the process, there is a difficulty of verifying data and mapping the environment in the context of EU elections. Data has to be ensured in the platforms by NRA and actors with competence over the matter. An authority is needed to mediate/address the issue, but it problem lays in that the authority needs to be accountable, and the privacy of the users has to be ensured.

To conclude, the panellist called for a comprehensive approach on the phenomenon, and to find a solution with the help of Social Media researchers on boards of the National Regulatory Authorities (NRA) in order to mediate with the phenomenon of disinformation. Finally, there is a short- term goal to be addressed immediately, the lack of a common definition of political advertising in Europe. Instead of every member state having their own definition of political advertising, there should be a harmonised definition common to all its members, so cooperation can be made, and regulation authorities can impose on the platform to follow the same rules for every State.

Mr Kergueno stated the need of looking at the Code of Practices from another angle, coming from political integrity.

The panellist addressed the study made about money and politics, with a common regulation of how the money flow works in political systems, the Member States can be free of outer-influence, and the money used to influence the political process can be ensured to be spent under the principles of transparency and accountability. Regarding this, **political finance regulation and control** is a mechanism that guarantees that the elections are fair (equal opportunities are given to all the political parties and actors to compete), clean (the money spent in the political process comes from authorised actors) and clear (the money flow into the elections is accountable and its tack is kept)

In political advertising, there is a set of clear rules about campaign regulations in the EU members states, but there are some issues about addressing social media in campaign regulation, in fact, not a single member state has in their national campaign finance rules provisions on online political advertising. This is due to the fact that the rules that address campaign regulations were made for the 20th century media panorama, and they are being applied for platforms that work in the context of the 21st century. Some examples can be seen below:

- The spending limits and campaign finance control ensures that every political actor spends the maximum same amount of money in the political elections, so no political parties have the ability to outspend and influence the elections in their favour. In social media, it is peculiarly difficult to track how the money is spent online
- The rules guaranteeing impartiality and equal airtime, a 20th century concept that addresses traditional media and broadcasting to ensure that the same amount of time is given to every political actor. In social media it is very difficult to implement this.
- The National campaign finance laws – in which countries have to mention their provisions on online political advertising is only being implemented in three national member states.

Most member states don’t have specific legislation on online political ads. The panellist called for a single common definition in the EU on what is online political advertising. With a single definition at the EU level, it would be easier to ensure that platforms respect national law, considering the said mentioned platforms operate in all member states.

The Code of Practice is the first step to bring transparency and accountability of spending in political finance and regulating political advertising. The three major platforms have signed it and are now implementing the “Ads-library”, in which the money flow and advertisers are shown.

The expert concluded his session with some questions: can the Code of Practice function as a political finance regulator to ensure that spending limits are respected? How can we encourage member states to introduce specific legislation on online political ads?

Second Panel

Misinformation, disinformation and hacking are some of the threats that the EU elections face. Who are the players behind this and what can be done about these threats? This panel will provide an overview on the types of disinformation and misinformation threats in elections, to identify the main players, the role of external influence and populism in Europe.

Discussants:

- Chair: **Lutz Güllner**, Head of Division Strategic Communications, European External Action Service
- **Martin Gajdoš** from the Slovak Ministry of Interior, Dept. of Elections, Referendum and Political Parties, Slovakia
- **Miroslava Sawiris**, Globsec NGO, Slovakia
- **Florian Pennings**, Cyber Security Policy Manager at Microsoft Brussels, Belgium
- **Rasťo Kužel**, MEMO 98 (specialist media monitoring organization), Slovakia Co-funded by the Horizon 2020 programme of the European Union

The second panel (from left): Martin Gajdoš, Miroslava Sawiris, Lutz Guellner, Rasto Kužel, Florian Pennings.

Mr. **Güllner** called for a coordinated approach and a clarification of objectives both externally and internally -nation-wise- to detect disinformation, in commercial and political advertising, and to identify the actors behind the disinformation campaigns. It is to be stated that the lack of data is one of the main problems in the disinformation issue that affects EU elections.

The panellist mentioned that disinformation comes in a broad spectrum, and that not all disinformation may be necessarily false. To be included as disinformation, it should include: **a)** clear intention ; **b)** coordinated action; **c)** clear objectives.

Finally, the expert raised the following question: when speaking about disinformation, is there an impact that we can measure? In his opinion, the disinformation issue is multi-faceted, and in that sense, an important factor to combat disinformation and the lack of data is to connect governments and the civil industry to tackle the issue.

Mr. **Pennings** stated that the role of nation states is increasing, the majority of cyber-space technology is in the hands of private organisations, and public and private corporations are constantly brought to the table to discuss responsibility issues about the cyber-technology pattern. Following that line, in 2017, Microsoft decided to conceptualise the cyber-space from a new paradigm, stating that private companies and nation states must work together to tackle issues that might fold, and to create a framework in which citizens, the industry and the civil society could participate and could contribute in the discussion about the opportunities or issues that the cyber-technology might bring.

In 2018 thirty large companies came together on a global scale to create a set of common norms, good practices and investing necessities in order to secure and stabilise thee cyber-space. It is important to set in the agenda that the companies who own cyber-technologies have a common responsibility. In the words of the Mr. Pennings, Microsoft has already understood this necessity and is investing in protecting campaigns, in safeguarding elections and to defend against disinformation trends.

The panellist concluded his session by stating that in order to measure the impact of disinformation and combat it, the society needs to promote a responsibility-sense on the issue, and this starts with education. Only with education there will be a constant effort to create a safe and trustworthy environment to defend the values of European democracy.

Mr. **Kužel** talked about the role of social media the elections, stating that although disinformation has been present in every election campaign, everything changed since the 2016 elections. Indeed, the emergence of social media changed the means of how information is spread, the new media environment is capable of amplifying the information and reaching millions of people instantly. In that sense, social media should me monitored during the elections, and in top of that, the whole methodology of monitoring should be revised: instead of an approach that focuses on the messenger (political actors, media, influencers), the message and the messaging (the ways in which messages are amplified) should be included in the monitoring analysis.

Although there should be a monitoring of social media elections to control the spread of disinformation, it is not quite possible to measure the impact of disinformation and the spreading effects of social media. It is crucial to understand the differences in the various EU electoral systems, and there should be a comprehensive research and data on the disinformation trends to try to tackle the issue with a comprehensive and efficient approach.

Mr. **Gajdoš** started by giving an example about a Facebook disinformation campaign during the Slovakian election day, in which a well-known disinformation media group posted an article stating that over 100,000 voters licences were falsified. Although it had no basis, it was shared by over 85,000 users. When this event occurred, Mr. Gajdoš himself was a member of the State Commission on Election Control, they decided to simply ignore the post to not give it wider public credibility. Ironically, the Police decided later that there was no breach of law.

How do we prevent such situations? It would be useful to create a database of political ads online for transparency, but it is difficult to create legislation around the topic. In Slovakia, however, there are guidelines on how to proceed in controversial cases. More guidelines should be needed, as there is a clear need for having guidelines to know when to do what, but again, it is hard to regulate disinformation in social media platforms.

In his working group, they are working on an approach to the public opinion polls, as those are a strong tool to approach voters and to create public opinion. Currently, they are working on a definition of public opinion poll and they want to create some standards about how it should look like, what information should the public get. One way to regulate things is to put the responsibility on the online platforms not just the political parties and candidates, because the platforms are part of the problem.

Mrs. **Sawiris** spoke about the information operations' impact on democratic institutions and on the public. Disinformation is only one aspect of information operations. There are two goals in terms of information operation: the first one can be immediate, such as trying to discredit particular political candidate. The second, the long term one, strives to undermine trust in democratic processes and democratic institutions.

The panellist highlighted the tactical change observed between the recent Slovak Presidential Election and the EU Elections. Instead of an easily identifiable disinformation deployment, dissemination of divisive narratives targeting LGBTI community or refugees have become more prevalent and efficient means of public manipulation. As an example of typical disinformation campaign, the researcher mentioned the photoshopped picture of the Slovak presidential candidate which attempted to suggest that the candidate had Semitic features. This example demonstrates that these campaigns are tailored to tap into pre-existing fears and stereotypes of the target audience, in this case the Slovak population, as 52% of them believe that 'Jews have too much power', (according to GLOBSEC Trends data 2018). However, the ease of divisive narratives spread is enabled by the recommendation algorithms on social media which favour sensationalist content. This significantly contributes to the growth of social polarization and increasing lack of trust in public institutions.

About measuring the impact of disinformation, the expert stated that there are always other factors that come to equation. But in Slovakia they have public opinion polls and the one in 2018 was focused on conspiracy theories. They do not have enough comparable data yet, but some quite astonishing numbers and proportion of people believing in conspiracy theory could be found there. Although the impact of disinformation cannot be measured exactly, it is clear that it is being used in mainstream politics.

During the round of questions, a Croatian researcher exposed the problem of microtargeting wanting to know what is being made about the problem of microtargeting. In the opinion of Gajdoš, microtargeting does not represent an issue at its base, the problem is that one candidate can target one group with one personalized message and the other group with something completely opposite. In that sense, the message that they are targeting with should be made public, and microtargeting should be more transparent but not forbidden.

Mr. Kužel also exposed the importance of transparency, the bait content should be clearly labeled. For the panellist, microtargeting is a big problem and GDPR in this matter is a step in the right direction. He stated that there should be bigger focus on microtargeting and data protection. Mr. Florian Pennings stated that that the focus should be done on exploring how to educate those first respondents to identify what is happening. Disinformation and misinformation require different angels.

Finally, Mrs. Sawiris spoke about the issue of transparency. Some kind of measures need to be put in place, because it is hard to get access to data at digital platform and it is lost very quickly.In her opinion it shouldn’t be up to digital platforms and their good will to provide said data, it should be provided in a transparent manner and accessible when requested. The expert stated there should be regulation in which political parties would be required to list all the ads placed as well as who they targeted. It should be ideal to have the same list from social media companies so the researchers could compare the data and see the real picture. Mrs. Sawiris concluded that answering disinformation with disinformation would contribute to the kind of atmosphere where we can’t trust anything anymore.

Recording: https://twitter.com/projectcompact/status/1186237273110695936?s=20

Third Panel

Discussion of COMPACT findings: Overview of regulatory initiatives and suggestions in Europe and beyond in the area of “Information disorder and social harms” Presentation by the consortium on some preliminary results of the project.

Discussants:

- Chair: Dr. **Lukasz Porwol**, Deputy leader at eGovernment Unit, Insight Centre for Data Analytics, NUI Galway, Ireland
- Dr. **Tanja Pavleska,** Laboratory for Open Systems and Networks, Jozef Stefan Institute, Slovenia
- Dr. **Andrej Skolkay**, School of Communication and Media, Slovakia
- **Oles Kulchytskyy**, Agency of European Innovations, Ukraine
- **Munir Podumljak**, the president, Partnership for Social Development, Croatia

Third panel (from left): Andrej Skolkay, Tanja Pavleska, Lukasz Porwol, Munir Podumljak, Oles Kulchytskyy

Dr. **Školkay** presented the findings from Compact Project. He spoke about the global debate on the prospects for social media legislation, and introduced all the sectors covered by the research, the follow-up to the symposium in Budapest. It can be observed that there has been a shift from standard legislative approaches to rather novel approaches, such as based on behavioural economy and technology. These analysis and findings are available in a written form.

The observations have not found enough understanding of the said awareness among the majority of state institutions in the EU M. S. responsible for SM regulation. The questions addressed to the challenges related to bots, immersive technologies, online digital identities have not been answered from their behalf. Mr. Školkay concluded by asking for an approach to regulate the data on social media

Dr. **Pavleska** reviewed the Social Disorder research, covering 140 initiatives to detect and combat disinformation and manipulation on both social networks and the public sphere in 24 different countries. The panellist stated that it was difficult to get some information about the initiatives, when it comes to stakeholders and to funding, she put the example that, fact-checking initiatives are often funded from one source. She also addressed that some of these information required lacked clear objectives, accountability and transparency in their methodology. According to the expert, social media are different from traditional media and therefore need a different approach to regulation.

Mr. **Podumljak** presented the preliminary findings of pre-standardisation initiatives. He addressed the issue about if standardisation is a solution or a constrain for development. Some examples from the industrial history and technology were addressed, but in the digital industry, everything has shifted. There is a need for an Industry Best Practices Code. The panelist concluded by stating that the standardisation process has to be transparent and meet ethical requirements.

During the round of questions, the topic of algorithms was addressed, and it was stated how balancing ethics, ethical guidelines and space for innovation is very important.

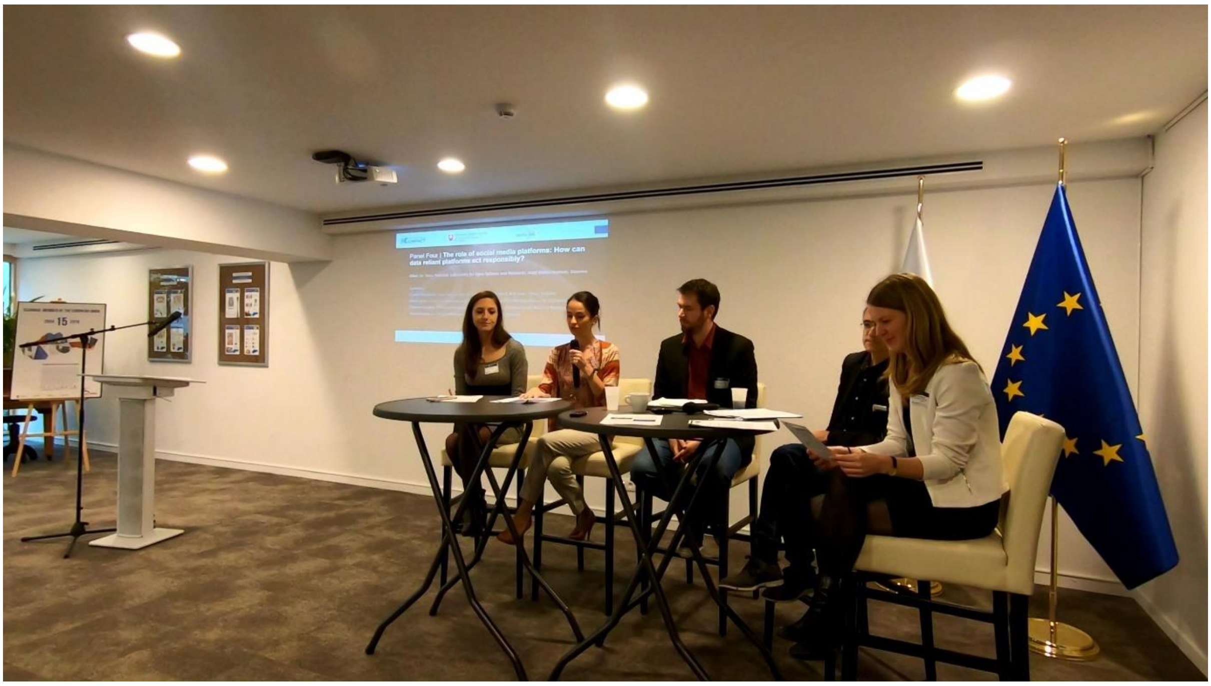
Recording: https://twitter.com/projectcompact/status/1186280052369084416?s=20

Fourth Panel

Role of social media platforms: How can data reliant platforms act responsibly? How can social media platforms be responsible players if their business model relies on collecting information on their users and to sell targeted advertisement?

Discussants:

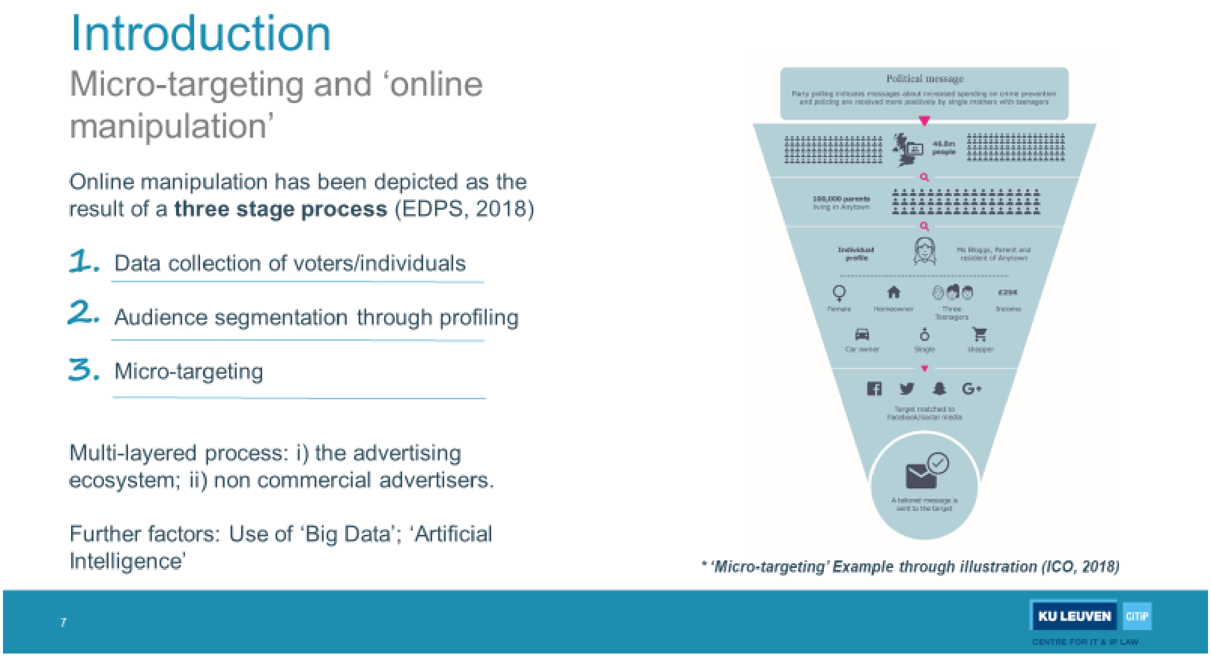
- Chair: **Dr. Tanja Pavleska**, Laboratory for Open Systems and Networks, Jozef Stefan Institute, Slovenia
- **Elisabetta Biasin,** Legal Researcher, KU Leuven Centre for IT & IP Law – imec, Belgium
- **Paolo Celot -** Founding Member and Secretary General, EAVI – Media Literacy for Citizenship
- **Thomas Carette,** Independent Data Scientist & Organiser of Data Science Brussels Meetups, Belgium
- **Annika Linck**, EU Project Manager, European DIGITAL SME Alliance



One recurrent problem with disinformation and misinformation is that information follows an attraction spiral; sensational content has more reach than “normal” content. At the same time, social media platforms build their algorithms in a way that favours this type of content. Therefore, the symposium also addressed the question of the business model of social media platforms—**how can actors behave responsibly when their business model builds on generating revenue from advertisements?** Smaller companies in the digital sector provide tailored and hands-on ICT solutions to their business partners, while some large platforms build their business on advertisement and understanding human behaviour by collecting huge amounts of data. Regulatory proposals such as the Digital Services Act provide comprehensive regulation that want to address the societal risks associated with large platforms, but that may have a negative effect on the business models of our SME companies.

Mrs. **Pavleska**, as the chair of the session, talked about data availability and raised questions about ownership of data when it comes to clouds and encryption as a solution for secure data storage. Then she gave the floor to the other participants by raising a question to each of them.

Mrs. **Biasin** spoke in more detail about the Cambridge Analytica Scandal and about the topic of her presentation: “Democracy disrupted? Continuing the debate on the (mis)use of personal data in political campaigning”. She started off by providing an insightful personal case study of information available about her online, and showing how this can be used for micro-targeting. By providing further information about the eco-system consisting of platform, she provided a general introduction about how this process can influence decision-making also during elections. Further, she explained the relevant legal frameworks and safeguards.



Introduction

Micro-targeting and ‘online manipulation’

Online manipulation has been depicted as the result of a **three stage process** (EDPS, 2018)

1. Data collection of voters/individuals
2. Audience segmentation through profiling
3. Micro-targeting

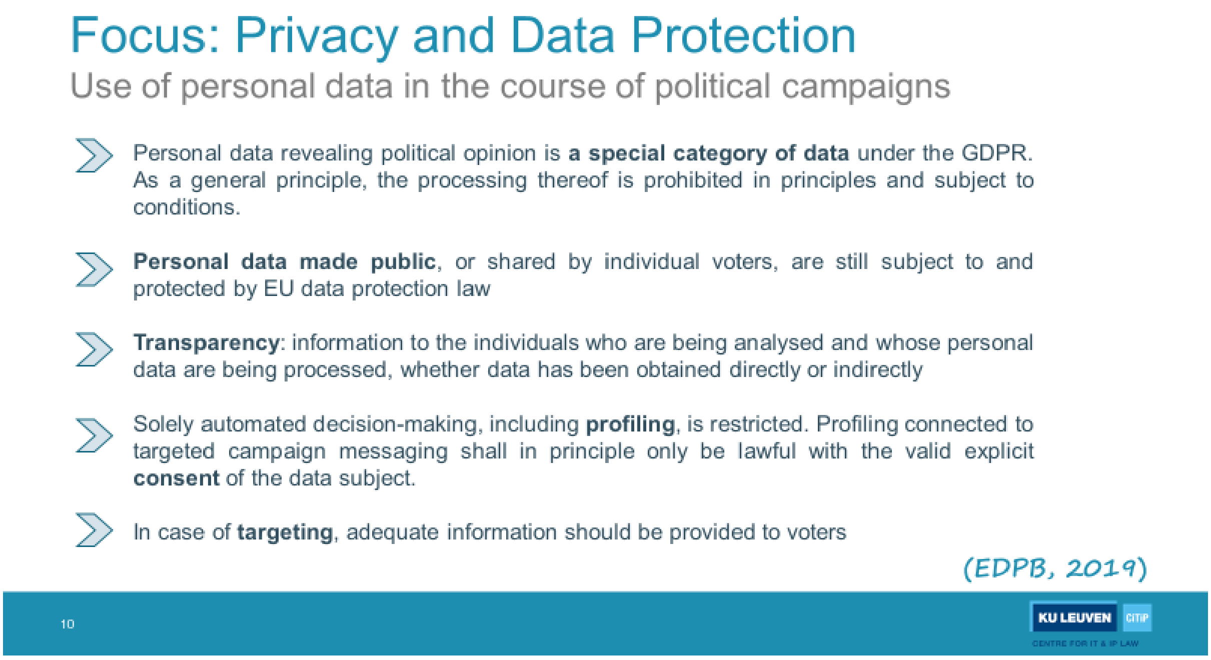
Multi-layered process: i) the advertising ecosystem; ii) non commercial advertisers.

Further factors: Use of ‘Big Data’; ‘Artificial Intelligence’

Political message
Party polling indicates messages about increased spending on crime prevention and policing are received more positively by single mothers with teenagers
46.8m people
100,000 parents living in Anytown
Individual profile
Ms Bloggs, Parent and resident of Anytown
Female
Homeowner
Three Teenagers
£25K
Income
Car owner
Single
shopper
G+
Target matched to Facebook/social media
A tailored message is sent to the target

* ‘Micro-targeting’ Example through illustration (ICO, 2018)

7
KU LEUVEN
CITIP
CENTRE FOR IT & IP LAW



Focus: Privacy and Data Protection

Use of personal data in the course of political campaigns

- Personal data revealing political opinion is **a special category of data** under the GDPR. As a general principle, the processing thereof is prohibited in principles and subject to conditions.
- **Personal data made public**, or shared by individual voters, are still subject to and protected by EU data protection law
- **Transparency**: information to the individuals who are being analysed and whose personal data are being processed, whether data has been obtained directly or indirectly
- Solely automated decision-making, including **profiling**, is restricted. Profiling connected to targeted campaign messaging shall in principle only be lawful with the valid explicit **consent** of the data subject.
- In case of **targeting**, adequate information should be provided to voters

(EDPB, 2019)

Mr **Celot** mentioned that all stakeholders including social media carry responsibilities. But we should not be too naive. We cannot expect them to behave ‘responsibly’ unless they are obliged to do so or they see a benefit for themselves. We should not forget that there are private companies, as such they aim at profit, not public interest. They are linked with political and commercial influence. Moreover, the magnitude of business here is huge. So, what to do? Obviously, regulation is necessary but probably is not sufficient per sé. Such large companies are well equipped to find loopholes and a way of pursuing their interests by employing large legal teams that help them navigate through the rules. These large companies are also gatekeepers of large amounts of data. In this regard, free competition rules could be an issue to be explored.

Mr. **Carette** said that ethics is not well defined in general. And if you do not define something, no one can be responsible in the strict sense. He also agreed with the previous speaker in that the responsibility is very difficult to trace to the origin of the problem. At the same time, it is difficult to regulate – you need the willingness from the responsible party to take ownership of the responsibility and ethics. However, in private companies and institutions, we try to be objective and we are driven by numbers. There are KPIs that can be short term, mid-term and long-term. But even the longest ones are only on a five-year basis. None of these however drive ethical conduct, but they only focus on money or costs of enforcing a regulation. Ethics need to be pushed to practitioners. You will always find someone who will want to make money for their company. In the end it's up to the users, it's enforced by the people and their public opinion. Companies try to mitigate the risk of loosing their customers by trying to be the good guys. They are driving innovation in what we think is ethical. These types of initiatives come from public opinion and education. Beyond regulation, governments can help perhaps by promoting standards – small companies need standards. Helping companies to establish the right standards and allowing data access, which could be promising.

In general, Mr. Carette believes that the only defence against unethical behaviour by companies is culture - the culture of the people outside of it, but also the one of the workers. If there is a culture of ethical behaviour in the lower ranks, it does still restrict a lot of possibilities for the more sociopathic management.

Further in the discussion, he touched upon the role of standards and technology for access to any market centered on data: In order to enable a affordable access to any market centered on user data, the norms and regulations need to be accompanied by investments from governments into accelerating software, technologies and standards; assets which lay the foundations for compliant data pipelines and are free of charge. The system as it is (regulations increasing risk but privatised development of compliant technology) converge into shutting SME out of the tech market at the moment. We see big tech companies investing millions (if not billions) in software and infrastructures that are compliant. They do that by developing a lot of it from scratch, often investing in research beyond what government funded academia has to offer. Another flourishing market is the one of consultancies which deliver more or less functioning solutions for very high prices.

Mrs. **Linck** presented DIGITAL SME's Manifesto for Europe Digital Future and explained that the business model of small companies in the ICT sector is very different from the business model of platforms, which largely rely on revenue from advertisement, which in turn relies on collecting personal information. When the legislator proposes new regulation, they often address this problem that arises from large platforms, but risk to harm small companies following a different business model at the same time.

To conclude, the experts talked about the GDPR and what the role of politicians is in introducing regulations.