Study on the impact of new technologies on free and fair elections

('Elections Study')

Literature Review

Version 3.0
March 2021

Document Control Information

Settings	Value
Document Title:	Literature Review
Project Title:	Study on the impact of new technologies on free and fair elections
Document Author:	Trasys International, part of the NRB Group
Project Owner (PO):	Ms Marie-Helene BOULANGER (Head of Unit) Ms Monika MOSSHAMMER (Deputy Head of Unit)
Project Manager (PM):	Ms Zuzana PUNDOVA (Legal and Policy Assistant) Mr Harry PANAGOPULOS (Legal Officer)
Contractor Project Manager (CPM)	Ms Dijana SPASOJEVIC, Head of Business Consulting
Doc. Version:	V3.0
Sensitivity:	Low
Date:	19/03/2021

Document Approver(s) and Reviewer(s):

Name	Role	Action	Date
Ms Marie-Helene BOULANGER	Project Owner	Reviewer and Approver	
Ms Monika MOSSHAMMER	Project Owner	Reviewer and Approver	
Ms Zuzana PUNDOVA	Project manager	Reviewer and Approver	
Mr Harry PANAGOPULOS	Project manager	Reviewer and Approver	

Document history:

Revision	Date	Created by	Short Description of Changes
V1.0	30/09/2020	Trasys International, part of the NRB Group	First version
V2.0	18/01/2021	Trasys International, part of the NRB Group	Minor updates
V2.7	08/02/2021	Trasys International, part of the NRB Group	Footnotes of summaries added
V3.0	19/02/2021	Trasys International, part of the NRB Group	Additional updates

Configuration Management: Document Location

The latest version of this controlled document is stored in:
https://pmo.trasys.be/confluence/display/DGJUSTELECTION/DG+JUST_Elections+study

Table of Contents

1. Introduction

This document presents an overview and analysis of relevant literature identified and reviewed in the context of a study on the impact of new technologies for free and fair elections. The following research questions were used in a search process: 'How using new technologies, such as artificial intelligence[1] and blockchain/ Distributed Ledger Technology (DLT)[2] and new online techniques, such as microtargeting[3] and algorithmic filtering[4], while relying on voters' data to create and disseminate online disinformation[5] and to target different categories of voters, could affect the outcome of the elections and the public confidence in them?' What are the possible threats and opportunities of these technologies when used in the electoral context? How to minimise the risks and maximise the opportunities of the technologies to strengthen the rule of free and fair elections as a backbone of democracy?

Main objective of the study is to examine how using data about voters and new technologies, including micro-targeting techniques, algorithms and artificial intelligence, can be used to affect the outcome of elections and public confidence in them. This would help ensure that the digital transformation and new technologies, such as AI and DLT, would be developing in line with European values of democracy and human rights. The European Commission contracted Trasys International, part of the NRB Group,

[1] In the context of this study, 'artificial intelligence' is a set of scientific methods, theories and techniques whose aim is to reproduce, by a machine, the cognitive abilities of human beings. Current developments seek to have machines perform complex tasks previously carried out by humans by means of Machine Learning/Deep Learning - empirical e.g. automatic learning of rules from past data; expert systems-rule-based systems (symbolic e.g. manually defined rules in a knowledge base), etc.

[2] In the context of this study, the term 'blockchain / DLT' instead of 'blockchain' is used. From a functional perspective, DLT should be used. Blockchain is a technical term referred to as the data structure most often used to implement an immutable distributed ledger. However, in mainstream use 'blockchain' is also frequently used as a 'bag word' for all technologies allowing to implement distributed ledgers. In the context of this study, the contractor proposes the following definitions:

- Distributed ledger = A ledger created and maintained across a set of nodes in a network by a distributed system.
- Distributed ledger technology (DLT) = any technology that enables the operation and use of distributed ledgers, including blockchain.
- Blockchain = The data structure of a distributed ledger implemented by a sequence of confirmed and validated blocks of data, organized in an append-only chain secured using cryptographic links

[3] 'Microtargeting' is a marketing strategy that uses consumer data and demographics to identify the interests of specific individuals or very small groups of like-minded individuals and influence their thoughts or actions. In the context of this study, "microtargeting" is understood as "online political microtargeting" and is a technique, often used by political parties and candidates in the form of personalised communication that involves collecting information about individuals and using that information to show them targeted political advertisements with the aim to convince them to vote for them.

[4] 'Algorithmic filtering' is the evaluation of data based on some formula. In general, all filters rely on some algorithm; however, the term typically refers to social media and search engines, wherein users are delivered ads, videos and news stories that appeal to their lifestyle and principles. Algorithmic filtering of social media news feeds, for political or economic reasons, may have implications for media pluralism, freedom of expression and exposure to diverse political messages. At the same time, algorithms can also play a positive role in fighting disinformation and promoting quality content.

[5] 'Disinformation' is verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Online disinformation campaigns, through social platforms (particularly, but not only, social media) are being widely used by a range of domestic and foreign actors to sow distrust and create societal tensions, with serious potential consequences. Disinformation is part of a wider array of tools used to manipulate electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians. Cyber-enabled operations may be used to compromise the integrity of public information and prevent the identification of disinformation sources. This is critical during election campaigns, where compressed schedules may prevent timely detection of disinformation and response.

via the ABC IV Framework Contract to carry out this project during the period of February 2020-March 2021.

Each reference included and analysed in this document was either suggested by the Commission, consulted stakeholders or identified based on the contractor's desk research. The selected references provide a good contextual framework and offer an excerpt of opinions and thoughts from different authors, regarding well debated concepts of disinformation, use of technologies and techniques, and related possible threats and opportunities in the electoral context.

1.1. Context of the study

Free and fair elections depend on the application of electoral rules, the rule of law and an open and pluralistic public debate supported by independent media. As media consumption and **elections campaigning move increasingly online**, what goes on in the digital world is increasingly likely to influence the outcome of an election. The many new digital technologies offer a mixed picture, and there are reasons to be both optimistic and cautious.

The possibility to reach out to very specific communities through **personalised political advertisements** presents opportunities to activate local democracy and can increase turnout in elections. On the other hand, **microtargeting** techniques can break down the public debate of society as a whole and prevent the required scrutiny of political communication by other actors (public at large, media and political opponents).

Differentiating the messages/information depending on the gender, the social class, the geographical area, the political views or the economic status of the recipients increases the potential for political actors to influence democratic processes and societal debates.

Similarly, **algorithmic filtering** of social media news feeds, for political or economic reasons, may have implications for media pluralism, freedom of expression and exposure to diverse political messages. At the same time, algorithms can also play a positive role in fighting disinformation and promoting quality content.

As artificial intelligence (AI) becomes more powerful, it will be able to leverage big data in a way that will allow an unprecedented ability to influence voters' decision-making processes. Deep fakes, the artificial intelligence-manipulated media, can make people appear to do or say things that they never did or said. Simultaneously, in a world with several billion online users, only AI has the capacity to moderate content and discover patterns of opaque influence campaigns online.

Eurobarometer data[6] has shown that 73 % of the EU population is concerned about disinformation and misinformation on the internet. Eurobarometer data also showed that most internet users (67 %) are concerned about the use of personal data to target political messages. 55% were concerned about restrictions and censorship of political debates on online social networks.

In this context, on 12 September 2018 the **European Commission issued an "Electoral Package" to address threats and secure free and fair elections**.

This study will examine how using data about voters and new technologies, including microtargeting techniques, algorithms and artificial intelligence, can be used to affect the outcome of elections and public confidence in them. This will help ensure that the digital transformation and notably emerging

[6] European Commission. 2018. Special Eurobarometer 477 - Democracy and elections

trends like artificial intelligence are developing in line with European values from democracy to human rights. It will also take into consideration the COVID-19 crisis and the possible impact that it may have on free and fair elections.

2. Methodology

This section describes the methodology applied throughout this study.

The study has been carried out in three phases:

- Fact-finding
- Analysis of results
- Recommendations for a way forward

Figure 3: *Phases of the study*

The figure below represents the data collection activities carried out as well as how each activity feeds in one or more of the other ones:

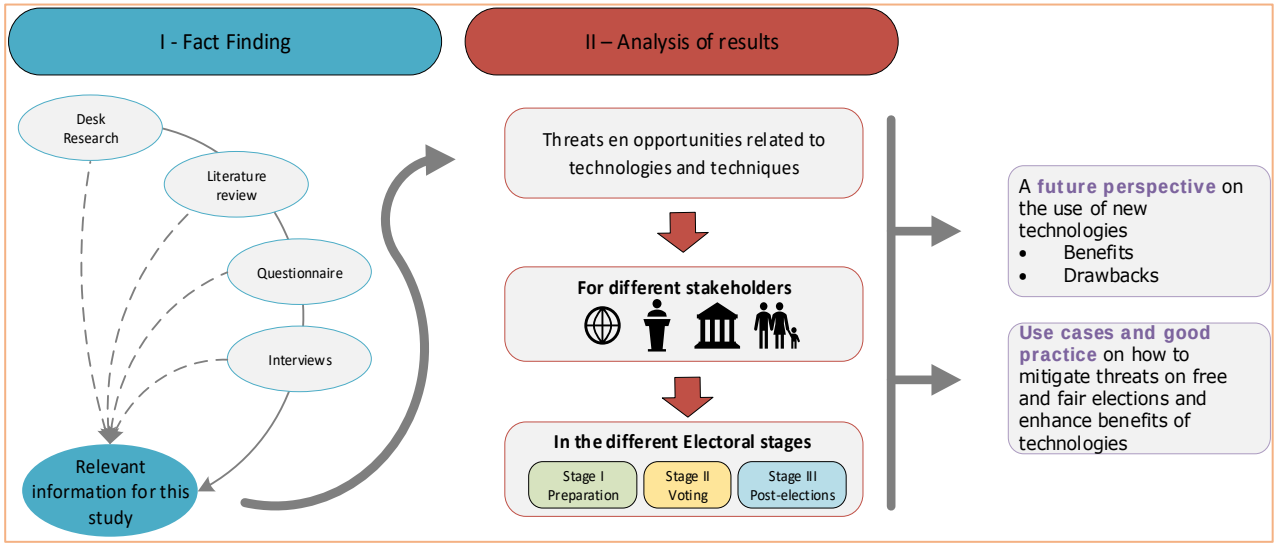

Figure 4: *Study methodology*

2.1. Fact-finding

In the first phase *Fact-finding* the contractor performed a number of data collection activities – desk research; literature review; stakeholder consultations by means of structured questionnaires, discussion sessions and interviews.

2.2. Desk research

The contractor conducted a comprehensive desk research throughout various sources of information[7] discussing the electoral process, such as official EU documents (strategies, studies, reports), national legislation and strategies and academic papers. These documents were listed in list of references which is integrated in **Section 5** at the end of this document.

The reviewed documents were categorised in three levels of relevance to the study defined as follows:

> **High =>** Literature, which is part of the horizontal legal and policy framework on the use of innovative technologies of the European Union, as well as literature, discussing uses and/or impact of new technologies and techniques such as disinformation, online microtargeting and algorithmic filtering, artificial intelligence (AI), blockchain/ DLT and other technologies, in the context of the electoral process and its stages.
>
> **Medium =>** Literature, discussing uses and impact of new technologies and techniques as online micro-targeting and algorithmic filtering, AI, blockchain/DLT and other technologies in a broader context, which could be horizontally applicable to the electoral process and its stages.
>
> **Low =>** Literature, which discuss issues related to the electoral process and its stages in general, without engaging topics of uses of new technologies and techniques in this process or their impact on it.

The desk research together with the literature review **(Section 4)** serve as primary sources of information for this study.

2.3. Literature review

The reviewed **High** relevance literature has been compiled in **Section 4** and classified per main concepts/phenomena which are subject of discussion in the respective reference. The table in **Section 2.4.** provides the contractor's proposed definitions of these main concepts.

The literature review conducted in the scope of this study is a comprehensive summary of previous research on the defined concepts. The literature review surveyed scholarly articles, books, and other sources relevant to the electoral process and the impact of new technologies and techniques on it. The review enumerates, describes, summarises, objectively evaluates and clarifies this previous research. The literature review aims to create a "landscape" for the reader, giving her or him a full understanding of the developments in the field[8].

[7] The term 'literature' is used interchangeably throughout this document.
[8] Definition of a literature review inspired by Bloomberg University Library

The figure below represents the methodology applied for the literature review starting from collection of a broader amount of information towards narrowing the review to literature highly relevant to the study's objectives.

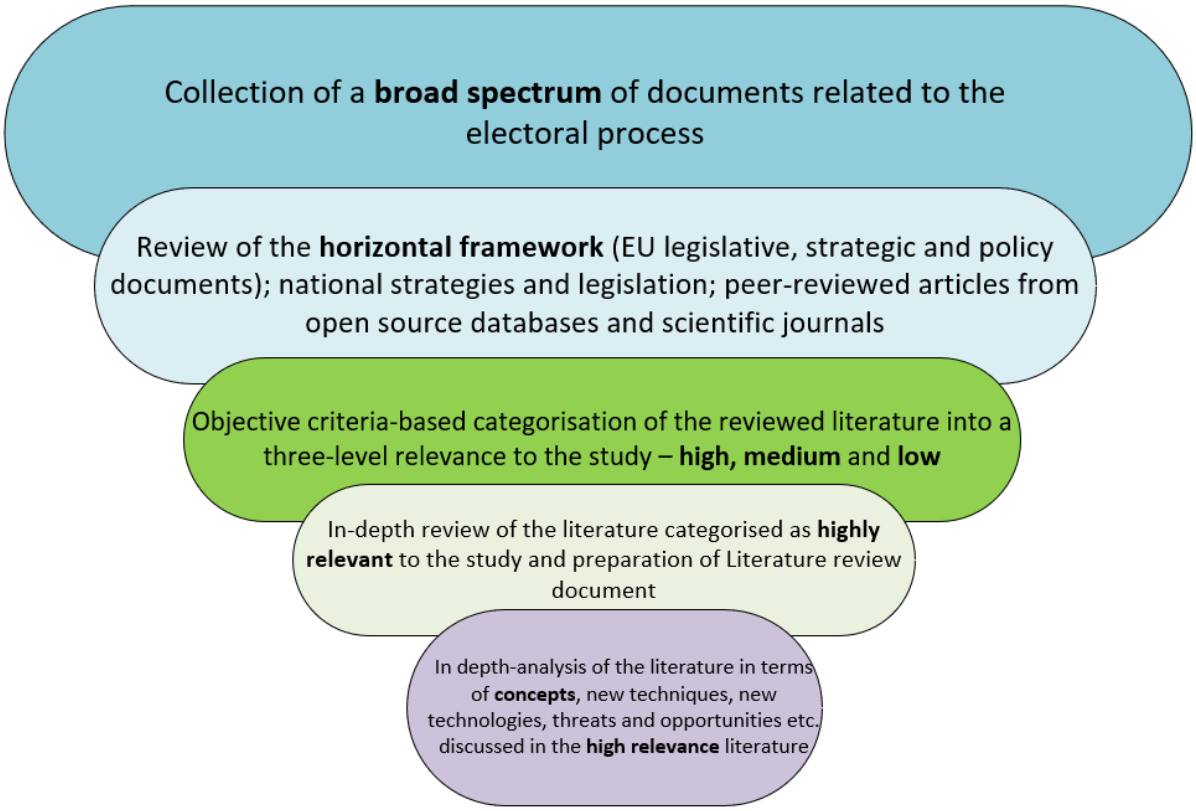

Figure 5: *Methodology for literature review*

First, the contractor collected a broad spectrum of documents related to the electoral process through desk research, from previous studies or provided by DG JUST. Afterwards, the contractor reviewed the horizontal framework (EU legislative, strategic and policy documents); national strategies and legislation; peer-reviewed articles form open source databases and scientific journals. The specific focus was laid on references that discuss the use of new technologies and techniques referring to one of the three stages of the electoral process. Thirdly, the contractor applied an objective criteria-based categorisation of the reviewed literature into a three-level relevance to the study – high, medium and low as defined in **Section 2.2**. Then, the contractor conducted an in-depth review of the literature categorised as highly relevant to the study and prepared summaries of the reviewed in **Section 4**. and for further use in the study reports. Finally, the literature was analysed in depth in terms of concepts, new techniques, new technologies, threats and opportunities, etc. discussed in the high relevance literature.

The results of the reviewed literature served as input for the preparation of questionnaires for the four groups of stakeholders consulted in this study. Additionally, the desk research and literature review results were used for the preparation of an analysis of the threats that new technologies and techniques hide for the democratic elections and the benefits they may bring.

2.4. Key concepts

Concepts	Definition
Microtargeting	Microtargeting is a customized marketing messages delivered to a niche audience sharing relevant interests, according to recorded data.[9] In the context of this study, "microtargeting" is understood as "online political microtargeting" and is a technique, often used by political parties and candidates in the form of personalised communication that involves collecting information about individuals and using that information to show the potential voters targeted political advertisements with the aim to gain their vote.[10]
Algorithmic filtering	Algorithmic filtering is the evaluation of data based on some formula. In general, all filters rely on some algorithm; however, the term typically refers to social media and search engines, wherein users are delivered ads, videos and news stories that appeal to their lifestyle and principles.[11] Algorithmic filtering of social media news feeds, for political or economic reasons, may have implications for media pluralism, freedom of expression and exposure to diverse political messages. At the same time, algorithms can also play a positive role in fighting disinformation and promoting quality content. Algorithmic content filtering. *"There are three parts to the definition of algorithmic filtering (AF). Filtering is the selection of content (e.g., posts, videos, photos, ads, comments, articles, etc.) that are shown on a user's feed. It is algorithmic because the selection typically utilizes an algorithm that takes certain features—such as the user's attributes (e.g., age or gender) and/or the user's history (e.g., web searches or previous actions on the platform)—as inputs and constructs the user's feed from current, available content as an output."*[12]

[9] https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-823
[10] Dobber, Fathaigh, Zuiderveen Borgesius, The regulation of online political micro-targeting in Europe
[11] https://www.computerlanguage.com/results.php?definition=algorithmic+filter
[12] Cen Sarah H., Shah Devavrat, Regulating algorithmic filtering on social media. See: https://arxiv.org/pdf/2006.09647.pdf

Online disinformation	Disinformation is verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.[13] Online disinformation campaigns, through social platforms (particularly, but not only, social media) are being widely used by a range of domestic and foreign actors to sow distrust and create societal tensions, with serious potential consequences.[14] Disinformation is part of a wider array of tools used to manipulate electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians. Cyber-enabled operations may be used to compromise the integrity of public information and prevent the identification of disinformation sources. This is critical during election campaigns, where compressed schedules may prevent timely detection of disinformation and response.[15]
Campaigning	The activity of taking part in a **campaign**, for example to achieve social or political change, or in order to win an **election**.[16]
Electronic voting (e-voting) and internet voting (i-voting)	Electronic voting or e-Voting is defined in the context of this study as "the use of electronic means in at least the casting of the vote"[17] Remote e-Voting is defined as " e-voting where the casting of the vote is done by a device not controlled by an election official".[18] e-Voting differs from internet voting, or i-Voting, which in the context of this study is defined as a system that allows voters to cast their ballots from any internet-connected computer anywhere in the world.[19]

[13] European Commission. 2018. Communication on tackling on-line disinformation, COM(2018) 236
[14] Idem
[15] European Commission. 2018. Communication on tackling on-line disinformation, COM(2018) 236
[16] https://www.oxfordlearnersdictionaries.com/definition/english/campaigning
[17] Council of Europe 2004 (See : https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp
[18] Idem
[19] https://e-estonia.com/solutions/e-governance/i-voting/

Use of new forms of fundraising for political parties	Political fundraising is raising money to help a particular political party and/or candidate to run for elections. The funds raised are used to promote the political party and/or candidate, their initiatives and activities such as preparing political advertising and campaigning strategy.[20] New forms of political fundraising can be (but is not limited to) online donations and online political crowdfunding whereby many individuals donate small amounts of money to a political initiative, very often a political party, through predominantly digital means/ via the Internet.[21]
Hate speech and extreme negative rhetoric	Hate speech is, public (online) behaviour that expresses hate or encourages violence towards a person or group based on their political orientation, race, religion, ethnic origin, gender orientation, sex, or other characteristics.[22] Illegal hate speech is defined in EU law[23] as the public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin. While the Framework Decision on combatting racism and xenophobia covers only racist and xenophobic speech, the majority of Member States have extended their national laws to other grounds such as sexual orientation, gender identity and disability. Based on the Council of Europe Recommendations R. (97) 20 hate speech is defined *"as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism 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".* [24]

[20] https://callhub.io/political-fundraising/
[21] https://www.idea.int/sites/default/files/publications/online-political-crowdfunding.pdf
[22] Cambridge dictionary (see: https://dictionary.cambridge.org/dictionary/english/hate-speech)
[23] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law (see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0913&from=en)
[24] See : https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-97-20-of-the-committee-of-ministers-to-member-states-on-hate-speech-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view

Transparency of the elections	A transparent election process is one in which each step is open to scrutiny by stakeholders (political parties, election observer, voters, civil society organisations, etc.), who are able to independently verify if the process is conducted according to procedures and no irregularities have occurred. Providing transparency in an election helps establish trust and public confidence in the process, as voters have a means to verify the results are an accurate reflection of the will of the people.[25]

[25] https://www.ndi.org/e-voting-guide/transparency

3. Literature review summary

This section includes the summaries of references assessed as being of high relevance to this study. References that are analysed and indicated as being in categories of 'medium level reference' and 'low level reference' are included in **Section 5** of this document.

3.1. European Union legal and policy framework

Author	Title	Brief summary	Ref. No.
European Parliament, Council of the European Union	Regulation (EU, EURATOM) No 11412014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations	The Regulation aims to create a specific legal, financial and regulatory system for European political parties and European political foundations. It increases their visibility, recognition and effectiveness by giving them a European legal personality and greater funding flexibility. The Regulation creates the independent Authority for European Political Parties that registers, verifies and may impose penalties on European political parties and foundations. It also sets the conditions for registration and de-registration and the obligation for transparent spending of EU funded campaigns.[26]	34
European Parliament, Council of the European Union.	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal	Art. 2 (TEU) 'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.'	142

[26] Summary prepared by the contractor.

	aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')		
European Parliament, Council of the European Union	Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market	The Directive establishes harmonised rules on issues such as transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. It also enhances administrative cooperation between the Member States and the role of self-regulation. The Directive exempts intermediaries from liability for the content they manage if they fulfil certain conditions.[27]	144
European Commission	White Paper on Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65 final)	The White Paper on Artificial Intelligence and the European data strategy are the first pillars of the new digital strategy of the Commission. They are fully aligned with the need to put people first in developing technology, as well as with the need to defend and promote European values and rights in how we design, make and deploy technology in the real economy and how we improve the services of the public sector towards the citizens.	147
European Commission	2019. Building Trust in Human-Centric Artificial Intelligence (COM(2019) 168 final)	With the focus on a more human-centric AI in Europe, new challenges have emerged for AI technologies. The learning capabilities of these digital machines enables them to take and implement decisions without human intervention. To avoid unintended harm, AI technology should be developed in a way that puts people at its centre and is thus worthy of the public's trust – compliant with law and with the ethical principles. The document refers to the Ethics Guidelines on AI of the AI High Level Expert Group (HLEG)[28], which elaborates on seven principles of a trustworthy AI	148

[27] Summary prepared by the contractor

[28] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

European Commission	Artificial Intelligence for Europe (COM(2018) 237 final)	The Strategy on AI for Europe places people at the centre of the development of AI (human-centric AI). It is a three-pronged approach: to boost the EU's research and industrial capacity and AI uptake across the economy, to prepare for socio-economic changes, and to ensure an appropriate ethical and legal framework. The Strategy identifies the necessity of coordinated actions and common efforts in order for the EU to stay at the forefront of the AI uptake and to ensure that EU values are respected. These actions should include, among others, increased investments in AI, research and innovation, increased data availability, increased trainings and digital awareness.	149
European Commission	Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)	Delivering on the Strategy on AI for Europe, adopted in April 2018, the Commission presented a coordinated plan for joint actions between the Commission and the Member States. The Coordinated plan sets as its main objectives: the promotion of the common efforts of the Member States (e.g. in adopting national strategies); the fostering of public-private partnerships; and the financing of start-ups and innovation enterprises. It also focuses on security-related aspects of the AI applications and infrastructure.	150
European Commission	Towards a common European data space (COM(2018) 232 final	The article presents a package of measures proposed by the Commission, in view of establishing a common data space in the EU. These measures include: the re-use of public sector information; update of the Recommendation on access to and preservation of scientific information; and guidance on sharing private sector data.	151
European Union	The Charter of Fundamental Rights of the European Union (CFR) [2012], OJ C 326/391 (Art. 8, 11, 39, 40 and others) (2000/C 364/01)	Enshrines through a range of personal, civil, political, economic and social rights in the EU, such as right of personal data protection (Art.8), freedom of expression and information (Art. 11), right to vote and to stand as a candidate at elections to the European Parliament (Art. 39), and municipal elections (Art. 40).[29]	154
European Commission	Communication from the Commission to the European Parliament,	EU action plan to create a fair democracy in a digital world. Including topics such as: rules on the financing of European political parties; implement professional standards; support media pluralism; Improving EU and Member State capacity to counter disinformation; More	181

[29] Summary prepared by the contractor

	the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan	obligations and accountability for online platforms; Empowering citizens to make informed decisions.

3.2. Microtargeting and algorithmic filtering

Author	Title	Brief summary	Ref. No.
Dobber, Fathaigh, Zuiderveen Borgesius	The regulation of online political micro-targeting in Europe	This paper focuses on the following questions: What is online political micro-targeting, and what are its promises and threats? It combines insights from both a legal and social science perspective. The authors focus mostly on European countries and the US. Section 2 Introduces the practice of online political micro-targeting. Section 3 discusses the promises of online political micro-targeting, and Section 4 the threats. Section 5 discusses why the threats, while serious, should not be overstated. Section 6 explores how policymakers in European countries could intervene and sketches some problems they would encounter if they wanted to intervene. Section 7 concludes that more research and debate about online political micro-targeting is necessary.[30]	01
International Institute for Democracy and Electoral Assistance	Digital Microtargeting	The paper explains the techniques of digital microtargeting in a political advertising context. It then exposes the legal, financial and ethical considerations before listing the risks.[31]	13

[30] Summary prepared by the contractor
[31] Idem

European Commission	Commission guidance on the application of Union data protection law in the electoral context	The paper discusses the problem of data protection in the context of political microtargeting. The objective of the guidance paper is to highlight the data protection obligations, of relevance for elections, by the different actors in the electoral process.[32]	15
Papakyriakopoulos et al.	Social media and microtargeting: Political data processing and the consequences for Germany	The report discusses that political campaigns employ microtargeting, a specific technique used to address the individual voter. The article elaborates on how the use of microtargeting can be more challenging depending on the laws of the country (USA, Germany, and France). The article further discusses on how the data can be collected, put into different clusters and analysed.[33]	45
United Nations Educational Scientific and Cultural Organization	Elections and media in digital times	'This report is about the increasing digitalization of societies across the world has led to unprecedented opportunities to seek, receive and impart political information and ideas, which are the lifeblood of elections. The Internet, and in particular social media and social messaging, have changed the way politicians, political parties and the electorate communicate with each other, with the chance of being more direct and quicker than at any point in history. But there are also growing concerns about the disruptive effects on public debate arising from the misuse of digital technologies. Political micro-targeting of individual voters is driven by aggregated personal data, which is not always obtained in lawful ways. Moreover, micro-targeting practices are sometimes manipulative. The report is a follow-up to UNESCO's 36 C/Resolution 53, wherein the Organization's Member States requested UNESCO to monitor the status of press freedom and safety of journalists and to report on the developments in these fields to the Organization's General Conference.'	74
Hegelich, Serrano	Microtargeting in Germany for the 2019 European Elections	This article aims to analyse how microtargeting techniques were used and if and how they had impact on 2019 European Parliament elections in Germany. In terms of methodology, as many other articles, this article also starts by analysing the tools made available by the platform operators (Google, Facebook or Twitter) - such reporting tools and the application	107

[32] Summary prepared by the contractor
[33] Idem

		programming interfaces (APIs) such Facebook Ad Library API or the Google Cloud BigQuery API. In conclusion, the article argues that though there is a clear evidence that in the last 2019 European Parliament election in Germany, the political parties' online advertising strategy had an important relevance on their campaigning strategy, it was not exploited to its maximum, for example by increasing the budget allocated for microtargeting technique. Secondly, and as other articles raised before, the data made available by the platforms operators is not fully complete and reliable, as they provide and work with different definitions of what are political ads for example.[34]	
European Data Protection Board	Guidelines 8/2020 on the targeting of social media users	The Guidelines focus on the use of social media as a significant development in the online environment over the past decade. They aim to clarify the role of social media providers and targeters as joint controllers of personal data, and their responsibilities under the General Data Protection Regulations (GDPR). Four groups of actors fall within the scope of the Guidelines: social media providers, their users, targeters and other actors which may be involved in the targeting process (data brokers, data management providers, marketing service providers, ad networks and exchanges, data analytics companies etc.). The Guidelines clarify each of these groups and their role in targeting. Regard taken of the joint responsibility that may be inherent to targeters and social media provider towards social media users, the document offers guidance concerning the targeting of these users as regards the said responsibilities.[35]	130
Kruikemeier, Sezgin, Boerman	Political Microtargeting Relationship between Personalised Advertising on Facebook and Voters' Responses	'This study examines the relationship between exposure to political personalized ads on Facebook and voters' responses toward those ads and studies the mediating role of the use of persuasion knowledge in this relationship. Results from an online experiment (N = 122) demonstrate that exposure to a personalized ad from a political party activates persuasion knowledge, which in turn leads to lower intentions to engage in electronic word of mouth, but only for those participants who recall seeing the Sponsored label. We found no effects on source trustworthiness. Adding a text explaining the practice of personalized advertising did not lead to higher levels of persuasion knowledge and did not change the responses toward the message.'	138

[34] Summary prepared by the contractor
[35] Idem

European Data Protection Supervisor	Opinion 3/2018 on online manipulation and personal data	'The ensuing debate has revolved around the misleading, false or scurrilous information ('content') served to people with the intention of influencing political discourse and elections, a phenomenon come to be labelled 'fake news' or 'online disinformation'. Solutions have focused on transparency measures, exposing the source of information while neglecting the accountability of players in the ecosystem who profit from harmful behaviour. Meanwhile market concentration and the rise of platform dominance present a new threat to media pluralism. For the EDPS, this crisis of confidence in the digital ecosystem illustrates the mutual dependency of privacy and freedom of expression. The diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy. This Opinion is therefore concerned with the way personal information is used in order to micro-target individuals and groups with specific content, the fundamental rights and values at stake, and relevant laws for mitigating the threats.'	152
Zuiderveen Borgesius et al.	Online Political Micro-targeting: Promises and Threats for Democracy	'Online political microtargeting involves monitoring people's online behaviour, and using the collected data, sometimes enriched with other data, to show people-targeted political advertisements. Online political microtargeting is widely used in the US; Europe may not be far behind. This paper maps microtargeting's promises and threats to democracy. For example, microtargeting promises to optimise the match between the electorate's concerns and political campaigns, and to boost campaign engagement and political participation. But online microtargeting could also threaten democracy. For instance, a political party could, misleadingly, present itself as a different one-issue party to different individuals. And data collection for microtargeting raises privacy concerns. We sketch possibilities for policymakers if they seek to regulate online political microtargeting. We discuss which measures would be possible, while complying with the right to freedom of expression under the European Convention on Human Rights.'	217

3.3. Online disinformation

Author	Title	Brief summary	Ref. No.
European Commission	Securing free and fair European elections: A Contribution from the European Commission to the Leaders' meeting	The paper sets the situation on free and fair European elections of 2019, exposing the challenges and threats. It then discusses policy priorities and measures for the defence of free and fair European elections.[36]	03
European Regulators Group for Audiovisual Media Services	Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation	The report contains the outcome of a follow-up analysis of the major social media companies – Google, Facebook, Twitter - with regards to its compliance with the commitment on the Code of Practice on disinformation, on different aspects of political and issue-based advertising during the European elections of May 2019. Finally, it draws conclusions of the monitoring and challenges encountered.[37]	04
European Parliamentary Research Service	Regulating disinformation with artificial intelligence	This study examines the consequences of the increasingly prevalent use of artificial intelligence (AI) disinformation initiatives upon freedom of expression, pluralism and the functioning of a democratic polity. The study examines the trade-offs in using automated technology to limit the spread of disinformation online. It presents options (from self-regulatory to legislative) to regulate automated content recognition (ACR) technologies in this context. Special attention is paid to the opportunities for the European Union as a whole to take the lead in setting the framework for designing these technologies in a way that enhances accountability and transparency and respects free speech.[38]	05

[36] Summary prepared by the contractor
[37] Idem
[38] Summary prepared by the contractor

European Commission	Flash Eurobarometer 464. Fake news and disinformation online?	This paper discusses the levels of trust in news and information, the people's perception of fake news, the public confidence in identifying in misleading news, the people's views on the extent of the problem and views on which institutions and media actors should act to stop the spread of fake news.[39]	09
Avaaz	Far right networks of deception - Avaaz investigation uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections	The report explores disinformation networks tactics and content in six (6) EU countries (Germany, UK, France, Italy, Poland and Spain) especially on Facebook. It than proposes the adoption of "Correct the record", which consists in a 5-step process that makes corrections verified by independent fact-checkers.[40]	10
European Commission	EU Code of Practice on Disinformation	This Code of Practice was signed by the major internet companies that disperse information and news amongst citizens of the European Union. For example, Facebook, Instagram etc. are concerned.[41]	12
European Commission	Tackling online disinformation: a European Approach	The Communication elaborates on the key challenges of online disinformation, its impacts on European democratic values and it aims at setting a framework of principles and objectives to be considered as guide to actions on raising public awareness on disinformation phenomena.[42]	14
Alaphilippe et al.	Automated tackling of disinformation Major challenges ahead	This study discusses the phenomenon of mis-, mal- and disinformation. It discusses how social platforms, search engines, online advertising, and computer algorithms enable and facilitate the creation and spread of online misinformation. It also presents current understanding in why people believe false narratives, what motivates their sharing, and how they impact offline behaviour (e.g. voting). This is complemented by a brief overview of self-regulation, co-regulation, and classic regulatory responses, as currently adopted by social platforms and EU	16

[39] Summary prepared by the contractor
[40] Idem
[41] Summary prepared by the contractor
[42] Idem

		countries. The study includes a roadmap of initiatives from key stakeholders in Europe and three case studies on the utility of automated technology in detecting, analysing, and containing online disinformation. The study concludes with the provision of policy options.[43]	
High Level Group on Fake News and Online Disinformation	A multi-dimensional approach to disinformation	'The High-Level Group of experts was convened to advice on policy initiatives to counter fake news and disinformation spread online. The final report contains interesting ideas on the definition of disinformation. It analyses the impact of disinformation before elaborating on policy recommendation. It advocates the use of multi-dimensional solutions involving different actors.'	17
Relatórios OberCom Outubro	Fake News em ano eleitoral Portugal em linha com a UE	The report makes an overview of European Union (EU) and Portugal positions and approaches against fake news. It also addresses the impact and different tactics of disinformation in electoral online campaigning (more focused in Portuguese case) and elaborates on three initiatives to mitigate such phenomena such fact-checking, media literacy and collaborative journalism.[44]	23
Martin, Shapiro	Trends in Online Foreign Influence Effort	'Foreign governments have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation. We analyse 53 distinct foreign influence efforts (FIEs) targeting 24 different countries from 2013 through 2018. FIEs are defined as (i) coordinated campaigns by one state to impact one or more specific aspects of politics in another state (ii) through media channels, including social media, (iii) by producing content designed to appear indigenous to the target state. The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization. We draw on more than 460 media reports to identify FIEs, track their progress, and classify their features.'	27
Chatham House	Online Disinformation and Political Discourse - Applying a Human Rights Framework	Chapter 2 of this paper clarifies core terms and concepts such as digital platforms, disinformation, personal data, elections and political discourse. Chapter 3 provides an overview of cyber activities that may influence voters with specific examples from different countries. These cyber activities include creation, distribution and maximisation of the influence of disinformation and divisive content. Chapter 4 summarises a range of responses	29

[43] Summary prepared by the contractor
[44] Idem

		to the issue in different countries (the UK, the US, Germany, France, Singapore), the EU and initiatives of the digital platforms like Facebook, Twitter and Verizon Media in the form of rules and standards. Chapter 5 discusses relevant human rights law, with specific reference to: the right to freedom of thought, and the right to hold opinions without interference; the right to privacy; the right to freedom of expression; and the right to participate in public affairs and vote. Chapter 6 offers some conclusions and sets out recommendations on how human rights ought to guide state and corporate responses.[45]	
Appelman et al.	The spreading of disinformation through internet services and the regulation of political advertisements	'The research is based on seven research questions submitted by the Ministry of Interior. The questions vary from very general to very specific, but all relate to the broader problems surrounding disinformation, the existing legal framework and the possibility of further regulation. These seven questions are therefore all answered in the context of the broad analysis in the report of the relevant legal framework for the dissemination of disinformation through internet services and possible regulatory options.'	31
European Commission	Report on the implementation of the Action Plan Against Disinformation	The report by the Commission and the High Representative provides a first assessment of the progress achieved so far and sets out the main lessons for the future. It explains in more detail how the Action Plan and the Elections Package helped to fight disinformation in the context of the European elections. It is also the contribution of the Commission and the High Representative to the European Council meeting on 20-21 June 2019.	36
Ferrara. 2017	Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election	This paper aims to analyse forms of social media manipulation, especially disinformation and social bot operations in the run up to the 2017 French presidential elections, focusing on the MacronLeaks disinformation campaign. "Nearly 17 million posts occurred between April 27 and May 7, 2017 (Election Day)" were collected from Twitter dataset. In conclusion, the paper confirms results from previous academic contributions sustaining the existence of a "black market of reusable political disinformation bots", but the study goes further this argument and add the new discovery of identifying bots already present during 2016 US presidential election campaign and supporting alt-right positions, however inactive since then. Secondly, the paper also concludes that regarding audience of MacronLeaks campaign, it was mainly	44

[45] Summary prepared by the contractor

		composed by "English-speaking American alt-right community, rather than French users", potential voters, which also explains the limited success of this disinformation campaign[46]	
Bentzen	Foreign influence operations in the EU	This briefing looks into how foreign powers influence political decision-making beyond one's own political sphere. Two approaches of projecting power are looked at: the soft and the sharp approach. It gives also examples of active measures then and now: the case of the Kremlin; and European responses to disinformation campaigns. At the end it focuses on evolving tools and actors.[47]	58
Martens et al.	The digital transformation of news media and the rise of disinformation and fake news: An economic perspective	'This report contains an overview of the relevant economic research literature on the digital transformation of news markets and the impact on the quality of news. It compares various definitions of fake news, including false news and other types of disinformation and finds that there is no consensus on this. It presents some survey data on consumer trust and quality perceptions of various sources of online news that indicate relatively high trust in legacy printed and broadcasted news publishers and lower trust in algorithm-driven news distribution channels such as aggregators and social media.'	62
Bayer et al.	Disinformation and Propaganda - Impact on the Functioning of the Rule of Law in the EU and its Member States	'This study assesses the impact of disinformation and strategic political propaganda disseminated through online social media sites. It examines effects on the functioning of the rule of law, democracy and fundamental rights in the EU and its Member States. It also formulates recommendations on how to tackle this threat to human rights, democracy and the rule of law. It specifically addresses the role of social media platform providers in this regard.'	68
Rapid Response Mechanism Canada	Open data analysis - European Parliamentary Elections: Comprehensive Report	"The main objectives of this report are to: shine light on any effort to artificially amplify unsubstantiated or false information challenging the legitimacy and fairness of the UK, Irish or EU democratic and electoral systems; identify key issues that were highly divisive and exploited within the context of the EU elections in the UK, Ireland and Italy in order to identify narratives that may transcend borders and be used in other contexts; and identify notable tactics used by malign, foreign actors. (…) In relation to the EU	83

[46] Summary prepared by the contractor
[47] Idem

		Parliamentary Elections, a key insight from RRM Canada is that while no significant evidence of state-based foreign interference was observed, the digital ecosystem is ripe and ideal for exploitation by foreign malign actors."	
Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation	Progress Report - November 2019	'This 2nd report of the Interdepartmental Group (IDG) on Security of the Electoral Process and Disinformation presents a first assessment of the progress achieved on the recommendations of the 1st IDG Report, since its publication in July 2018. (…)The main finding was that risks to the electoral process in Ireland are relatively low but that the spread of disinformation online and the risk of cyber-attacks on the electoral system pose more substantial risks. This aligned with EU findings and recent international experience. The Report outlined 7 recommendations, which were developed to form the basis for a multi-faceted, whole of government approach to safeguarding of the electoral process from disinformation and security risks.'	86
European Commission	First Annual Self-Assessment Reports on the Code of Practice of Disinformation	The document provides information on the annual reports submitted by the signatories of the Code of Practice on Disinformation such as Facebook, Twitter, Google and Microsoft, on the various measures they have implemented in compliance with their obligations to fight online disinformation.[48]	96
European Commission	Tackling COVID-19 disinformation - Getting the facts right (JOIN (2020) 8 final)	The Joint Communication focuses on the immediate response to disinformation around the coronavirus pandemic, looking at the steps already taken and concrete actions to follow, which can be quickly set in motion based on existing resources. It also highlights areas where the crisis has pointed to more fundamental challenges, to be further assessed as the crisis evolves and to form part of the wider approach to strengthen democracy, which will be set out in the European Democracy Action Plan, as announced in President von der Leyen's Political Guidelines. Its aim will be to further strengthen the EU's work to counter disinformation and to adapt to evolving threats and manipulations, as well as to support free and independent media. The upcoming Digital Services Act, regulating digital services, is part of this comprehensive approach.[49]	102

[48] Summary prepared by the contractor

[49] Idem

Lim	Disinformation as a Global Problem – Regional Perspectives	'This research project discusses disinformation in the European Union (EU) and Southeast Asia (SEA). The report examines the characterisation and context of disinformation, provides an overview of its creators and its circulation, where creation refers to production and its underlying motivations and circulation refers to the different ways it is disseminated, amplified and sustained, and rounds up with a discussion on foreseeable trends. It finds that disinformation is ultimately a national security problem, and any assessment of, and response to, disinformation must be formulated with developments in other domains.'	106
European Regulators Group for Audiovisual Media Services	Assessment of the Implementation of the EU Code of Practice on Disinformation	The overarching study objective is to support the European Commission's evaluation of the Code of Practice's effectiveness. The assessment focuses on the 13 current Signatories of the Code of Practice on Disinformation (online platforms and business associations). The study's overall conclusion is that the Code of Practice has produced positive results. Firstly, it has established a common framework under which to agree on and implement activities to tackle disinformation. Secondly, it has established a platform for negotiation that has produced concrete results in the form of regular monitoring of Signatory activities and continuous action to combat disinformation activities. The main criticism of the Code relates to its self-regulatory nature, lack of uniformity of implementation, monitoring, and lack of clarity around its scope and some of the key concepts.[50]	109
European Economic and Social Committee	The effects of campaigns on participation in political decision-making	This document is an exploratory opinion requested by the Croatian presidency to the EESC. It presents a set of recommendation such as the improvement of self-regulation in the field of online disinformation or the improvement of EU action against domestic to foster 'timely monitoring, enhances professional journalism and fosters media literacy.[51]	116
Joint Research Centre	Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives	This report analyses how disinformation campaigns have evolved into more complex hostile narratives, taking Italy, France, and Spain as case studies to prove what has been observed and determined from analytical and numerical research. This report highlights how hostile narratives target citizens' vulnerabilities using algorithmic content curation. The case studies describe how different disinformation campaigns have been used in Italy, France and Spain.	118

[50] Summary prepared by the contractor
[51] Idem

		It also provides examples on how hostile disinformation narratives were employed in France and Italy.[52]	
Joint Research Centre	Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda	'This report discusses that disinformation strategies have evolved from 'hack and dump' cyber-attacks, and randomly sharing conspiracy or made-up stories, into a more complex ecosystem where narratives are used to feed people with emotionally charged true and false information, ready to be "weaponised" when necessary. Manipulated information, using a mix of emotionality and rationality, has recently become so pervasive and powerful to the extent of rewriting reality, where the narration of facts (true, partial or false) counts more than the facts themselves. Every day, an incredible amount of information is constantly produced on the web. Its diffusion is driven by algorithms, originally conceived for the commercial market, and then maliciously exploited for manipulative purposes and to build consensus. Citizens' vulnerability to disinformation operations is not only the result of the threats posed by hostile actors or psychometric profiling - which can be seen as both exploiters and facilitators - but essentially due to the effect of three different factors: Information overload; Distorted public perceptions produced by online platforms algorithms built for viral advertising and user engagement; The complex iteration of fast technology development, globalisation, and post-colonialism, which have rapidly changed the rules-based international order. In rapidly and dynamically evolving environments, increasing citizens' resilience against malicious attacks is, ultimately, of paramount importance to protect our open democratic societies, social values and individual rights and freedoms.'	119
European Commission	Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement	The document sets out the key findings of the EC services' assessment of the implementation and effectiveness of the Code of Practice on Disinformation during its initial 12-months period of operation and provides an overview and an assessment of the implementation and effectiveness of the commitments subscribed to by the signatories of the Code.[53]	128
Garnett, James.	Cyber Elections in the Digital Age: Threats	'Elections are essential for delivering democratic rule, in which ultimate power should reside in the citizens of a state. This introduction argues that the management and contestation of	133

[52] Summary prepared by the contractor
[53] Idem

	and Opportunities of Technology for Electoral Integrity	elections have now entered a qualitative new historical period because of the combined development of new technology and broader sociological developments. The era of cyber-elections is marked by: (a) the new ontological existence of the digital, (b) new flows of data and communication, (c) the rapid acceleration of pace in communications, (d) the commodification of electoral data, and (e) an expansion of actors involved in elections. These provide opportunities for state actors to incorporate technology into the electoral process to make democratic goals more realizable. But it also poses major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals such as political equality and popular control of government. The article argues that this new era therefore requires proactive interventions into electoral law and the rewriting of international standards to keep pace with societal and technological change.'	
Huckle, White	Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains	'The document introduces a prototype of an innovative technology for proving the origins of captured digital media. The document aims to introduce a blockchain-based distributed application, Provenator (intended as the agent noun of the verb form of provenance, which means establishing the origin of something), a tool that helps prove the originator of media sources.'	136
Terzis et al.	Disinformation and Digital Media as a Challenge for Democracy	'The book discusses diverse academic and professional comments from all over the world, touching upon topics that range from the theoretical approaches to and the conceptualisation of disinformation, to the experiences of dealing with disinformation, to the solutions for dealing with disinformation and their critique. The book aims through a collection of expert analyses, to deepen the understanding of the dangers of fake news and disinformation, while also charting well-informed and realistic ways ahead.'	155
Broadband Commission for Sustainable Development	Balancing Act Countering Digital Disinformation While Respecting Freedom of Expression	'Targeted analyses and recommendations address the life cycle of online disinformation: from production to transmission, reception and reproduction. The chapters could be of special interest to legislators and policy makers (counter disinformation campaigns, electoral-specific responses, the Freedom of Expression Assessment Framework); Internet companies, producers and distributors (content curation, technical and algorithmic, advertisement policy, demonetisation responses); journalists, investigative researchers and fact checkers; universities and applied and empirical researchers; target audiences (educational, ethical and normative, empowerment and credibility labelling responses).	156

		The findings are organised into a typology of 11 different categories of responses to disinformation – ranging from identification and investigatory responses, through to policy and legislative measures, technological steps, and educational approaches. For each category of response, the reader will find a description of work being done around the world, by which actors, how it is funded and who or what is targeted. The report further analyses the underlying assumptions and theories of change behind these responses, while weighing up the challenges and opportunities. Each category of response is also assessed in terms of its intersections with the universal human right of freedom of expression, with a particular focus on press freedom and access to information. Finally, case studies of responses to COVID-19 disinformation are presented within each category. At the heart of this knowledge product is the need to balance responses to disinformation with respect for freedom of expression. The research shows us that this can be done.'	
Kofi Annan Foundation	The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms	Analyses specific dangers of the internet and technologies on the elections, and reform options to combat these digital dangers to democracy.[54]	198

3.4. Campaigning

Author	Title	Brief summary	Ref. No.
Committee of experts on media pluralism and transparency of media ownership	Internet and electoral campaigns - Study on the use of internet in electoral campaigns	This study was conducted on request of the Committee of Ministers to 'carry out a study on a possible standard-setting instrument on media coverage of elections with particular regard to the use of internet in electoral campaigns. The study analyses the key concepts of fair, clean and clear elections and explains the context and evolution of internet advertising for	06

[54] Summary prepared by the contractor

		political objectives. The study concludes with a list of recommendations to existing policies of Member States on the organisation and regulation of elections.[55]	
Davies	Social media and election campaigning	This briefing is about how social media is used and what the effect is in election campaigns across Europe.[56]	59
Boucher	Technology and social polarisation	Briefing about two STOA studies which explores the mechanisms by which technologies and techniques may foster polarisation in Europe. One study approaches the question with reference to trends in the production and consumption of news media, while the other focuses on trends in political campaigning and communication strategies.[57]	60
Neudert, Marchal	Polarisation and the use of technology in political campaigns and communication	'This report offers a comprehensive overview of the relationship between technology, democracy and the polarisation of public discourse. It provides an in-depth analysis of the technological affordances that enhance and undermine political decision-making, both now and in the future. As conclusion, two principles and policy options for fostering a better relationship between digital technology and public life were formulated.'	61
Organization for Security and Co-operation in Europe	Political advertising and media campaign during the pre-election period: A Comparative Study	'The present Comparative Study provides for findings within the project "Political advertising and media campaign during the pre-election period". The final objective of the project is to improve the quality of the media legal framework regulating political advertising.'	84
Electoral Administration Team of the UK Cabinet Office	2018. Protecting the Debate: Intimidation, Influence and Information	This consultation document reviews the following recommendations and issues: governmental consultation on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners; A consolidation and clarification of the electoral offence of undue influence; an extension on the electoral law requirements for an imprint on campaigning materials to electronic communications.[58]	92
European Commission	a)Report on the 2019 elections to the	The report shows that young and first-time voters drove turnout figures to the record high. The 2019 election campaign was the most digital to-date – almost half of EU citizens now rely on online news as their main source for information about national and European politics. Yet	103

[55] Summary prepared by the contractor
[56] Idem
[57] Summary prepared by the contractor
[58] Idem

	European Parliament (COM (2020) 252 final) b)Report on the 2019 elections to the European Parliament (SWD (2020) 113 final)	the Member States have differing rules when it comes to digital campaigning, including on paid-for political content online. A dynamic European debate emerged on a number of topics, showing progress in developing a European political dimension; however, national-specific issues remain key for candidates and voters alike. European citizens expressed increased satisfaction with free and fair elections in the EU, but further work is necessary to protect democracy from foreign interference and manipulation and promote free and fair elections in Europe.[59]	
Davis, Livingston, Hindman	Suspicious Election Campaign Activity on Facebook	This article elaborates on the techniques used to create artificial promotion of political campaigns on Facebook, done by the German political far right party Alternative für Deutschland (AfD).[60]	108
Esposito, Tse, Entsminger, Jean	AI in the election industry demands transparency	Whatever shapes voting, shapes democracies. Increasingly, AI is becoming such a go-to tool for shaping voting. As the race for the US presidency picks up speed, another area we should expect is the expanding use of AI in election prediction.	115
Democracy Reporting International (DRI)	Lessons Learned: Social Media Monitoring during Humanitarian Crises	'Where do you start if you want to monitor social media during elections? To help get you started, DRI's Madeline Brady summarizes lessons learned from five projects that covered national elections across Europe in 2019 and 2020. We dive into each project, provide examples for teams deciding on what to monitor, how to assemble a team and other critical questions. The lessons learned from these five projects show that further steps are needed from government, social media companies and research institutions to improve the quality of monitoring work by civil society. For example, civil society groups require clear processes to access data from companies and access to additional metrics to successfully monitor social media. DRI is also working on other tools to address the challenges faced by social media monitoring teams, which will be available in July 2020.'	175
Wahlbeobachtung.org	Social Media Monitoring Early Parliamentary Election- Final Report	'Online campaigning on social media platforms has become an integral part of electoral politics in Austria. Two thirds of the Austrian public use Facebook and YouTube, and half of them also use these platforms to inform themselves about political news. It is therefore important to closely monitor the inner workings and dynamics of these new electoral arenas. Wahlbeobachtung.org assembled an international team consisting of election observers,	216

[59] Summary prepared by the contractor
[60] Idem

		political scientists, data scientists, and social media experts to conduct a social media monitoring project at the occasion of the Austrian early parliamentary elections on 29 September 2019. The goal was to monitor the electoral campaign on the social media platforms Facebook, Twitter, and YouTube.'

3.5. e-Voting

Author	Title	Brief summary	Ref. No.
Russel, Zamfir	Digital technology in elections - Efficiency versus credibility?	Reference to several examples of innovative technologies introduced in different countries' electoral process discussing their benefits and problems.[61]	20
Trechsel, Kucherenko, Silva	Potential and Challenges of E-Voting in the European Union Study	'This study was commissioned and supervised by the European Parliament's Department for Citizens' Rights and Constitutional Affairs at the request of the AFCO Committee. It addresses the potentials and challenges of the implementation of Internet voting in European Parliament elections. It considers the social, political, legal, and technological implications of its introduction as an alternative to on-paper ballot and builds on the recent experience of previous trials and successful e-enabled elections to issue technical recommendations regarding Internet voting in the European Union.'	28
Boucher	What if blockchain technology revolutionised voting How blockchain technology could be used for e-voting	This article provides a brief explanation on how blockchain technology could be used in electronic voting and what its potential impacts and further developments are.[62]	37
Bulut et al.	Blockchain-Based Electronic Voting	'Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of	46

[61] Summary prepared by the contractor
[62] Idem

	System for Elections in Turkey	voters. Additionally, it takes too much time to count the votes. This paper proposes a solution using Blockchain to eliminate all disadvantages of conventional elections. Security and data integrity of votes is absolutely provided theoretically. Voter privacy is another requirement that is ensured in the system. Lastly, waiting time for results decreased significantly in proposed Blockchain voting system.'	
Jefferson et al.	What We Don't Know About the Voatz "Blockchain" Internet Voting System	This article aims to urge the disclosure of more information on the features and functionalities of the "Voatz" blockchain internet voting system. In terms of methodology, the article explains that Voatz is a recent start-up company that is operating an Internet voting system intended for public elections, used in West Virginia, US in the recent years. The authors consider that the functioning mechanisms of the Voatz system should be more transparent and clearer to the public, and therefore urges Voatz to reveal some technical details on their system by asking a number of important questions.[63]	47
a) Lupiáñez-Villanueva et al	Study on the Benefits and Drawbacks of Remote Voting + Technical Appendices	The study examines the barriers to voting encountered by different groups of citizens and maps the different types of remote voting solutions available in the EU Member States, outlining their benefits and drawbacks. In conclusion, the study points out that options for remote voting and how they operate vary greatly from one country to another, depending for example, on the electoral system, the method by which voters are registered, the design of the solution, demographic factors, and the aspects of the voting process (such as ballot secrecy) most valued by the population. This implies that in European elections, citizens vote under different systems. While proposing a common approach to the availability of remote voting for European Parliament elections would reduce the complexity of the current status quo, it would also affect the prerogatives of Member States.[64]	93
b) Faulí et al.	Study on the benefits and drawbacks of remote voting solutions - Presentation of Main findings		
Geller. Politico	Some states have embraced online voting. It's a huge risk	People's phones, tablets and computers are vulnerable to hackers. Securing the internet could take a decade or more. But some states are implementing online voting anyway. The article puts forward some main security issues that make online voting more vulnerable than other online operations.[65]	114

[63] Summary prepared by the contractor
[64] Idem
[65] Summary prepared by the contractor

Loeber	Use of technology in the electoral process: Who governs?	'There have been major concerns about the role of technology in elections, as highlighted by debates in different countries such as the U.S., the Netherlands, and Norway. One area of concern is that a lot of the equipment is not owned by the public sector—but there has been barely any research on election technology ownership in a comparative perspective. This article reports new data from an international survey of electoral management bodies (EMBs) (N = 78) with data from 72 countries. There are large differences between countries in the number and kinds of technology they use in the election process. An important finding is that even though most countries use some form of election technology, the use of election technology for actual voting (voting computers or Internet voting) is relatively rare. In terms of the difference between independent and governmental model EMBs, independent EMBs seem to be more ''in control'' of the technology used. This means that they are more likely to have a decisive role in the decision-making process and to have ownership of the technology and provide the technological support for it. These findings signal that the introduction of technology does not seem to have a negative impact on the independent position of EMBs. This means that EMBs that have a formal independent position are also in most cases independent from other actors in the election process, such as other governmental agencies and vendors, when it comes to the use of technology.'	134
Council of Europe	1289th meeting - Democracy and Political Questions	'The present guidelines are the updated version of the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections. The original two guidelines were approved in 2011 with the aim of providing guidance on how to implement the provisions on certification and transparency of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting of 30 September 2004.'	159
Gibson et al.	A review of E-voting the past, present and future	'Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process.	194

		Electronic voting has been deployed in many different types of election throughout the world for several decades.'	
Krimmer	Constitutional Constraints for the Use of Information and Communication Technologies in Elections	Electronic elections are increasingly popular worldwide. Almost every discussion addressing the introduction of electronic processes into an election begins with the question of whether such a system would be in line with existing legislation. Here we outline the basic regulations that can be derived from constitutional rules, electoral principles and special case law on the matter. Based on our findings, we propose principal considerations for developing a legal basis for the introduction of electronic elections.	203
Krimmer	Internet Voting in Austria History, development and building blocks for the future	This dissertation aims to investigate the origins of Internet voting, analyse several deployments of Internet voting technology in Austria and identify – based on these accumulated experiences – building blocks that can be useful in decision-making on and planning of future uses of Internet voting technology within Austria and throughout the world.[66]	204
Organization for Security and Co-operation in Europe (OSCE)	Handbook for the Observation of New Voting Technologies	This handbook is designed to provide basic guidance on how to observe the use of new voting technologies (NVT) in electoral processes. Several OSCE participating States have implemented or tested NVT during their elections, making use of electronic voting machines, ballot scanners, Internet voting or other electronic means. This handbook is designed to assist election observers in identifying and assessing the various elements of NVT that may impact the conduct of democratic elections.[67]	208

3.6. Hate speech and extreme negative rhetoric

Author	Title	Brief summary	Ref. No.

[66] Summary prepared by the contractor
[67] Idem

Council of Europe	Media Regulatory Authorities and hate speech	This regional publication resulting from Reinforcing Judicial Expertise on Freedom of Expression and the Media in south-east Europe (JUFREX) project, aims to contribute to a wider understanding of the concept of hate speech while providing recommendations and identifying mechanisms to prevent and tackle this problem. The publication first explores the concept of hate speech and then analyses cases of hate speech in seven (7) Europe southeast region countries (Albania, Bosnia and Herzegovina, Croatia, Macedonia, Montenegro, Kosovo and Serbia). These cases occurred in media outlet and online media. This publication also compiles in final annexes "legal framework overviews of participating countries" and "Relevant case-law of the European Court of Human Rights (ECHR)". Finally, it represents a useful tool to further activities for various relevant stakeholders such as media regulatory bodies.[68]	33

3.7. Use of new forms of fundraising for political parties

Author	Title	Brief summary	Ref. No.
International Institute for Democracy and Electoral Assistance	Open Primary Elections	This paper discusses the innovative methods of political parties to include non-members, who may be close to the party in its structures by means of open primaries. On the one hand, open primaries could be an opportunity for political parties to connect with disengaged citizens, and on the other hand to allow these citizens to influence the party's decisions. However, they may give rise to illicit funding techniques.[69]	42
European Parliament, AFCO	Institutions and foreign interferences	'This study, commissioned by the European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs at the request of the AFCO Committee, assesses the EU responses to counter foreign interferences. It examines in particular the effectiveness of the EU action against foreign interferences in the 2019 European Parliament elections, the COVID-19 crisis and the issue of foreign donations to European political parties. The study concludes with specific policy recommendations to enhance the EU's responses.'	125

[68] Summary prepared by the contractor
[69] Idem

3.8. Transparency of the elections

Author	Title	Brief summary	Ref. No.
European Parliamentary Research Service	Artificial intelligence, data protection and elections	The paper briefly elaborates on the importance of the set of European Union (EU) initiatives to strengthen free and fair election, following Facebook/Cambridge Analytica (CA) case in 2018. In conclusion and as a way forward, the paper underlines the importance of privacy and data protection to fundamental rights and freedoms, thus suggesting that the use of automated and algorithm based decision-making practices requires further transparency, shared accountability from various actors and ethical considerations.[70]	38
European Commission for Democracy Through Law (Venice Commission)	The impact of the information disorder (disinformation) on elections	'This brief is to support the 'Study on the role of social media and the Internet in democratic development' prepared by José Luis Vargas Valdez* for the Venice Commission of the Council of Europe (hereinafter: the Valdez-Study). The aim of the Brief is to (a.) provide input on relevant Council of Europe (hereinafter: CoE) standards and other instruments and materials relating to elections and the internet; and (b.) suggest additions to the Valdez-Study for a better presentation of the critical aspects regarding the enjoyment of the right to free elections within the transformed communicative spheres." In conclusion, it is recognised the importance of social media intermediaries as a positive facilitator of public and democratic debate. On the other side, it also held these intermediaries accountable for safeguarding the respect for fundamental rights such the right to free elections on their platforms.'	81
European Commission for Democracy Through Law (Venice Commission)	Joint Report on Digital Technologies and Elections (CDL-AD(2019)	'At its 59th meeting (15 June 2017), the Council for Democratic Elections, upon an initiative by Mr José Luis Vargas Valdez and on the basis of his "Study on the role of social media and the internet in Democratic development" (CDL-LA(2018)001), decided to undertake a study on the use of digital technologies during electoral processes, jointly with the Council of Europe's Information Society Department. 2. In addition to Mr Vargas Valdez, Ms Herdis Kjerulf Thorgeirsdóttir, Mr Richard Barrett and Mr Rafael Rubio Nuñez acted as rapporteurs. Ms Krisztina Rozgonyi and Ms Nevena Ružić acted as experts on behalf of the Information Society and Action against Crime Directorate, Media and Internet Governance Division and of the Data Protection Division respectively. Mr Alexander Seger, head of the Cybercrime	87

[70] Summary prepared by the contractor

		Division, also contributed to the relevant parts of this joint report. 3. This joint report was prepared on the basis of Mr Vargas Valdez's original study and of the comments submitted by the rapporteurs and experts above; it was examined at the meeting of the Sub-Commission on Latin America on 30 November 2018, by the Council for Democratic Elections at its … meeting (Venice, …) and was subsequently adopted by the Venice Commission at its … plenary session (Venice, …).'	
European Commission	Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final	The Recommendation points out that ahead of the elections for the EU Parliament the Member States should form Election cooperation networks, ensure transparency in political advertising, impose appropriate sanctions for infringements of rules on the protection of personal data and perform awareness raising activities.[71]	101
Kofi Annan Commission on Elections and Democracy in the Digital Age	Protecting Electoral Integrity in the Digital Age	The Annan commission was convened before Kofi Annan's death in 2018 in defence of electoral integrity against the misuse and abuse of social media. The Report prepared by the commission puts forward 13 recommendations grouped in 4 main categories – building capacity, building norms, actions by public authorities and actions by platforms.[72]	105
Yannakoudakis, EESC	Protection of personal data in the context of EP elections	'Opinion of the EESC: The EESC supports the objectives of the Commission proposal and agrees that democracy is one of the fundamental values on which the EU is founded. The EESC recognises that the procedures for the elections of the EP are Member State governed within the EU framework. Enabling the Authority for European political parties and European	110

[71] Summary prepared by the contractor
[72] Idem

		political foundations (the 'Authority') to impose sanctions is one way of ensuring personal data is protected and not misused for political gain. The EESC supports the additional staffing of the Authority with a view that this staff will be better positioned to work with the national DPAs to ensure that data protection infringements are properly investigated and where found sanctions applied.'	
Privacy International	Challenging Data Exploitation in Political Campaigning	'Around the world, political campaigns are becoming increasingly reliant on the exploitation of people's data for political gain. Privacy International considers that there are certain baseline safeguards that should be in place: More transparency is needed from all actors involved; Comprehensive data protection laws must be implemented; Electoral laws need to be updated for the digital age; supervisors of data protection must have sufficient independence.'	112
Democracy Reporting International	Guide for Civil Society on Monitoring Social Media during elections	This document provides important support regarding methodology, definitions and approaches to be used by civil society organisations on monitoring social media during election.[73]	131
Who Targets Me	How to take a "gold standard" approach to political transparency and policy	The article briefly introduces some issues related to political advertising. It then proposes six "gold standards" for the improvement of the transparency of the online political advertising. As the interests of civil society, private companies, political parties and other stakeholders are considerable different, the proposed six "gold standards" acceptance will depend on the discussion and balance of the trade-offs between those stakeholders.[74]	184
Kofi Annan Foundation	The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age	'New information and communication technologies (ICTs) pose difficult challenges for electoral integrity. In recent years foreign governments have used social media and the Internet to interfere in elections around the globe. Disinformation has been weaponized to discredit democratic institutions, sow societal distrust, and attack political candidates. Social media has proved a useful tool for extremist groups to send messages of hate and to incite violence. Democratic governments strain to respond to a revolution in political advertising brought about by ICTs. Electoral integrity has been at risk from attacks on the electoral process, and on the quality of democratic deliberation. The relationship between the Internet,	199

[73] Summary prepared by the contractor

[74] Idem

	social media, elections, and democracy is complex, systemic, and unfolding. Our ability to assess some of the most important claims about social media is constrained by the unwillingness of the major platforms to share data with researchers'

4. Detailed summaries of relevant literature

Disclaimer: The following summaries do not have any analytical nature. They are prepared by the contractor and only aim to reproduce to the closest extent possible the findings of the reviewed documents. Therefore, where possible, they include direct citations from the articles and their executive summaries.

4.1. European Union legal and policy and framework

4.1.1. Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and European political foundations (Ref. no. 34)

Reference title: European Parliament, Council of the European Union. 2014. Regulation (EU, EURATOM) No 11412014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations

Key words: *statute of political parties, political foundations, Authority for European Political Parties, budget, donations*

The aim of this Regulation No 1141/2014 is to create a specific legal, financial and regulatory system for European political parties and European political foundations. It increases their visibility, recognition and effectiveness by giving them a European legal personality and greater funding flexibility. The Regulation is amended in 2018 by Regulation (EU, Euratom) 2018/673 which tightens up the rules regarding registration of political parties and foundations, and transparency regarding political programmes and party logos.

In particular, the Regulation No 1141/2014, creates the independent Authority for European Political Parties that registers, verifies and may impose penalties on and/or de-register European political parties and foundations. It also creates a publicly accessible online register containing information concerning the parties and foundations and sets out registration conditions a political party or foundation, needs to satisfy, e.g. it needs to have a seat in an EU country as indicated in its statutes or it needs to have member parties represented, in at least one quarter of the EU countries, by members of the European Parliament, of national parliaments, of regional parliaments or of regional assemblies (a stipulation in Regulation (EU) 2018/673). Additionally, a political party or its member parties need to have received, in at least one quarter of the EU countries, at least 3% of the votes cast in each of those countries at the most recent elections to the European Parliament. Its member parties cannot be members of another European political party.

The Regulation also stipulates that parties may use the EU funding they receive to finance European Parliament election campaigns. Spending linked to campaigns must be clearly identified as such by the parties in their annual financial statements. A registered European political party that has at least one

Member of the European Parliament (MEP) may apply for EU funding. Important to mention is that National parties must display the logo and political manifesto of their affiliated European party on their websites as a condition to access funds. This must be done by member parties at least 12 months before the funding applications are submitted.

Last but not least, the Regulation ensures that 10% of the annual EU funding is allocated equally between the eligible parties. The remaining 90% is distributed according to their number of MEPs. The same distribution key is used for political foundations, which may have 90% of their annual costs reimbursed. Finally, it imposes strict rules apply to individual annual donations that parties and foundations may accept. These must not exceed €18,000 and any donations above €12,000 must be immediately reported to the authority. The names of donors of individual donations not exceeding €1,500 do not need to be published. Anonymous donations may not be accepted

4.1.2. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Ref. no. 144)

Reference title: European Parliament, Council of the European Union. 2000. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*

Key words: *electronic commerce, advertising, online orders, electronic contracts, liability of service providers, self-regulation, co-regulation*

Directive 2000/31/EC (the e-Commerce Directive) establishes standard rules in the EU on various issues related to electronic commerce. The following online services enter in its scope: news services (such as news websites); selling (books, financial services, travel services, etc.); advertising; professional services (lawyers, doctors, estate agents); entertainment services; basic intermediary services (internet access, transmission and hosting of information); free services funded by advertising, sponsorship, etc.

The Directive establishes the principle that operators of these services are subject to regulation (related to the taking up and pursuit of the services) only in the EU country where they have their registered headquarters – not in the country where the servers, email addresses or post boxes they use are located.

In line with the e-Commerce Directive, national governments must ensure that operators publish basic information on their activities (name, address, trade register number etc.) in a permanent and easily accessible form.

In particular, national implementing rules should ensure that advertising, the person or company responsible for it and promotional offers, games or competitions are clearly identifiable and the conditions are easily accessible and presented in clear and simple terms. Unrequested e-mail ('spam') must also be clearly identifiable. In every EU country, electronic contracts must be given equivalent legal status to paper contracts. These contracts must also include in clear and understandable terms the technical steps consumers must follow to conclude the contract; whether or not the contract will be filed by the service provider and whether consumers can view it at a later stage; how consumers can identify and correct typing errors before placing their order and the languages in which the contract can be signed. Consumers must be able to save and print out contracts and general conditions. Online orders are also subject to specific

requirements under the Directive. The service provider must confirm receipt of the order without undue delay and electronically (email, other electronic message) the order (or receipt confirmation) is considered to have been received when the seller (consumer) is able to access it.

The Directive encourages both self-regulation by operators and co-regulatory efforts with governments. Examples include codes of conduct at EU level and online systems for settling disputes out of court, especially when the seller and buyer are in different countries. EU countries must also provide fast, efficient solutions to legal problems in the online environment and ensure penalties are effective, proportionate and dissuasive.

The e-Commerce Directive also includes provisions regarding liability of service providers. Online service providers who act as mere conduit, caching or hosting services providers are not responsible for the information they transmit or host if they fulfil certain conditions. In the case of hosting service providers, they are exempted from liability as long as they do not have actual knowledge of illegal activity or information and, if they obtain such knowledge or awareness, they act at once to remove or to disable access to the information.

National governments cannot impose any general monitoring obligation on these 'intermediaries' over the information they send or store, to look for and prevent illegal activity.

4.1.3. White Paper on Artificial Intelligence - A European approach to excellence and trust (Ref. no. 147)

Reference title: European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, February 2020

Key words: *artificial intelligence (AI), technology, excellence, policy options*

This White Paper presents policy options to enable a trustworthy and secure development of AI in Europe, in full respect of the values and rights of EU citizens.

In terms of methodology, the main building blocks of this White Paper are firstly the policy framework which sets out measures to align efforts at European, national and regional level ('ecosystem of excellence'). Secondly, the key elements of a future regulatory framework for AI in Europe that will create a unique 'ecosystem of trust'.

In particular, **the White Paper puts forward recommendations** to set up partnership framework between the private and the public sector, with the aim to mobilise resources to achieve an 'ecosystem of excellence' along the entire value chain, starting in research and innovation, and to create the right incentives to accelerate the adoption of solutions based on AI, including by small and medium-sized enterprises (SMEs).

In addition, in order to create an 'ecosystem of trust', the regulatory framework must ensure compliance with the EU rules, including the rules protecting fundamental rights and consumers' rights particularly with AI systems that pose a high risk. According to the White Paper building an ecosystem of trust is a

policy objective in itself and should give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to innovate using AI.

The White Paper sets some suggestions to improve the legislative framework and address some AI-related risks and situations: Effective application and enforcement of existing EU and national legislation; Limitations of scope of existing EU legislation; Changing functionality of AI systems; Uncertainty as regards the allocation of responsibilities between different economic operators in the supply chain; Changes to the concept of safety.

When designing the future regulatory framework for AI, it will be necessary to decide on the types of mandatory legal requirements to be imposed on the relevant actors. These requirements may be further specified through standards. Such requirements should be in place regarding the training of the dataset; record-keeping; information provision, robustness and accuracy of the AI, human oversight, specific requirements for remote biometric identification. The White Paper also suggests voluntary labelling for those AI systems that do not qualify at 'high-risk' ones and are not subject to the proposed requirements.

Regarding the addressees of these requirements, in the Commission's view, each obligation should be addressed to the actor(s) who is (are) best placed to address any potential risks. The geographical scope of the legislative intervention should also be considered. In the view of the Commission, it is paramount that the requirements are applicable to all relevant economic operators providing AI-enabled products or services in the EU, regardless of whether they are established in the EU or not.

Finally, the implementation of the regulatory framework should rely on a governance structure comprising a network of national authorities, sectorial networks and regulatory authorities, at national and EU level and committee of experts providing assistance to the Commission.

In conclusion, with this White Paper and the accompanying Report on the safety and liability framework, the Commission launches a broad consultation of Member States civil society, industry and academics, of concrete proposals for a European approach to AI.

4.1.4. Building Trust in Human-Centric Artificial Intelligence (Ref. no. 148)

Reference title: Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the regions, 'Building Trust in Human-Centric Artificial Intelligence', 8 April 2019, COM(2019) 168 final

Key words: *artificial intelligence (AI); ethical AI; human-centric AI, trustworthy AI*

The Communication builds on the work of the AI High Level Expert Group (HLEG on AI) on ethical guidelines for trustworthy AI by focusing on new AI projects.

The Communication aims to launch a comprehensive piloting phase involving stakeholders on the widest scale in order to test the practical implementation of the ethical guidance for AI development and use.

In terms of methodology, the Communication focuses on the ethical guidelines developed by the HLEG on AI, an independent expert group set up by the Commission in June 2018, in view of using them from the onset of the development of new AI initiatives.

The Communication discusses the fact that in the near future AI will become an integral part of our everyday life. Nevertheless, AI brings new challenges as it enables machines to 'learn' to take and implement decisions without human intervention. Decisions taken by algorithms could suffer from data that is incomplete, tampered with by cyber-attackers, biased or incorrect. Unreflectively applying the technology as it develops could lead to problematic outcomes as well as reluctance by citizens to accept or use it. Therefore, it needs to be ensured that AI is trustworthy and human-centric.

The guidelines drafted by the HLEG on AI propose the following three components in order to achieve trustworthy AI: (1) it should comply with the law, (2) it should fulfil ethical principles and (3) it should be robust.

Based on these three components and the European values, the guidelines identify seven key requirements that AI applications should respect, so as to be considered trustworthy: (1) Human agency and oversight; (2) Technical robustness and safety; (3) Privacy and data governance; (4) Transparency; (5) Diversity, non-discrimination and fairness; (6) Societal and environmental well-being; (7) Accountability.

In conclusion, with this Communication the Commission aims to ensure that the guidelines developed by the HLEG on AI are followed in view of developing ethical and human-centric AI.

As next steps, the Communication notes the launch of a set of networks of AI research excellence centres through the EU Research and Innovation programme Horizon 2020. In addition, the Commission will begin setting up networks of digital innovation hubs focusing on AI in manufacturing and on big data, as well as will start preparatory discussions to develop and implement a model for data sharing and making best use of common data spaces together with stakeholders and MS.

4.1.5. Artificial Intelligence for Europe (Ref. no. 149)

Reference title: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, '*Artificial Intelligence for Europe*', 25 April 2018, COM(2018) 237 final

Key words: *artificial intelligence', European Union, Digital Single Market, European Initiative on AI*

The Communication explores the importance of artificial intelligence for Europe and describes the steps taken towards making the EU one of the leading global players in the development and deployment of AI solutions in AI. It further explores the current and future position of the EU in the competitive international landscape and elaborates on the impact of AI on both the public and private sectors.

The Communication aims to raise awareness of the significant positives AI will bring and is already bringing into the lives of people. It describes the necessity for the EU to join the AI race and the importance of being proactive in the development of this new technology by supporting the private and public sectors. Additionally, the Communication exposes the lack of private investment in AI development and strongly advocates leveraging public funding in order to expedite the inevitable alignment with the rest of the world.

In terms of methodology, the Communication provides statistics on funding from the public sector along with the current situation in AI adoption by countries and private companies in the EU, its Member States and in third countries.

The Communication discusses the need for the EU to continue its work on creating an environment that stimulates investments and highlights the importance of the role the Union plays in the development and exploitation of platforms providing services to companies. It emphasises the projects already being funded by the EU that focus predominantly on robotics. Funded projects include an unmanned agricultural vehicle that can mechanically remove weeds, a highway pilot using AI and Internet of Things to provide safe driving recommendations and reduce road fatalities, a robotic ortho-prosthesis and others. Furthermore, the Communication introduces the European Initiative on AI aiming to boost the EU's technological and industrial capacity. On this aspect, it describes in figures the stepping-up of investments, including project plans at a high level and budgetary figures. One of the main goals is to facilitate access to the latest technologies for all potential users, especially small and medium-sized enterprises, companies from non-tech sectors and public administrations, and encourage them to test AI by supporting an 'AI-on-demand platform' that will offer relevant services. Additionally, the Communication mentions that the EU aims to attract private investments under the corresponding research and innovation framework programme. The EU has made significant efforts over the past 15 years to open up public sector information and publicly funded research results for reuse. There is a need for data available for reuse for the purpose of training deep learning algorithms. The Communication explores the actions taken by the EU at the level of directives and guidance for data sharing and handling. One of the main messages is the rule of 'no one to be left behind' the AI bandwagon. The communication acknowledges the inevitable transformation AI will bring for jobs and states that the EU is prepared to assist in training and any preparation needed for making changes.

In conclusion, the Communication iterates the strong objective of the EU to build on through research and education.

4.1.6. Coordinated Plan on Artificial Intelligence (Ref. no. 150)

Reference title: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Coordinated Plan on Artificial Intelligence', 7 December 2018, COM(2018) 795 final

Key words: *coordinated actions on AI, investments, public-private partnership, strategies, innovation*

The coordinated plan reflects the importance of coordinated actions at European level between the Commission and the Member States to in line with the Strategy on AI for Europe, adopted in April 2018[75].

The coordinated plan sets several main objectives, such as common efforts of the Member States (e.g. in adopting national strategies); fostering public-private partnerships and financing of start-ups and innovation enterprises; promoting best practice and expertise exchange; building up the European data space and better understanding the AI security aspects.

In particular, the coordinated plan envisages that Member States and the Commission join efforts towards, among others:

Scaling up public and private investments in AI in order to meet the EUR 20 billion annual budget target in the next decade.

Bringing companies and research organisations together to develop a common strategic research agenda on AI, defining priorities in line with the needs of the market and encouraging exchanges between sectors and across borders.

Scaling up national research capacities and reaching critical mass through tighter networks of European AI research excellence centres. The large-scale reference test sites, open to all actors across Europe, will be developed using up to EUR 1.5 billion from the AI strand of the proposed Digital Europe Programme.

Exchanging best practices among Member States on how to reinforce excellence and retain talented workers.

Supporting Masters and PhDs programmes in AI through the proposed closer cooperation between AI research excellence centres and the EU's research and innovation programmes.

[75] COM (2018) 237

Developing guidelines by the European Data Protection Board on the issue of the processing of personal data in the context of research. This will facilitate the development of large cross-country research datasets that can be used for AI.

Better understanding of how AI can impact security in three dimensions: how AI could enhance the objectives of the security sector; how AI technologies can be protected from attacks; and how to address any potential abuse of AI for malicious purposes.

In conclusion, the Commission invites the European Council to endorse the coordinated plan; Member States to implement it, including by adopting national AI strategies by mid-2019, outlining investment levels and implementation measures; and the co-legislators to swiftly adopt the remaining legislative initiatives, which are essential for the success of the European AI Strategy, including the proposals put forward in the context of the next Multiannual Financial Framework.

4.1.7. Towards a common European data space (Ref. no. 151)

Reference title: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space', 25 April 2018, COM (2018) 232 final

Key words: *artificial intelligence (AI), common European data space*

The Communication presents a package of measures proposed by the Commission as a key step towards a common data space in the EU. These measures include: the reuse of public sector information; update of the Recommendation on access to and preservation of scientific information; and guidance on sharing private sector data.

The Communication is the first step in the follow-up on the mid-term review of the Digital Single Market Strategy with proposed measures for a common European data space.

In terms of methodology, the Communication highlights the socioeconomic benefits of data-driven innovation, focuses on service of data-driven innovation (including re-use of public sector information and access to scientific information), and presents private sector data as a key driver of innovation including B2B and B2G data sharing.

The Communication discusses the socio-economic benefits of data-driven innovation, from which new technologies such as AI and IoT are benefiting enormously. It stresses that the EU must take its opportunities to stimulate innovation in healthcare solutions such as telemedicine and mobile health

applications, and in full compliance with data protection legislation. Three key areas have been identified: (1) citizens' secure access to and sharing of health data; (2) better data to promote research, disease prevention and personalised health and care; and (3) digital tools for citizen empowerment and for person-centred care. Some of the proposed measures are:

To promote the re-usability of public and publicly-funded data by: reducing market entry barriers by lowering charges for data; increase the availability of data by bringing new types of public and publicly-funded data into the scope; minimise the risk of excessive first-mover advantage; and increase business opportunities by encouraging the publication of dynamic data and the uptake of application programming interfaces (APIs).

To give access to and preserve scientific information by, for example, funding a pan-European portal for the European Open Science Cloud.

To arrange access to and re-use of private sector data as further major cornerstones of a common European data space. In the context of B2B data sharing and in order to ensure fair and competitive markets for the Internet of Things objects and for products and services that rely on non-personal machine-generated data created by such objects, the following key principles should be respected: Transparency, Shared value creation, Respect for each other's commercial interests, Ensure undistorted competition, and Minimise data lock in.

To arrange access to and re-use of private sector data for the purposes of public sector bodies, the following key principles could support the supply under preferential conditions for re-use: Proportionality in the use of private sector data; Purpose limitation; 'Do no harm' (legitimate interests are respected); Conditions for data re-use; Mitigate limitations of private sector data; and Transparency and societal participation.

In conclusion, with the presented measures, the Commission hopes it will be easier for businesses and the public sector actors to access and re-use data coming from different sectors in the EU. Together with other existing initiatives (i.e. the new regulatory framework for the protection of personal data that enters into force in May 2018, free flow of non-personal data and the initiatives on boosting connectivity), these measures will create a truly European common data space essential for EU economic growth and competitiveness.

As next steps, the Communication calls upon the co-legislators to work towards a rapid adoption of the legislative element of the proposed data package to ensure that the EU can fully benefit from the opportunities offered by the data economy. It also calls upon the Member States and all other stakeholders to contribute to the announced measures and initiatives.

4.1.8. Charter of Fundamental Rights of the European Union (Ref. no. 154)

Reference title: The European Parliament and the Council and the Commission. 2000. The Charter of fundamental rights of the European Union

Key words: *Fundamental rights, personal data protection, freedom of expression, right to vote, right to stand as a candidate*

The article compiles the fundamental rights of the European Union.

The article aims to bring to the fundamental right of the citizens of the European Union.

The paper enshrines through a range of personal, civil, political, economic and social rights in the EU. For this study the articles below are especially relevant:

Article 8: Protection of personal data. Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

Article 11: Freedom of expression and information. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom and pluralism of the media shall be respected.

Article 39: Right to vote and to stand as a candidate at elections to the European Parliament. Every citizen of the Union has the right to vote and to stand as a candidate at elections to the European Parliament in the Member State in which he or she resides, under the same conditions as nationals of that State. Members of the European Parliament shall be elected by direct universal suffrage in a free and secret ballot.

Article 40: Right to vote and to stand as a candidate at municipal elections. Every citizen of the Union has the right to vote and to stand as a candidate at municipal elections in the Member State in which he or she resides under the same conditions as nationals of that State.

4.1.9. The European democracy action plan (Ref. no. 181)

Reference title: European Commission. 2020. The European democracy action plan

Key words: *Action plan, democracy, free and fair elections, media freedom, media pluralism, disinformation*

The European Democratic Action plan describes the European Union's plans to create a fair democracy in a digital world, by acknowledging the risks and setting up some rules, standards, and means of support.

The aim of this action plan is to create more clarity and have a European common way of handling the challenges of free and democratic elections in a digital environment.

As a methodology, this action plan is one of the major initiatives of the Commission's Work Programme for 2020[76], announced in in the Political Guidelines of President von der Leyen[77].

The Action plan sets out measures around three main pillars: (1) to promote free and fair elections; (2) strengthen media freedom and pluralism; and (3) counter disinformation.

In the first pillar, to promote free and fair election, democratic participation and protecting against election integrity, the Commission proposes legislation on Transparency of political advertising and communication and to make clear rules on the financing of European political parties. Also, a stronger cooperation between the Member States to ensure free and fair elections is envisaged, by exchanging information on elections' integrity related issues. Various authorities will be brought together to tackle challenges related to the electoral processes. Citizens will be motivated for more democratic engagement and to participate as a voter and/or as a candidate.

In the second pillar, strengthen media freedom and pluralism, the safety of journalists needs to be guaranteed. Therefore, the Commission will propose a recommendation on the safety of journalists in 2021. Initiatives will be launched to fight the abusive use of strategic lawsuits against public participation. These initiatives will go hand in hand with sustainable funding for projects on legal and practical assistance to journalists in the EU and elsewhere. Further measures need to be implemented to ensure more media pluralisms and to strengthen transparency of media ownership and state advertising, through the new Media Ownership Monitor. Additionally, the Commission will encourage the development and implementation of professional standards for the protection of journalists.

In the third pillar, countering disinformation, the Commission proposes to improve the Member States' capacities and the EU toolbox for countering foreign interference and disinformation. Ameliorations will be made to the Code of Practice on Disinformation in collaboration with the online platforms in a co-regulatory framework, and a more robust framework for monitoring its implementation will be set up. Finally, the Commission plans to empower the citizens to make informed decisions.

In conclusion, this European democracy action plan will be a key driver for the new push for European democracy to face the challenges and reap the benefits of the digital age. The gradual delivery of the set of measures proposed in the action plan will ensure that Europe has a stronger democratic underpinning to take up the challenges of the unprecedented economic, climate and health crises we face, in full respect for our common principles and values.

[76] https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en
[77] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

As a way forward, the Commission will review the implementation of the action plan in 2023, a year ahead of the elections to the European Parliament and reflect on whether further steps are needed.

The Commission looks forward to the further engagement of the European Parliament and the Council as well as of the wide circle of national actors, public and private, beyond government authorities, who will be instrumental to ensure the resilience of our democracy.

4.2. Microtargeting and algorithmic filtering

4.2.1. The Regulation of Online Political Micro-Targeting in Europe (Ref. no. 01)

Reference title: Dobber, Fathaigh, Zuiderveen Borgesius. 2019. The regulation of online political micro-targeting in Europe

Key words: *online political micro-targeting, political parties, privacy, data protection, right to freedom of expression, democracy, right to receive information*

This paper examines how online political micro-targeting is regulated in Europe. While there are no specific rules on such micro-targeting, there are general rules that apply.

In terms of methodology, the paper focuses on three fields of law: data protection law, freedom of expression, and sector-specific rules for political advertising; for the latter the authors examine four countries – The Netherlands, Germany, France and the UK. They argue that the rules in the General Data Protection Regulation (GDPR) are necessary, but not sufficient. They show that political advertising, including online political micro-targeting, is protected by the right to freedom of expression, which is not, however, an absolute right. From a European human rights perspective, it is possible for lawmakers to limit the possibilities for political advertising.

Firstly, the paper analyses the threats and opportunities of micro-targeting. For individuals, on the one hand, these threats are related to their privacy and personal data; the risk of manipulation of the voters, and the risk of underrepresentation of some social groups if certain voter groups are ignored when using micro-targeting. The threats for political parties on the other hand, are related to unfair advantage being given to those parties that could "afford" a digital campaign by means of micro-targeting, as the cost is high. First, this worsens the inequality between rich and poor political parties and restrains the free flow of political ideas. Second, digital intermediaries benefit from the vast amounts of personal data on their intuitive infrastructure and leverage this, as political parties are dependent on them. On the level of public opinion, micro-targeting could lead to a fragmentation of the marketplace of ideas and could make it difficult to identify the issues which the political party deems most important and those it cares the least about.

The article examines data protection legislation in Europe and concludes that the GDPR does not categorically prohibit micro-targeting, however Europe's data protection laws make micro-targeting more difficult than in, for instance, the US. This is for instance, because under GDPR it is harder for political parties to buy data about people, and in most European countries it is impossible to access voters' registration records. On the other hand, the authors highlight that the GDPR is an "omnibus" law, covering almost all usage of personal data without specific focus for instance on "micro-targeting. Therefore, it is vague and abstract. For example, freedom of expression and democracy play a larger role in the area of micro-targeting than in cases where, for instance, an app provider collects personal data for behavioural advertising.

The paper goes further to analyse political micro-targeting which, as a form of political communication, enjoys the right to freedom of expression (RFE) under Art. 11 of the EU Charter of Fundamental Rights, and Article 10 of the European Convention on Human Rights (ECHR). The authors ascertain that there are several rights at stake – the election candidate's RFE, the political party's RFE, the online platform's RFE and the public's (voters') right to receive information - and examine these rights through the prism of the case law of the European Court of Human Rights.

Third, the authors provide an overview of the national rules on political advertising in France, Germany, the Netherlands and the United Kingdom. For instance, in France, newly adopted rules obliging online platforms to provide users with fair, clear and transparent information of the use of their personal data in the context of "promotion of content related to a debate of general interest" (including who paid for it), have led Twitter, Microsoft, YouTube and Google to ban political campaigning ads with such content. Furthermore, the authors point out that at EU level the European Commission has adopted the Code of Practice on Disinformation, but the EU has never stepped into the regulatory domain of national election regulation, as it has no specific competence in this domain. National governments are therefore best placed to regulate micro-targeting. However, the question is whether online platforms should be left to "self-regulate" and ensure political micro-targeting is not damaging democracy.

As next steps, the article states that there are a range of possibilities - from not regulating micro-targeting at all, to banning micro-targeting during certain periods. In between those two extremes there are many options, including rules that aim for more transparency. More debate and research are needed on what lawmakers should do.

4.2.2. Digital Microtargeting (Ref. no. 13)

Reference title: International Institute for Democracy and Electoral Assistance. 2018. Digital Microtargeting, Political Party Innovation Primer 1

Key words: *microtargeting, elections, political parties, campaigns*

The Primer describes digital microtargeting by political parties and concentrates on examples of political parties around the world that have used legitimate microtargeting practices in their campaigns

The Primer aims to focus on European cases by showing different examples that suit different contexts, as electoral contexts differ by jurisdiction.

In terms of methodology, the primer uses different examples of political parties from around the world that have used legitimate microtargeting practices in their campaigns.

The Primer discusses that the availability and granularity of voter data has become the new cornerstone of political campaigning. Political parties and campaigns, with the help of data- driven communication experts, increasingly use big data on voters and aggregate them into datasets. In many countries, politics is becoming more issue-based and less ideology-based; therefore, larger and more precise datasets allow political parties to find out what issues matter the most to voters. With the help of microtargeting, they can reach voters with customized information that is relevant to them.

A significant part of the academic debate on microtargeting has focused on understanding the different legal contexts and its affordances. In addition, the debate has also shed light on how political digital microtargeting is affected by data-protection laws (Bennett 2016) and the current lack of capacity of these laws to fully grasp the impact of digital microtargeting in electoral campaigns. Yet the most substantial debate is around the confrontation between the negative and positive effects of digital microtargeting in political campaigns, especially the former.

Targeting voters is firstly about collecting data and dividing voters into segments based on characteristics: The first and foremost source of data is a person's voter profile. In addition to public data, political parties collect their own voter data. The third source of data is consumer data. Secondly, it is about designing personalized political content for each segment: In simple terms, voter segmentation means dividing the electorate into smaller blocks, and using different campaign methods for each segment. Lastly, targeting voters is about using communication channels to reach the targeted voter segment with these tailor-made messages: Voter profiles and consumer data combined can be a good predictor of how an individual intends to vote, and what issues the individual cares about. For a political party, this may mean the ability to create hundreds of customized messages for each constituency, each with highly personalized political content, even down to a household level.

In conclusion, microtargeting is a powerful tool available and likely to intensify, political parties and regulators have a joint responsibility to use microtargeting in a way that strengthens democratic participation.

As a way forward, the issue remains a nascent one, and the coming years will surely allow for much more comprehensive and detailed research on the effects and roles of digital microtargeting in political campaigns.

4.2.3. Commission guidance on the application of Union data protection law in the electoral context (Ref. no. 15)

Reference title: European Commission. 2018. Commission guidance on the application of Union data protection law in the electoral context

Key words: *data protection, elections, microtargeting*

The article examines the actions, from actors involved in elections, of exploring the possibilities to use data in order to win votes. Addressing issues such as microtargeting of voters based on the unlawful processing of personal data (e.g. Cambridge Analytics) is most important to restore the trust in the fairness of the electoral process.

The article aims to address actions and points of attention when dealing with sensitive data in electoral context for the parties involved.

In terms of methodology, the article sets the scene with the GDPR background and the Union data protection framework, then the key obligations of various actors are elaborated on, to end with the rights of individuals.

The paper discusses the GDP Regulation (Regulation (EU) 2016/679) which provides the Union with the tools necessary to address instances of unlawful use of personal data in the electoral context. With help from the GDPR, enforcements have to make full use of their power to address possible infringements, in particular those relating to the micro-targeting of voters.

Being part of the Union data protection framework, the GDPR addresses the shortcomings form the data protection regime from the last 20 years. It gives individuals in the Union additional and stronger rights which are particularly relevant in the electoral context. The 'e-Privacy Directive' (Directive on privacy and electronic communications 2002/58/EC) completes the Union Data Protection Framework and is relevant in the electoral context.

The application of the GDPR in the electoral process must give clarity to the actors involved: national electoral authorities, political parties, data brokers and analysts, social media platforms and online ad networks.

Data controllers and processors. The data processor processes personal data only on behalf and under the instructions of the controller. A number of actors can be (mostly) data controllers: national electoral authorities, political parties, individual candidates and foundations. Platforms and data analytics companies can be (joint) controllers or processors.

Regarding the principles and lawfulness of processing data and special conditions for "sensitive data", collected data for one purpose, can only be further processed for a compatible purpose.

Transparency, towards the individuals concerned, is required, regarding what happens with personal data and who processes it. Political parties who process data obtained from third party sources typically need to inform and explain how they combine and use this data to ensure fair processing.

Profiling can be used to micro target individuals, namely, to analyse personal data to identify the particular interests of a specific audience or individual in order to influence their actions. Micro-targeting may be used to offer a personalised message to an individual or audience using an online service e.g. social media. Organisations can be mining the data collected through social media users to create voters' profiles. This might allow such organisations to identify voters who can be more easily influenced and therefore allow such organisations to exert an impact on the outcome of elections.

Related to security and accuracy of personal data, the GDPR requires controllers to notify personal data breaches to the competent supervisory authority.

The data protection impact assessment is a tool introduced by the GDPR for assessing the risk before processing starts. It is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals.

In conclusion, the GDPR gives stronger rights of individuals in the matter of the processing of their data, but also the right to object to processing. In order to be able to exercise these rights, all parties must provide the tools necessary. According to the GDPR ways to lodge a complaint should be given.

As next steps, key data protection issues relevant in the electoral process are given for the actors (controller or processor) involved such as: Comply with purpose limitations; Choose the appropriate legal basis for processing; Ensure security of processing through technical and organisational measures; Conduct a data protection impact assessment, etc.

4.2.4. Social media and microtargeting: Political data processing and the consequences for Germany (Ref. no. 45)

Reference title: Papakyriakopoulos et al. 2018. Social media and microtargeting: Political data processing and the consequences for Germany

Key words: *microtargeting, social media, influence, datafication, electorate, algorithmic processing, AI*

The report analyses the use for political campaigning purposes of personal data and digital traces in microtargeting the voter, and to identify the possibilities and dangers of microtargeting in electoral campaigning, taking into consideration 'state of the art' technology.

The article aims to demonstrate a proof of concept regarding the ways political actors could establish the conditions for political microtargeting in Germany, through the utilization of social media platforms.

As a methodology, the ethical and political consequences are evaluated for microtargeting based on data from the social media platform Facebook, taking samples from German parties (CDU, CSU, SPD, Greens, Left party (radical left), and AfD (radical right)).

The report discusses the use of microtargeting, which can be defined as "*a strategic process intended to influence voters through the direct transmission of stimuli, which are formed based on the preferences and characteristics of an individual*."

Data gathered from the people, manually, or with data mining techniques, with the aim to be used for political campaigning is called "Big political data". It feeds into advanced statistical and machine learning algorithms (AI), with the possibilities of enabling the development of new political strategies.

On the big political data certain algorithms are used to categorise the topics of interest to be used in the microtargeting. Through machine learning, it is possible to track someone's interests and subsequently develop personalised political advertisement that can be used to influence social media users. This

practice does not necessarily lead to manipulation of voters, but anyway has the effect to influence their decision. It is important for the voter in this case to fully understand that they are microtargeted thus evaluate the send message differently.

Certain measures are proposed to help the voter correctly evaluating the received (manipulative) message send via microtargeting: transparency of data collection, processing and application, autonomy of the subject on having control of their own personal data and (in)visibility, the right to choose if and to know how personal data might be collected and used. These are stated as necessary for supporting someone's privacy. For the ethical evaluation of microtargeting, to know how data is acquired is equally important as to know who acquired it.

The use of microtargeting has some beneficial points: It has the potential to partly track the predispositions or general interests of a voter, and based on them, to modify the candidates' public images in a way that complies with the voters' opinions, avoiding sending them a message they would disagree with. Another advantage is that microtargeting allows political actors to target voters from the entire political spectrum, rather than exclusively developing their campaign on the characteristics of the median voter.

Related to measures against wrong usage, microtargeting in the EU cannot be used to its full potential due to certain barriers. Barrier 1 is the privacy and data protection policies such as the GDPR. Barrier 2 is a data bias. Most of the data is harvested from social media, and these are not an ideal representation of the real world.

In conclusion, microtargeting has its positive and negative points. Microtargeting cannot be used to its full capacity due to European regulations and the data bias caused by the way of data collecting procedures. Apart from that, a voter when receiving political messages must be aware that it was possibly send via microtargeting, and may be tailored to his profile, so would correctly evaluate the message.

As a way forward, further qualitative and quantitative research is needed, in order to uncover: (1) How political communication on social media influences the formation of political attitudes in terms of polarization, political mobilization and opinion formation? (2) What is the effect of political campaigning services offered by social media and other internet platforms? (3) At which level current privacy policies protect individuals and what else could be done?

4.2.5. Elections and media in digital times (Ref. no. 74)

Reference title: United Nations Educational Scientific and Cultural Organization. 2019. Elections and media in digital times

Key words: *elections, disinformation, fake news*

The study zooms in on a key issue related to the 2019 World Press Freedom Day theme, which focused on "Media for Democracy: Journalism and Elections in Times of Disinformation".

The aim of the study is to identify recent trends on disinformation, attacks on the safety of journalists, and disruption in election communications. The study lists possible responses in order to safeguard media freedom and integrity while strengthening news reportage on elections in digital times.

The methodology used for this study is a selection of trends on 'Elections and media in digital times' from across the world during the past three years. The study is based on desk research reviewing academic literature, selected regulatory and policy developments and an extensive range of online sources and resources.

The study describes in the first topic the International Human Rights law framework. The most relevant provisions for the purposes of the present report guarantee the right to freedom of expression (including media freedom and access to information) along with various democratic rights (including the rights of peaceful assembly and to freedom of association, the right to participate in public affairs, the right to vote in secret and the right to education). These rights permeate the principles and commitments that govern the organization of free, fair, periodic and credible elections.

The second topic discusses that disinformation distorts democracy. Disinformation can be broadly understood as falsehoods deliberately created to deceive others. It can be embedded within a range of different types of expression, including hoaxes and other types of fabricated content; manipulated images and documents; propaganda; clickbait; conspiracy theories; pseudo-science and historical revisionism. The challenges for society, and during elections in particular, that are posed by online disinformation are complex and there is no single solution.

The third topic is about threats and violence against journalists and other media actors. Journalists and other media actors continue to be subject to a litany of threats and violence, which is often aggravated on the occasion of elections. Killings of journalists and impunity for the killings persist worldwide. Rhetorical assaults, legal curbs and digital attacks on journalists, too, are on the rise. All this casts a cloud on the safety of journalists more generally, even if attacks are not evenly spread around the world and are not exclusively within an electoral context.

The last topic discusses the changes impacting on election rules and media's role. Digital developments are affecting electoral arrangements and communications, often with a disruptive impact on the potential for journalism to make its contribution.

In conclusion, Effective strategies are needed to respond to digital-enabled changes to the life cycles of elections so as to guarantee in practice the rights and standards that govern the integrity of voting, as well as the robust, but informed and inclusive public debate that underpins opinion-making processes in democratic society.

As a way forward, this study serves as a steppingstone towards the next full World Trends in Freedom of Expression and Media Development edition to be published in 2021.

4.2.6. Microtargeting in Germany for the 2019 European Elections (Ref. 107)

Reference title: Hegelich, Serrano. 2019. Microtargeting in Germany for the 2019 European Elections

Key words: *political advertising, political online advertising, microtargeting, organic reach, hyperactive users*

This article aims to analyse how microtargeting techniques were used and if and how they had impact on 2019 European Parliament elections in Germany.

In terms of methodology, as many other articles, this article also starts by analysing the tools made available by the platform operators (Google, Facebook or Twitter) - such reporting tools and the application programming interfaces (APIs) such Facebook Ad Library API or the Google Cloud BigQuery API. This advertising archive provide aggregated information on paid advertising on Facebook, Instagram, Google, and on YouTube, during the 2019 European Parliament elections. These APIs were analysed between 15th of March 2019, when they were made available until one week after elections, 2nd of June 2019. Only advertisements from Germany have been analysed, representing a total of approximately 34 000 ads, from the official accounts of the seven political parties in the German Bundestag (limiting the analysis to the official accounts of the federal parties and their state chapters).

The article starts with contextualising the increasingly importance of microtargeting as an important instrument to win election since the successful case of Obama campaign and then amplified and consolidated in Trump's campaign where over $44 million were allocated only to Facebook advertising. The author suggests that Microtargeting "means communicating targeted advertising to voters based on data analysis". This approach it is not new, as when making a speech, a politician adapts the language, topics, content, etc. to its audience. However, the author highlight that the problem arises when target advertising in social networks. As the communication in these channels is fragmented, thus the public might receive different or even contradictory messages as well.

The author then proceeds with one of the mains risks of target advertising in social network is the transparency of data, which might rise a conflict of objectives between different actors such users, advertisers, etc. For the sake of keeping transparency as one of important elements between different actor's communication, aggregated information was made available by the different platform operators (such Google, Facebook or Twitter). This made possible to track, analyse and know where and by whom a specific advertising was posted.

As other articles supported, this commitment by the platforms operators is an important step towards transparency, however, one of the problems lays on the fact that the different platforms operators have a different definition on what is political advertising. This problem is amplified by the fact that information on how the political advertisement was identified and placed for example, is only in the possession of those platforms. A resulting form of these limitations is that the data shared for scientific analysis purpose is compromised because of its reliability.

From the analysis of the political online paid advertising, it was possible to see that two parties (Christian Democratic Union and Social Democratic Party) have intensively used microtargeting approach. The findings showed also that CDU was the political party that invested the most online advertising, meaning that consolidated its professional microtargeting strategy.

After these findings, the author proceeds by proposing a new data set to measure the success of online advertising, as linking elections results to only advertising budget is too limited.

Regarding German case, the author considers that microtargeting is gaining floor on the political campaigning strategies, however, this seemed not to be fully exploited in these elections, however, it is also not possible to truly know which strategy they are taking. This is partially because, based on the data made available by the platform operators, it is not possible to know 100% what is the political party targeting strategy as this would mean to disclose full users and advertisers information, therefore, those platforms only publicly share aggregated information. On the other hand, political parties will also not publish such information, even though they possess such information and could do so.

For this reason, the author argues that is still possible to deduce what are the political parties targeting strategies based only on the aggregated data available on the APIs, because it is possible to know where and to which type of audience (in which state and to what gender i.e. women) a specific ad was first seen, meaning the it was likely showed deliberately – it is a sponsored ad. For different platforms, the author prepared furthered analysis per platforms such Principal Component Analysis for Facebook and other experiments for YouTube channels.

As final findings, the article raises the evidence on how one political party (AfD) revealed to have a successful online strategy, though using other techniques rather than microtargeting. On this matter, the article highlights that even though the organic advertising was applied, this specific case seems to be linked to the impact of hyperactive users, which the author suggests being a topic that need further analysis.

In conclusion, the article argues that though there is a clear evidence that in the last 2019 European Parliament election in Germany, the political parties' online advertising strategy had an important relevance on their campaigning strategy, it was not exploited to its maximum, for example by increasing the budget allocated for microtargeting technique. Secondly, and as other articles raised before, the data made available by the platforms operators is not fully complete and reliable, as they provide and work with different definitions of what are political ads for example.

4.2.7. Guidelines 8/2020 on the targeting of social media users (Ref. no. 130)

Reference title: European Data Protection Board. 2020. Guidelines 8/2020 on the targeting of social media users

Key words: *Targeting, personal data, special categories of personal data, social media providers, users, risks, fundamental rights and freedoms, joint controllers, roles and responsibility, transparency, access*

The Guidelines focus on the use of social media as a significant development in the online environment over the past decade.

They aim to clarify the role of social media providers and targeters as joint controllers of personal data, and their responsibilities under the General Data Protection Regulations (GDPR).

In terms of methodology, four groups of actors fall within the scope of the Guidelines: social media providers, their users, targeters and other actors which may be involved in the targeting process (data brokers, data management providers, marketing service providers, ad networks and exchanges, data analytics companies etc.). The Guidelines clarify each of these groups and their role in targeting. Regard taken of the joint responsibility that may be inherent to targeters and social media provider towards social media users, the document offers guidance concerning the targeting of these users as regards the said responsibilities.

In particular, the Guidelines, explain the targeting services offered by social media as part of their business model and the mechanisms to target social media users which have become increasingly more sophisticated over time. Specifically, targeting is done based on target criteria. These criteria can either be developed on the basis of the personal data that the users have (1) shared, or on the basis of the personal data (2) observed or derived (inferred) by the social media provider or by third parties and collected by them for advertising purposes. In addition, the Guidelines discuss the potential risks that the heterogenous data sources and their sensitive nature may create to the fundamental rights and freedoms of individuals. The Guidelines provide examples for each of the three targeting mechanisms. In the first case, targeting may take place either when the user shares data with the social media provider (e.g. age, civil status etc.) and these data is used by targeters to create their advertisements, or when the user shares data with the targeter, which data are then matched with the data held by the social media platform. In both cases the Guidelines explain the roles of the social media providers and targeters as joint personal data controllers, as well as the legal basis for their responsibilities. In the second case, the Guidelines describe the possible ways social media providers may observe users' behaviour – pixel-based targeting, geo-targeting and through the social media service itself. In the third case, inferred data are data that the social media providers or targeting infer from information regarding the interests of the user, e.g. if the later likes photos of impressionist paintings it can be inferred that s/he is a fan of impressionism.

First group of risks include exercising profiling activities that may go beyond the reasonable expectations of the data subject, and involve an interference and interests or other characteristics, which the data subject did not actively disclose. In other words, the individual may no longer control his or her personal data. Second group of risks relates to the possibility to manipulate the user's behaviour and political or purchasing decisions. Certain targeting approaches may however go so far as to undermine individual autonomy and freedom, e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns. The article mentions online political microtargeting which may sometimes involve disinformation or polarising messages and stimulate certain emotions or reactions, which may undermine the democratic electoral process. Additionally, collection of personal data on the individuals' browsing behaviour, may create chilling effects on freedom of expression, including access to information, because individuals may think they are constantly monitored.

The Guidelines go further to discuss the various obligations of joint controllers under the GDPR, such as transparency and right of access. They encourage joint controllers to perform data protection impact assessments (DPIA) if they estimate that the envisaged targeting operations are "likely to result in a high risk". It should also be determined that processing involves special categories of personal data and if so, to find a legal basis of this processing.

In conclusion, the Guidelines discuss the roles and responsibilities of social media providers and targeters. The EDPB considers that the they should have a joint arrangement which should encompass all processing operations for which they are jointly responsible (i.e. which are under their joint control). Insofar

as the terms of the joint arrangement do not bind supervisory authorities, supervisory authorities may exercise their competences and powers in relation to either joint controller, as long as the joint controller in question is subject to the competence of that supervisory authority.

4.2.8. Political Microtargeting Relationship between Personalised Advertising on Facebook and Voters' Responses (Ref. no. 138)

Reference title: Kruikemeier, Sezgin, Boerman. 2016. *Political Microtargeting Relationship between Personalised Advertising on Facebook and Voters' Responses*

Key words: *personalised ads, political microtargeting, persuasion, political posts, Facebook.*

The study examines the effects of exposure to regular political posts vs. personalised political ads on Facebook on the intention to engage in electronic word of mouth (eWOM) and perceived trustworthiness of the post's source. It also investigates whether informing voters about the practice of personalised advertising may change effects.

It aims to understand citizens' responses toward political messages on social network sites (SNS) and to address the gap in the literature as regards the persuasiveness of personalised ads.

In terms of methodology, in order to examine the underlying process, the study looks into the mediating role of the use of persuasion knowledge, defined as personal beliefs toward, and knowledge about, advertising. It uses quantitative methods for analysis.

In particular, the article points out some benefits people see in personalised ads, such as reducing information overload, serving users' needs, and providing aids for decision-making. However, it also mentions privacy concerns and perception that personalised ads are creepy. Especially in when the ad content is political, positive impact almost does not exist. Personalised ads lead to lower support for politicians, lower engagement in political behaviour, negative attitudes, lower source trustworthiness, and more ad scepticism. It compares the degree of persuasion knowledge of users when they receive personalised ads or regular posts. Research has demonstrated that making the commercial purpose of an ad more salient, by disclosing it using a label 'Sponsored', enhances the activation of persuasion knowledge. Therefore, the authors expect that compared with a regular post, a personalised Facebook ad may activate citizens' persuasion knowledge. However, research has also provided evidence for the fact that labels, such as Sponsored, are often unnoticed and misunderstood. This means that the label, Sponsored, may not be sufficient to activate citizen's persuasion knowledge. For that reason, the authors examine whether a training that informs citizens about the practice of targeted advertising may help them develop their persuasion knowledge and, consequently, use this knowledge in response to a personalised ad.

The authors therefore put forward a hypothesis 1, expecting that a regular political post on Facebook is less likely to 'unlock' motivation in the user to scrutinise the post, a personalised ad is more likely to motivate him/her to do so, and an ad together with a training has the highest potential to activate his persuasion knowledge. In the situation where a label is not provided, and people are not aware of the commercial nature of a Facebook post, they are probably more

likely to use the peripheral route. The fact that their friends like the sender of a post or the post itself may then be a cue that influences their attitude and behaviour. In addition, the authors expect that the different Facebook posts and a training may influence citizen's likelihood to engage in eWOM. In this study, eWOM is defined as any positive or negative statement made by potential, actual, or former voters about a political party or politician, which is made available to a multitude of people through the Internet. On Facebook, eWOM includes, for instance, liking the post, commenting on it, or sharing it with others. People are more likely to engage in eWOM when they see their friends' involvement in ads on Facebook. Therefore hypothesis 2 reads that the level of persuasion knowledge in response to the three types of Facebook posts (regular post vs. personalised ad vs. personalised ad plus training) negatively affects (a) the perceived trustworthiness of the political party and (b) the intention to engage in eWOM. The two hypotheses are examined by specific analysis methods.

In conclusion, the study finds that citizens seem to understand the techniques that are used on Facebook and this can generate resistance toward the ad. Thus, what appears to be an opportunity—personalizing ads to reach possible voters—might not always be beneficial in practice.

As next steps, the study recommends further work to be done in order to examine whether personalising ads also leads to more positive implications, such as mobilizing citizens to vote, or other negative implications, such as political content avoidance.

4.2.9. Opinion 3/2018 on online manipulation and personal data (Ref. no. 152)

Reference title: European Data Protection Supervisor. 2018. Opinion 3/2018 on online manipulation and personal data

Key words: online manipulation, personal data, privacy, microtargeting, predictive profiling, algorithm-determined personalisation

The Opinion discusses online manipulation and the implications on fundamental rights it may have, specifically but not limited to the right of data protection.

They reason for publishing the Opinion is because of the intense ongoing public debate about the impact of today's vast and complex ecosystem of digital information on not only the market economy but also on the political economy, how the political environment interacts with the economy. Personal data is needed to segment, to target and to customise messages served to individuals, but most advertisers are unaware of how such decisions are taken and most individuals are unaware of how they are being used. In addition, the fundamental rights to privacy and to data protection are clearly a crucial factor in remedying this situation, which makes this issue a strategic priority for all independent data protection authorities.

The aim of the Opinion is to help the European Union lead by example in the global dialogue on data protection and privacy in the digital age by identifying cross-disciplinary policy solutions to the Big Data challenges and developing an ethical dimension to processing of personal information.

The EDPS points out that the issue of using information and personal data to manipulate people and politics goes beyond the right to data protection. A personalised, microtargeted online environment creates 'filter-bubbles' where people are exposed to 'more-of-the-same' information and encounter fewer opinions, resulting in increased political and ideological polarisation. It increases the pervasiveness and persuasiveness of false stories and conspiracies.

According to the Opinion, research suggests that the manipulation of people's newsfeed or search results could influence their voting behaviour. The Opinion states that respect for fundamental rights, including a right to data protection, is crucial to ensure the fairness of the elections.

In particular, the Opinion first summarises the process whereby personal data fuels and determines the prevailing cycle of digital tracking, microtargeting and manipulation. It then considers the roles of the various players in the digital information ecosystem as well as the fundamental rights at stake, the relevant data protection principles and other relevant legal obligations.

In conclusion, the EDPS is of the view that the problem of online manipulation is only likely to worsen, that no single regulatory approach will be sufficient on its own, and that regulators therefore need to collaborate urgently to tackle not only localised abuses but also both the structural distortions caused by excessive market concentration.

4.2.10. Online Political Micro-targeting: Promises and Threats for Democracy (Ref. No. 217)

Reference title: Zuiderveen Borgesius et al. 2018. Online Political Micro-targeting: Promises and Threats for Democracy, Utrecht Law Review, Vol. 1(1)

Key words: online political micro-targeting, political parties, online platforms, threats, promises, democracy, data protection, GDPR

This paper focuses on the questions of what online political micro-targeting (OPM) is, and what its promises and threats for democracy are.

In terms of methodology, it combines insights from both a legal and social science perspective. The authors focus mostly on European countries and the United States (US). It introduces the practice of OPM, discusses its promises and the threats for democracy for regarding citizens, political parties, and public opinion and why the threats, while serious, should not be overstated. The article also explores how policymakers in the EU could intervene and sketches some problems they would encounter if they did so.

In particular, the article starts with referring to the origin of OPM, namely it was developed in the US in the context of offline canvassing and has since developed and enriched this traditional form of OPM with new methods of data collection and analysis, because in the US, political parties and intermediaries hold extremely detailed information about possible voters. Although not yet widely deployed in Europe, it appears that political parties across Europe look to the practices in the US for inspiration (e.g. during the 2015 elections in the UK and the Dutch Green Party which has hired the US-based digital strategy firm Blue State Digital).

Furthermore, according to the authors, some of the main promises of OPM for citizens are increased political participation and thus strengthened democracy; mobilisation of voters to cast their vote on elections day; more informed voting choices through increased political knowledge provided by media; amplified campaigning effects, because micro-targeting enables politicians to engage audiences through more relevant advertisements and to reach citizens that opted out of traditional media exposure like television and newspaper but still use Internet. However, there are also threats for citizens, such as privacy invasion,

manipulation risks and risks of being ignored. From the perspective of political parties, promises of OPM are that it can be cheap, efficient, and effective, as smaller and newer parties can target in a more agile way only their likely supporters and campaigns can focus only on the actual and potential constituencies and not on a broad range of voters, which will save money to the party. On the other hand, OPM can also be expensive and thus give more power to intermediaries. Certain types of microtargeting require political parties to develop know-how; to build and maintain voter records; to collect and analyse business intelligence; to design and manage campaigns; to use digital communication channels to target voters; and to integrate all those elements in a system that enables a minute-by-minute adjustment of campaigns. In addition, in recent years, a new industry has developed that provides data-driven services (e.g. measuring public opinion, building and maintaining voter profiles with voters' interests and anxieties, to design personalised political messages and deliver them to individual voters). Some intermediaries, such as social media platforms, are in a near-monopoly position in providing certain service, which gives them unprecedented power to set prices and dictate the terms upon political parties. Regarding public opinion, microtargeting promises to increase the diversity of political campaigns, and voters' knowledge about certain issues, that are of their interest. However, information about how important these issues are to the political party is not communicated. In other word, voters may wrongly assume that their issue of interest is also a central issue in the party's programme. In addition, fragmentation of the marketplace of ideas is also a threat. The authors believe that these threats would not necessarily materialise in Europe and be as big as in the US. This is because the rules of the GDPR are well-designed in this regard, but also because the electoral systems in Europe are not majoritarian like in the US and the United Kingdom and there is no possibility to win elections based on winning the majority of votes only in specific regions. Moreover, campaigns in Europe have much lower budgets. Finally, voters do not live in a digital bubble and cannot be easily manipulated as they learn from sources other than the Internet, as well.

In conclusion, policymakers have several options to mitigate the risks of microtargeting. However, first more information about this technique is necessary.

As next steps, the authors suggest 1) more research on micro-targeting, specifically on its effects on citizens, including a normative component. and debate about online political micro-targeting is necessary; 2) more transparency, specifically in terms of amount of money political parties spend on online campaigning or introducing a requirement for parties to provide a copy of each online ad to a central repository, to allow to see what a party promises to different people. 3) If research or experience shows that micro-targeting is indeed a problem that needs a solution, more substantive regulation could be considered, e.g. campaign expenditure restrictions could be imposed on political parties, placing caps on online political microtargeting, or even an outright ban on OPM, which could be limited to election periods.

4.3. Online disinformation

4.3.1. Securing free and fair European elections: a Contribution from the European Commission to the Leaders' meeting (Ref. no. 03)

Reference title: European Commission. 2018. Securing free and fair European elections: a Contribution from the European Commission to the Leaders' meeting

Key words: *elections, political campaigns, disinformation, transparency, GDPR*

The contribution describes how the resilience of the EU's democratic system is part of the Security Union and attacks against the electoral infrastructure and campaign information systems are hybrid threats that the Union needs to address.

The contribution aims how the EU should take all actions within its powers to defend its democratic processes against manipulation by third countries or private interests.

In terms of methodology, the European Commission (EC) proposes to the European Parliament (EP), together with this Communication, a package for bolstering democratic resilience for: balanced, comprehensive and targeted actions to support the integrity and effective conduct of the 2019 elections to the EP.

The contribution discusses that election periods have proven to be periods which are particularly prone to targeted disinformation. These attacks affect the integrity and fairness of the electoral process and citizens' trust in elected representatives and as such they challenge democracy itself. Therefore, the EC proposes several instruments to counter this. The General Data Protection Regulation (GDPR) provides the tools necessary to address instances of unlawful use of personal data in the electoral context. The revised Regulation on the statute and funding of EU political parties, increases the recognition, effectiveness, transparency and accountability of EU political parties and EU political foundations. The Directive on privacy and electronic communications (Directive 2002/58/EC) applies to unsolicited communications for direct marketing purposes, including political messages conveyed by political parties and other actors involved in the political process. It also ensures confidentiality and protects information stored on a user's terminal equipment. The proposed Regulation on Privacy and Electronic Communications will further strengthen citizens' control by enhancing transparency and widen the scope of protection beyond traditional telecom operators to include internet-based electronic communication services. The EC has put forward an EU approach for tackling online disinformation in its Communication of 26 April 2018. Through this, the EC seeks to promote a more transparent, trustworthy and accountable online environment. One of its key deliverables is the development of an ambitious Code of Practice on Disinformation which should commit online platforms and the advertising industry to ensuring transparency and restricting targeting options for political advertising. The EC also encourages MS to establish and support a national election network and appoint contacts to take part in a EU cooperation network for elections to the EP.

In conclusion, online activities in the electoral context present a novel threat and require specific protection. All involved actors have to step up their efforts and cooperate to deter, prevent and sanction malicious interference in the electoral system. The measures put forward by the EC in this package support these efforts.

As a way forward the EC urges the EP and the Council to ensure that the proposed targeted changes to Regulation (EU, Euratom) No 1141/2014 are in place in time for the 2019 elections to the EP. The EC will report after the 2019 elections to the EP on the implementation of this package of measures.

4.3.2. Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation (Ref. no. 04)

Reference tile: European Regulators Group for Audiovisual Media Services. 2019. Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation

Key words: *disinformation, online platforms, political advertising, issue-based advertising, Code of Practice*

The report describes the analysis of ERGA sub-group responsible to assist the European Commission (EC) on monitoring the implementation of commitments made by main online platforms Google, Facebook and Twitter and signed in the Code of Practice on disinformation (Code).

In terms of methodology thirteen (13)[78] countries' team produced reports on political and issue-based advertisements from 05th May to 25th of May 2019 and were submitted to ERGA sub-group. Such monitorisation was based on stored material in the archives of political advertising of each platform (which use different criteria) only when available online. These teams – National Regulator Authorities (NRA)– used six (6) main questions related to the Code and 3 questions related to the degree of transparency of advertisements.

This report elaborates in first place the non-existing common definition to the phenomena, where different concepts are used: fake news, false information and disinformation. However, to the context of this report, ERGA uses disinformation's definition as provided by the EC on the "Communication on tackling online disinformation: a European approach".

The report then explores the reasoning behind ERGAs' action and observation on this topic, which is explained following the adoption in December 2018 of the Action Plan against Disinformation, where the EC and ERGA (in a support role) were made responsible for monitoring the implementation of the Code of Practice on Disinformation five areas of commitment.

The report underlines several conclusions. In general, platforms monitored are implementing important initiatives to meet Codes' commitment in terms of making their platforms compliant to the law and to increase cooperation with competent institutions. Secondly is concludes that there was positive progress

[78] Belgium, Croatia, Cyprus, France, Hungary, Italy, Ireland, Latvia, Luxembourg, Poland Slovakia, Sweden and Spain.

on implementation of Codes' commitment such creation of an ad hoc procedure for political ads identification and online repository of political ads was made publicly available, though information presented on those repositories lacks in detail being shared in summary format.

Regarding the platform's database: even though the Code comprises the commitment of empowering the research community, the platforms were not collaborative on consenting access to overall database of advertising and data in online archive. As a result, the information accessed was not complete and not all political advertising was correctly labelled which compromised fully comprehensive and credible conclusions.

Another finding refers to the fact that Facebook was the only platform that made "issue-based" advertising more transparent within the archives.

Several challenges were encountered during the monitoring process such as diversity of disinformation and political ads definitions across the Member States (MS) and in some cases even inexistent; restricted legal competences and resources of NRA which affected their capacity to engage in monitoring activities of online platforms

In MS where more than one type of election take place at the same time, was not possible to examine if political ads identification covered regional or national elections, besides European elections

There are current challenges on regulating and monitoring audiovisual sector that are posed by new communications technologies that could be tackled with innovative technologies.

Finally, the report also concluded that in order to achieve a co-regulatory approach, the report states that first the provision in the Code should become enforceable and secondly, the institution responsible for monitoring should have autonomy and necessary tools and information, which will enable more comprehensive conclusion.

4.3.3. Regulating disinformation with artificial intelligence (Ref. no. 05)

Reference title: Alaphilippe et al. 2019.

Key words: *artificial intelligence (AI), automated content recognition (ACR), freedom of expression, disinformation*

The article examines the consequences of the increasing use of artificial intelligence (AI) disinformation initiatives upon freedom of expression, pluralism and the functioning of a democratic polity.

The article aims to examine the trade-offs in using automated technology to limit the spread of disinformation online, and to presents options to regulate automated content recognition (ACR) technologies.

In terms of methodology, the article presents the background and definitions used, then it scopes the policy boundaries, then maps existing regulatory and technological responses to disinformation, and concludes with presenting the policy options.

The paper discusses definition for “disinformation” and suggests 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit'. This is in line with the European Commission High Level Expert Group. The study distinguishes disinformation from misinformation, which refers to unintentionally false or inaccurate information.

Automated content recognition (ACR) technologies can be used for moderation and identification of content. For moderation at large scale it serves as a help for a human. Using ACR for detection is prone to false positives and negatives because due to the difficulty of parsing multiple, complex, and possibly conflicting meanings emerging from text.

Evidence of harm from disinformation is still inconclusive. Restrictions to freedom of expression must be provided by law, legitimate and proven necessary, and as the least restrictive means to pursue the aim. The illegality of disinformation should be proven before filtering or blocking is deemed suitable.

Different aspects of the disinformation problem merit different types of regulation. All proposed policy solutions stress the importance of literacy and cybersecurity.

Disinformation differs on the internet compared to other forms of media, focusing on (a) the changing media context and (b) the economics underlying disinformation online. Alongside the use of AI, which also has its limitations, a typology of self- and co-regulatory solution can be considered. Identifying components of the disinformation problem helps in the identification of the various components of the solution, and to comprehend the uses of disinformation, it is necessary to understand user behaviour.

A view is given into the policy and technology initiatives relevant to disinformation and illegal content online with the aim of understanding: (a) how the technology is recommended as a solution, (b) necessary safeguards to limit the impact, and (c) the existing initiatives onto the typology of self- and co-regulatory solutions.

In conclusion, the policy options are presented, paying particular attention to interactions between technological solutions, freedom of expression and media pluralism. Disinformation is best tackled through media pluralism and literacy initiatives, as these allow diversity of expression and choice. Source transparency indicators are preferable over de-prioritisation of disinformation. Regulatory action is not advised when it would encourage increased use of AI for content moderation purposes, without strong human review and appeal processes. Independent appeal and audit of platforms' regulation of their users should be introduced. When technical intermediaries need to moderate content and accounts, detailed and transparent policies, notice and appeal procedures, and regular reports are crucial. Standardise notice and appeal procedures and reporting and create a self- or co-regulatory multi-stakeholder body, such as the UN Special Rapporteur's suggested 'social media council'. And finally, a lack of independent evidence or detailed research in this policy area means that the risk of harm remains far too high for any degree of policy or regulatory certainty. Greater transparency must be introduced into the variety of disinformation reduction techniques used by online platforms and content providers.

As next steps, that the authors of the article believe legislation may be premature and potentially hazardous for freedom of expression: collaboration between different stakeholder groups with public scrutiny is preferable, where effectiveness can be independently demonstrated via audit.

4.3.4. Fake news and disinformation online (Ref. no. 09)

Reference title: European Commission. 2018. Flash Eurobarometer 464 - Fake news and disinformation online?

Key words: *fake news, disinformation, public survey, Eurobarometer*

The article examines explores EU citizens' awareness, by means of the Eurobarometer, of and attitudes towards the existence of fake news and disinformation online.

The article aims to have a view of the levels of trust of citizens in new media sources, and their awareness of fake news. Additionally, it takes a view on media actors on how they act to stop the spreading of fake news.

In terms of methodology, the study was carried out by means of the Eurobarometer survey (by DG COMM) in the 28 MS, and then analysed by DG CNECT, based on the results per country, but also by responses given by different social-demographic groups.

The paper discusses the findings of the study, in which they saw that most of the respondents (citizens of the Union) are less likely to trust news and information from online sources than from more traditional sources. It is seen that the radio, TV and printed media are perceived more trustworthy, where video hosting websites, podcasts and online social networks are seen as less trustworthy.

The majority of the respondents are convinced that they encounter fake news at least once per week. Most of the people are confident that they are able to identify fake news (information that misrepresents reality or is false), still a quarter of the citizens is not confident they would recognize it. Respondents who use online social networks more regularly, and who come across fake news more frequently, are more confident in their ability to identify them.

The big majority of the citizens thinks that fake news is a problem in their country and could be of some threat to democracy. The more fake news is encountered, the more it is perceived as a problem.

Most respondents are of the opinion that it is up to the journalists to act and stop the spread of fake news. This is followed (in descending order) by national authorities, media, the citizens themselves. Less than a quarter of the citizens thinks this task is up to the EU institutions, and non-governmental organisations.

In conclusion, the current survey indicates a degree of mistrust of the media, where most people at least 'tend to trust' traditional media sources. Only a minority of respondents thought that their national media provide information free from political or commercial pressure. The fake news is encountered by most at least once per week, and this is perceived as a problem for the country as well as for democracy in general. The level of concern is widespread across different MS and between different socio-demographic groups.

As next steps, the study confirms that the existence of fake news is acknowledged as a genuine, serious issue by the public. There is no clear consensus on who should act to stop the spread of fake news. All involved actors have some part in this act, and it is suggested that, at least in the view of the public, co-ordinated efforts are required from a range of different institutions and media actors.

4.3.5. Far right networks of deception (Ref. no. 10)

Reference title: Avaaz. 2019. Far right networks of deception - Avaaz investigation uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections

Key words: *Facebook, EU elections, disinformation*

The article examines, EU wide, the networks of disinformation on Facebook, in the period ahead of the EU elections.

The article aims at finding these networks and their tactics in the different MS, and eventually in cooperation with Facebook, to close them.

In terms of methodology, the report focuses on two main aspects of disinformation on Facebook. Firstly, it exposes pages, accounts and groups that are spreading "disinformation content," secondly, it identifies networks that are using "disinformation tactics". This with a focus on 6 Member States: Germany, UK, France, Italy, Poland and Spain.

For this study, researchers studied monitored disinformation operations across the continent, focusing on identifying fake news and hate speech, uncovering the networks driving them, and working with platforms and governments to take action against malign actors and issue corrections to false information. 550 groups and 328 accounts were identified, which had a total amount of 32 million followers in Europe. As a reaction Facebook took down 66% of the reported profiles. The scale of these profiles is an amount of activities which is bigger than all the activities of the European far right parties' official pages together. From the analysis per country, reoccurring tactics were identified such as: Using face and duplicated accounts. With hiding the real identity of the people managing groups and pages they avoid responsibility; Abnormal coordination and sharing of alternative outlets. Pages and groups mostly share and post content in a highly coordinated manner from a handful of specific "alternative outlets", Recycling followers. Pages start off as an innocent group, but after a name change, turn into far right or disinformation pages that recycle the follower, serving them content completely different than what they had initially signed up for; And 'Bait and switch'. A page starts off with a name covering popular interests. Once the audience is built, the page admins appear to deliberately start boosting political or divisive agendas.

The detected pages and analysis per country, mostly from far-right networks. The main detected activities per country were: Germany - Fake pages to artificially amplify messages, illegal page content; France - Disinformation spreading pages, pages concerning racism and anti-migrants; Italy - Pages spreading false information, and pages with hateful and anti-migrant messages; UK - Spam pages to boost low-trust websites, pages with open support of dangerous

individuals, duplicated and fake profiles; Poland - Pages with anti-immigration and anti-EU topics and false and misleading information; and Spain- Networks spreading disinformation and hateful content.

Avaaz describes a "Correct the Record" approach as a process to deal with disinformation pages: (1) Define. Independent fact-checkers verify that content with significant reach is false or misleading; (2) Detect. Platforms must make it easy for users to report potential disinformation; (3) Verify. Independent, third-party, verified fact-checkers determine whether reported content is disinformation; (4) Alert. Each user exposed to verified disinformation should be notified immediately; (5) Correct. Each user exposed to disinformation should receive a correction, at best effort equal to the original content.

In conclusion, the study resulted in the shutdown of numerous Facebook pages, just before the polls.

As next steps, the article recommends that social media platforms, such as Facebook, immediately issue corrections from verified fact-checkers to every single user who has seen or interacted with disinformation on the platform; and inform followers of pages that have been taken down or demoted about the malign efforts of those pages. It also needs to run a proactive and EU-wide scan for further suspicious activity on its platform.

4.3.6. EU Code of Practice on Disinformation (Ref. no. 12)

Reference title: European Commission. 2018. EU Code of Practice on Disinformation

Key words: *disinformation, Code of Practice*

The Code describes a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation.

The Code aims to achieve the objectives set out by the European Commission's (EC) Communication presented in April 2018. It outlines the key overarching principles and objectives which should guide actions to raise public awareness about disinformation and tackle the phenomenon effectively, as well as the specific measures which the EC intends to take in this regard.

In terms of methodology, the Signatories have drafted the Code and its Annexes which are an integral part of the Code. The Signatories commit themselves to the commitments listed next to their names.

The Code discusses for the first time worldwide that industry agrees, on a voluntary basis, to self-regulatory standards to fight disinformation. The Signatories recognise and agree with the EC's conclusions that "the exposure of citizens to large scale Disinformation, including misleading or outright false information, is a major challenge for Europe. Open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes". "Disinformation" is defined as "verifiably false or misleading information" which, cumulatively, "Is created, presented and

disseminated for economic gain or to intentionally deceive the public"; and "May cause public harm", intended as "threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security".

The Signatories recognize that because the various Signatories operate differently, with different purposes, technologies and audiences, the Code allows for different approaches to accomplishing their goals.

In conclusion, the Code of Practice was signed by the online platforms Facebook, Google and Twitter, Mozilla, as well as by advertisers and advertising industry in October 2018 and signatories presented their roadmaps to implement the Code. In May 2019, Microsoft subscribed to the Code of Practice and also presented its roadmap.

As a way forward, the signature of the Code of Practice will be followed by an assessment period of 12 months, during which the Signatories will meet regularly to analyse its progress, implementation and functioning. The Signatories will meet at the end of the assessment period to evaluate the effectiveness of the Code of Practice in connection with each of the commitments set forth above. After the assessment period, the Signatories will meet annually to review the Code and to take further steps if necessary.

4.3.7. Tackling online disinformation: a European Approach (Ref. no. 14)

Reference title: European Commission. 2018. Tackling online disinformation: a European Approach

Key words: *online disinformation, cyberattacks, electoral process, social media, media pluralism, quality journalism, new technologies, Artificial Intelligence, blockchain, fundamental rights, freedom of expression*

The Communication elaborates on the key challenges of online disinformation, its impacts on European democratic values and it **aims** at outline principals and objectives to be consider as guide to actions on raising public awareness on disinformation phenomena.

In terms of methodology, the Communication was prepared based on an extent consultation process to experts and to citizens, as it comprehends the inputs from High-Level Expert Group, a public consultation process including almost 3000 replies to online questionnaire and broader dialogue with key stakeholders. Moreover, it also includes an opinion poll to all EU Member States (MS), prepared by the Eurobarometer.

The Communication starts by exposing the potential of social media and Internet in a more participatory and inclusive democratic process as it enables citizens the easily access to a diverse volume of information. However, on the downside, the use of new technologies through social media helps spreading and amplifying disinformation in a personalised and in an unprecedent fast way which has effects in numerous aspects such weaken the trust in institutions, harm fundamental rights such freedom of expression, create societal tensions, influence decision-making processes while influencing public opinion and debate and impacts on democratic and transparent electoral processes – which protection is primarily responsibility of MS, however, the Communication draws the importance of a response at EU level to effectively tackle online disinformation.

The Communication then enters on exploring the scope and causes of online disinformation. First define disinformation[79] that is having an increasing and greatly impact and resulting from a combination of "economic (insecurity), technological, political and ideological (rising extremism) causes combined with the context of media sector going through a deep transformation with the arising of platforms undertaking the role of content aggregators and distributors from media outlets[80], however without assuming editorial frameworks and capabilities as well". Finally, it indicates the impact of social networking technologies that are manipulated to spread disinformation trough: creation of disinformation (use of real pictures, articles, audio, as well as deep fakes); amplification trough social and other online media (with algorithm-based mechanisms, advertising-driven and technologic-enabled e.g. "bots") and trough dissemination by users which propagates more rapidly on social media, without a previous verification of the content.

The Communication indicates five principles of transparency (regarding the origin, sponsoring and dissemination of information), diversity and credibility (of information) and inclusive solutions, which serve as guide to actions as follows:

A more transparent, trustworthy and accountable online ecosystem. The lack of transparency and traceability in the current platforms are the key enablers to creation, amplification and dissemination of disinformation, thus it is crucial actions based on the following objectives such as adequate changes in the platforms: including the EC creation of Code of Practice on Disinformation to support online platforms and other actors to achieve objectives such improve transparency with regard to sponsored content; intensify efforts to eliminate fake accounts or setting rules for bot in order to their activities not to be confused with human communication. At the same time, the EC proposes to deliver a study to assess the applicability of EU rules and if there are gaps on identifying online sponsored content.

Another action is related to increase fact-checking capabilities and enhance the use of new technologies on how information is created and disseminated. Such fact-checker process should operate based independence principle, be guided by high standards[81] and perform activities such identifying and mapping disinformation mechanisms. Parallel to this, the EC proposes to support the establishment of an independent European network of fact-checkers focused in the exchange of best-practices. This network will be supported by a new European online platform on disinformation.

The Communication enumerates new technologies and how they can be used to support several outlined activities: Artificial Intelligence (AI) could be used for process of identification and tagging disinformation, blockchain could support on validating reliability and traceability of information. The incentive of initiatives on new technologies by the EC is particularly visible through the Next Generation Internet initiative.

Secure and resilient election process . Acknowledging the fact that for the last years, 18 countries have experienced manipulation or disinformation techniques during electoral process and considering the context of 2019 pre-European elections period, the EC encouraged MS[82] to identify and share best practices on

[79] "verifiable false or misleading information that is created, presented or disseminated for economic gain or to intentionally deceive the public, and may cause public harm".
[80] Includes newspaper, magazines, radio, TV or Internet.
[81] Such the International Fact-checking Network *Code of Principles*
[82] Via RECOMMENDATION (EU) 2018/234 – on enhancing European nature and efficient conduct of the 2019 elections to the European Parliament

detection, mitigation and risk management of disinformation and cyberattacks on elections. In line with this initiative, another Directive on security of Network information systems (NIS Directive), established a Cooperation Group for the mapping of "existing initiatives on cybersecurity of network and information systems used for electoral process"

Fostering education and media literacy. The risk that disinformation poses to different spheres of society is enormous, where the increasing of resilience to that technique depends intimately on the development of digital competences and skills. For that reason, in 2018, the EC adopted the Digital Education Action Plan[83]. Furthermore, the Communication lists another set of actions from EC with objective of stimulate the dissemination of good practices among MS and relevant actors such supporting "Media literacy for all" pilot project.

Support for quality journalism as an essential element of a democratic society will require actions such as investing in high quality journalism, rebalance media and online platform relation and embrace opportunities offered by new technologies in order to improve fact-checking and verification

Countering internal and external disinformation threats through strategic communication. The Communication supports that efficient response to disinformation depends on strong adequate communication and awareness-raising by public authorities. To this end, besides detection and data analysis measures above-described a strategic communication requires a suitable diffusion of activities.

In conclusion, the European Commission via this Communication calls for all relevant actors' efforts to address the phenomena properly and encouraging to implement the outlined actions.

As a way forward, the Commission planned a report on advances made by end of 2018, with the purpose of analysing the need for furthered actions on the monitoring and evaluation on the outlined actions.

4.3.8. Automated Tackling of Disinformation (Ref. No 16)

Reference title: Alaphilippe et al. 2019. Automated tackling of disinformation Major challenges ahead

Key words: *disinformation, deepfakes, fact-checking, regulation, malinformation, misinformation, social media manipulation, media platforms, online advertising, computer algorithms*

This study discusses the phenomena of mis-, mal- and disinformation and how social media platforms, search engines, online advertising and computer algorithms enable and facilitate the creation and spread of online misinformation.

[83] COM/2018/022 final - on the Digital Education Action Plan

In terms of methodology, the study presents the current understanding of why people believe in false narratives, what triggers their sharing, and how they impact offline behaviour (e.g. voting). This is complemented by a brief overview of self-regulation, co-regulation, and classic regulatory responses, as currently adopted by social platforms and EU countries. The study includes a roadmap of initiatives from key stakeholders in Europe and three case studies on the utility of automated technology in detecting, analysing, and containing online disinformation. The study concludes with the provision of policy options.

The study points out that 8 EU countries (AT, CZ, DE, HU, IT, NL, PL and the UK) have been affected by disinformation[84], where the actors involved in social media manipulation vary from country to country and include government organisations, parties and politicians, and private contractors. The most widely used social media manipulation strategies use fake accounts and bots, primarily to carry out attacks on the opposition, post distracting messages, or engage in trolling and harassment. This is achieved not only through posting replies or comments, but also through the creation of new content such as fake videos, blogs, memes, or websites. In addition, the study refers to a Eurobarometer, 2018 survey findings that 83 % of the questioned 26 000 EU citizens from 28 EU member states consider online disinformation a "threat" to democracy. Furthermore, the study explains the different terms related to "information disorder" – disinformation, misinformation and malinformation and highlights some propaganda techniques[85] employed in making online disinformation more credible.

The study examines some of the techniques used to create and spread online disinformation, such as using designated websites for creation of fake news; creating fake profiles and groups in Facebook, Twitter, and Instagram; using less popular platform to create the news and then spread the most read ones on bigger platforms; online advertising and clickbait; microtargeting and third-party data analysis of user data. It looks into online news consumption habits, confirmation bias and polarisation techniques, in an attempt to explain why people fall for online misinformation, what motivates them to share it, and what is the impact of online misinformation on their offline behaviour (e.g. does it affect their voting in elections). These key questions, however, need further research. In addition, the study explains the fake amplifiers associated with social bots, political bots, trolls, cyborgs, fake followers, fake comments etc, as well the 'deepfakes', generated through deep neural network models (AI), which could pose significant legal and ethical concerns, including lack of consent and private-only use. The study mentions some tools and techniques that platforms and journalists use to identify deepfakes (e.g. Gfycat GIF-hosting platform uses facial recognition and AI-based video matching). The majority of academic research is focused on methods for macro-level analysis. Broadly speaking, we can identify three classes of approaches. The first set of approaches focused on investigating the role of echo chambers - questioning the influence of social media platforms and online news sites and their influence in creating partisanship echo chambers. The second strand of research focused on detecting fake amplifiers of false narratives. The role of automated or semi-automated accounts (bots) in amplifying false narratives has been demonstrated especially during the US elections and the Brexit referendum. The third strand of work is on combining content analysis with network analysis through the use of semantic tools

[84] According to Bradshaw & Howard, 2018 study

[85] Deceitful propaganda techniques (e.g., selective use of facts, unfair persuasion, appeal to fear), however, are employed much more widely, e.g. in anti-EU campaigns, post-truth politics, ideology-driven web sites (e.g., misogynistic or Islamophobic), and hyper partisan media, often with the intent to deepen social division, increase polarisation, influence public opinion, or impact key political outcomes.

and machine learning (Conroy, Rubin & Chen, 2015), which highlighted the necessity to have a combined machine/human approach and to fuse different techniques to assess veracity of information.

A number of automated fact-checking tools are being developed in response by fact-checking organisations and start-up companies, e.g. FullFact, Duke University's Reporters Lab, Factmata, Chequado, ContentCheck. The aim is to assist the human fact-checkers in tasks, such as automatic detection of factual claims made by politicians and other prominent figures in TV transcripts and online news.

The study goes further to analyse the possible legal responses to the phenomenon of disinformation, and groups them into self-regulation, co-regulation (which approach is undertaken by the Commission, Belgium and Denmark), and classic regulation (like in Germany, France and the UK).

In conclusion, the study provides projects and initiatives roadmap, aiming to provide an overview of what is going on in the Member States and in the EU institutions, bodies, offices and agencies with regard to disinformation tools and studies that are being developed and conducted.

As next steps, there are some policy options examined, such as (1) enabling research and innovation on technological response; (2) improving the legal framework for transparency and accountability of platforms and political actors for content shared online (which includes setting up a transnational regulation with a strong focus on privacy and user-centric moderation and fiduciary responsibilities of social platforms); (3) strengthening media and improving journalism and political campaigning standards; (4) supporting interdisciplinary approaches and investing in platforms for independent evidence-based research, promoting media literacy for citizens and empowering civil society to multiply efforts.

4.3.9. A multi-dimensional approach to disinformation (Ref. no. 17)

Reference title: High Level Group on Fake News and Online Disinformation. 2018. A multi-dimensional approach to disinformation

Key words: *disinformation; fake news*

The Report describes a wide array of material that will help to put forward a number of policy initiatives to better address the risks posed by disinformation spread online.

The Report aims to define the scope of the phenomenon, identify the roles and responsibilities of relevant stakeholders, and formulate recommendations.

In terms of methodology, the Report puts forward possible options to counter disinformation spread online and to help develop a comprehensive EU strategy for tackling disinformation. It gives a definition of the phenomenon, identifies measures already taken by various stakeholders and establish key principles and general objectives for the short and long term.

The Report discusses that disinformation as a phenomenon that goes well beyond the term 'fake news'. Disinformation as defined in this Report includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. Problems of

disinformation are intertwined with the development of digital media and can be handled most effectively, and in manner that is fully compliant with freedom of expression, free press and pluralism, only if all major stakeholders collaborate. The multi-dimensional approach recommended by the HLEG is based on a number of interconnected and mutually reinforcing responses. These responses rest on five pillars. The first pillar is designed to enhance transparency of online news, involving an adequate and privacy-compliant sharing of data about the systems that enable their circulation online. The second pillar promotes media and information literacy to counter disinformation and help users navigate the digital media environment. The third pillar develops tools for empowering users and journalists to tackle disinformation and foster a positive engagement with fast-evolving information technologies. The fourth pillar is designed to safeguard the diversity and sustainability of the European news media ecosystem. The last pillar promotes continued research on the impact of disinformation in Europe to evaluate the measures taken by different actors and constantly adjust the necessary responses

In conclusion the HLEG calls on the EC to consider, in its upcoming Communication on "fake news" and online disinformation, a multi-dimensional approach based on the five pillars and consisting of concrete, inter-dependent actions. For the short to medium term, the HLEG suggests, as a first step, a self-regulatory approach based on a clearly defined multi-stakeholder engagement process, framed within a binding roadmap for implementation, and focused on a set of specific actions. As a second step, the EC is invited to re-examine the matter in Spring 2019 and decide, on the basis of an intermediate and independent evaluation of the effectiveness and efficiency of these measures, whether further actions should be considered for the next EC term.

As a way forward, the report is just the beginning of the process and will feed the EC reflection on a response to disinformation. The challenge will lie in delivering concrete options that will safeguard EU values and benefit every European citizen.

4.3.10. Fake News em ano eleitoral Portugal em linha com a UE (Fake news in election year in Portugal in line with EU)[86] (Ref. no. 23)

Reference title: OberCom. 2019. Fake news in election year in Portugal in line with EU

Key words: *elections, fake news, disinformation, media literacy, collaborative journalism, fact-checking*, hate speech, *Artificial Intelligence, machine learning techniques*

The report discusses the impact of fake news on elections throughout social media and explains what the European Union (EU) and Portugal approaches, initiatives and projects are on tackling disinformation in election context, with especial focus on the 2019 European Parliamentary elections and Portuguese regional, national and European elections.

[86] Contractors' translation

In terms of methodology, the report makes reference to various studies, reports and other documents and its divided in three main chapters: 1) overview of European Union (EU) and Portugal positions and approaches against fake news; 2) addresses the impact and different tactics of disinformation in electoral online campaigning (more focused in Portuguese case) and elaborates on three initiatives to mitigate such phenomena; 3) this chapter is dedicated to data analysis of Portuguese news consumptions' behaviour problematising on fake news.

The report presents in a first chapter, an overview of European Union (EU) and Portugal approaches against disinformation tactics.

At EU level, it highlights the creation of the East StratCom Task force, in 2015, in response to Russian based online interference. It also refer to the presentation of a European Strategy against disinformation, in 2018, that resulted in several initiatives such the incentive to fact-checking projects and media literacy; promoting synergies such the creation of SOMA Disinformation Observatory; accountability of online platforms with the adoption of the "Code of Conduct against disinformation"; reinforced the importance of data protection rules and adoption of the "Action Plan against disinformation" focusing on the 2019 European Parliamentary elections.

Regarding Portugal, the report considers that national initiatives on the topic are more reactive and enforcing EU positions. However, it describes important national initiatives such as the "Poligrafo", first Portuguese website exclusively for fact-checking with collaboration with an important TV channel for its divulgation to population. Another initiative referred is the "StopProgagHate"[87], a project that aim at using a tool using Artificial Intelligence (AI) and based on machine learning techniques, to fight online hate speech. "Monitorização de propaganda e desinformação nas redes sociais"[88] – project that aimed at identifying disinformation campaigning with political purposes on 2019 national elections.

On a second chapter, the report highlights initiatives to be continued in order to tackle the impact of disinformation namely fact-checking organisations work, more investment in media literacy and in collaborative journalism.

In conclusion, based on analysis of different studies, reports and other documents, this report validates its premise that disinformation phenomena is a reality in the Portuguese context, and it is in line with EU and is sufficiently relevant to influence public opinion and potentially weaken quality of democracy.

4.3.11. Trends in Online Foreign Influence Effort (Ref. no. 27)

Reference title: Martin, Shapiro. 2019. Trends in Online Foreign Influence Effort

Key words: *disinformation, elections, foreign influence efforts (FIE), social media*

[87] http://stop-propaghate.inesctec.pt/
[88] Monitoring disinformation propaganda on social netwok – contractos' translation

The Report describes a new database of 53 foreign influence efforts (FIE) targeting 24 different countries from 2013 through 2018.

The Report aims to compile a list of distinct FIEs. This by summarizing evidence regarding trends in these operations, providing baseline information about a wide range of FIEs, and offer high-level context for the growing literature about disinformation campaigns.

In terms of methodology, they draw data on more than 460 media reports to identify FIEs, track their progress, and classify their features.

The Report discusses that new platforms create novel opportunities for a wide range of political actors. In particular, foreign actors have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation.

FIEs are defined as coordinated campaigns by one state to impact one or more specific aspects of politics in an-other state; through media channels, including social media; and by producing content designed to appear indigenous to the target state

The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization.

To be included in the database, an influence effort must involve an action by one state against another in the media; an identifiable political goal; and producing content that is meant to appear as being produced organically in the target state.

The most commonly used strategy is defamation, defined as attempts to harm the reputation of people or institutions, which is used in 65% of FIEs. Persuasion, which we define as trying to move the average citizen to one side of an issue, is used in 55% of FIEs. Only 15% of FIEs used polarization - defined as trying to move opinion to the extremes on one or more issues. These findings contradict the idea that FIEs most often work to polarize public opinion. Twitter has been the most commonly used platform (83%), followed by news outlets (66%), and Facebook (50%).

In conclusion, FIEs have targeted countries around the world since 2014. While Russia has been the most active user of this new form of statecraft, other countries are following. Iran and China have deployed similar tactics beyond their own borders and even democratic states such as Mexico have adapted these techniques for internal purposes.

As a way forward, the underlying data and the Report will be updated regularly.

4.3.12. Online Disinformation and Political Discourse - Applying a Human Rights Framework (Ref. no. 29)

Reference title: Chatham House. 2019. Online Disinformation and Political Discourse - Applying a Human Rights Framework

Key words: *online disinformation, political discourse, human rights*

This paper discusses online disinformation, the response of the US, the EU and some member states to the phenomenon and the application of a human rights framework to it.

In terms of methodology, the article clarifies core terms and concepts such as digital platforms, disinformation, personal data, elections and political discourse. It provides an overview of cyber activities that may influence voters with specific examples from different countries. It this context, it summarises a range of responses to the issue in different countries (the UK, the US, Germany, France, Singapore), the EU and initiatives of the digital platforms like Facebook, Twitter and Verizon Media in the form of rules and standards. The article also discusses relevant human rights law and the implications of online disinformation on it.

In particular, the paper clarifies the cyber activities that may influence voters – creation, distribution and maximisation of the influence of disinformation and divisive content. It specifies that content may be **created** by use of words, pictures and videos, memes, curation of untrue, deliberately misleading, or exaggerated material (including hate speech and divisive speech), 'trolling' of people or issues, use of 'deep fakes', impersonation of news websites, the use of fake websites and fake identities and presentation of a political campaign as a 'war'. Methods for **distribution** of disinformation and decisive content include distribution through adverts, posts of targeted political messages, as well as likes, shares, retweets, etc., understanding of how best to exploit the digital platforms' algorithms for promotion of content, '*content laundering'* (encouraging others to innocently like, share, retweet, etc.), '*astroturfing*' (development of an appearance of grassroots support by using multiple posts or using bots, fake accounts, or closed peer-to-peer distribution networks such as WhatsApp and Facebook Messenger, apart from the open social media sites Facebook and Instagram. Specific example is given how Facebook influenced political sentiment all over the world, including with mistrust of information during elections in India, and paid Russian disinformation campaigns with anti-EU biased articles during Brexit referendum. The same took place with WhatsApp channels which are widely used in India, Malaysia and Brazil for political news and led to WhatsApp reducing in 2019 the number of contacts/groups to whom a message could be forwarded in one action to 5 globally. Maximisation of the influence of disinformation is based on using personal data to perform micro-targeting. Data harvesting is strongly observed in the United Kingdom.

The article goes farther to provide an overview of the response to these cyber activities in the US, and in the EU, by adopting the eCommerce Directive and the obligation for EU member states to exempt digital platforms from liability for the content provided on their services, on condition that, if aware of illegal content, they will remove it or disable access to it expeditiously. Some member states like Germany, France and the UK implemented additional laws in this regard. Regarding hate speech the European Commission agreed a Code on Countering Illegal Hate Speech Online in 2016. In 2018, High Level Expert Group on Fake News and Online Disinformation was set up, and a joint Action Plan against Disinformation was adopted. Furthermore, the digital platforms like Facebook, Twitter and Verizon Media undertook some initiatives and adopted standards to monitor content with a view to removal, suppression and/or de-prioritisation of certain material. However, under domestic law, these standards seem to be more restrictive of expression than human rights law. The author therefore argue that it should be allowed to smaller platforms to adopt their own standards under domestic law even more restrictive than human rights law entails. On the other hand, this should not apply to the biggest platforms like Facebook, Google and Twitter, because their accessibility has as major impact on public conversation.

Finally, the paper looks into five human rights: the right to freedom of thought; the right to hold opinions without interference; the right to privacy; the right to freedom of expression (online); and the right to participate in public affairs and vote. It explains their content, challenges and potential breaches by use of algorithms.

In conclusion and as a way forward, the author recommends that states, digital platforms and other actors undertake specific steps to tackle the impact of online disinformation on these 5 rights. These include among others, further studying of this impact; elaboration of guidelines; introducing more transparency in collection, use, sales and purchase of personal data; promotion of digital literacy and free journalism campaigns; setting up independent regulatory bodies and scrutiny mechanisms; establishing frameworks by digital platforms that enable efficient, fair, context-specific decision-making, that reflects the standards of human rights law; implementation of measures to tackle hate speech, bots and trolls, algorithms that prioritise disinformation, and micro-targeting for the purpose of manipulating voter behaviour; requiring transparency of political adverts; tackling overseas interference; enforcing limits on campaign spending and rules on political communications, and ensuring equal treatment of candidates.

4.3.13. The spreading of disinformation through internet services and the regulation of political advertisements (Ref. no. 31)

Reference title: Appelman et al. 2019. The spreading of disinformation through internet services and the regulation of political advertisements

Key words: *disinformation, political advertisements, internet services, microtargeting*

This report describes what the regulatory framework for the dissemination of political advertisements via internet services is, and what the possibilities are with regard to regulation (transparency in particular) in the light of the applicable normative frameworks and the country studies.

The report aims to respond to the calls to regulate online political advertisements and disinformation.

In terms of methodology, this report is based on judicial research to answer the question on how to regulate online political advertisements and the dissemination of disinformation. In the Annex, an overview is given of the regulations of paid political advertising in six countries (UK, France, Germany, Sweden, US and Canada).

The report discusses that the changed media landscape created the opportunity to disseminate disinformation on a large scale and with a major impact on local democratic processes. This was caused by a relatively small group of internationally operating internet services. In response, both at European and national level, several initiatives have been launched to regulate the dissemination of disinformation via these internet services. In Chapter 2 the definition of 'disinformation' will be analysed. Chapter 3 will give an overview of the relevant internet services which are involved in the spreading of disinformation. Chapter 4 discusses the constitutional standards in the Netherlands and the EU. Chapter 5 focuses on the EU legislate framework in detail and Chapter 6 the legislative framework in the Netherlands. In Chapter 7, the insights offered by the analysis of the problem and the legal framework carried out are listed and brought together.

In conclusion, after analysing of existing laws and regulations regarding paid political ads, including through the country studies, seven policy options, ranging from disclaimer rules to a total ban on paid political ads, were provided. The first policy option provided is transparency rules aimed at the person who paid for an advertisement. The second option is transparency rules focused on personal data that is used when targeting an advertisement. The third option is transparency rules aimed at archiving political advertisements. The fourth option is rules on the obligation to report expenditure on online campaigns. The fifth option is campaign financing rules that prohibit foreign election advertising expenses. The sixth option is a ban on paid political advertisements during the elections. The seventh option is banning paid political advertisements during and outside election time

4.3.14. Report on the implementation of the Action Plan Against Disinformation (Ref. no. 36)

Reference title: European Commission. 2019. Report on the implementation of the Action Plan Against Disinformation

Key words: *disinformation*

The Report describes in more detail how the Action Plan and the Elections Package helped to fight disinformation in the context of the European elections.

The Report aims to have a coordinated approach to tackle disinformation.

In terms of methodology, the report provides a first assessment of the progress achieved and sets out the main lessons for the future.

The Report discusses that all relevant actors, including EU institutions, Member States, industry and civil society play their respective role along four strands of action:

Improving capabilities and strengthening coordinated responses through the Rapid Alert System. It facilitated daily exchanges and sharing of information on a number of cases and trends related to disinformation between EU authorities and Member States.

Implementation of the Code of Practice on Disinformation by the main platforms, including Facebook, Google, Twitter, along with software companies and bodies representing the advertising industry. In doing so, they voluntarily committed to improve the transparency, accountability and trustworthiness of their services and stepped up in the fight against disinformation.

Awareness raising and improving societal resilience can be done by empowering citizens and civil society and ensuring fact-based communication on the EU. Ahead of the European elections, the EU institutions have worked closely in the following areas: a) raising awareness of disinformation, b) better communication on EU policies, c) boosting the EU capacity to react to disinformation, d) Strengthening societal resilience through media literacy, e) empowering civil society.

Protecting the integrity of elections and increase societal resilience, in particular with EC's Election Package. The actions helped achieve concrete results in the following areas: a) improved coordination of election authorities b) better protection against cyber threats, c) misuse of personal data; d) boosting transparency.

In conclusion, the coordinated EU approach helped to ensure stronger preparedness and coordination in the fight against disinformation. The preliminary analysis shows that it contributed to expose disinformation attempts and to preserve the integrity of the elections.

As a way forward, disinformation is an evolving threat that requires continuous research to update the policy toolbox in line with new trends and practices. The rise of targeted disinformation campaigns will remain a major challenge for the future and calls for joint action by EU institutions and Member States to counter the threat. The EEAS, EC and MS, will further strengthen cooperation within the Rapid Alert System, including developing a common methodology for analysis and exposure of disinformation campaigns and stronger partnerships with international partners, such as G7 and the North Atlantic Treaty Organization. The EC will report in 2019 on the implementation of the Election Package and assess the effectiveness of the Code of Practice. On this basis further actions may be considered to ensure and improve our long-term response to the threat.

4.3.15. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election (Ref. no. 44)

Reference title: Ferrera. 2017. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election

Key words: *elections, disinformation campaign, social bot, online social media, MacronLeaks, machine learning, cognitive behavioural modelling techniques*

This paper aims to analyse forms of social media manipulation, especially disinformation and social bot operations in the run up to the 2017 French presidential elections, focusing on the *MacronLeaks* disinformation campaign.

In terms of methodology, approximately 17 million posts on Twitter between 27 April and election day – 07 of May 2017 were collected. By means of machine learning and cognitive behavioural modelling techniques, two groups of humans and social bots[89] were created being their activities analysed both independently and in interaction. Further characterisation was made to bots and users who engaged with those groups and oppose to those bots and user who did not engaged with them.

[89] An effective bot detection algorithm was created using user metadata and activity features, some with binary fields such availability of geo-coordinates, or "verified" as gives the indicator that the account belongs to a human.

The paper explains in first place the background story of the case of MacronLeaks a disinformation campaigning that culminated in a publication of incriminating material on Wikileaks, even though with the disclaimer of "unverified authenticity".

In the context of this study, disinformation is defined as "exhibiting two necessary ingredients namely, first, the "unverified nature" (which traditionally is called a "rumour") of the shared information, and second the coordinated effort behind its sharing". Regarding the first, it ended up in an investigation of several weeks concluding that there was no evidence to support such allegations. On the other hand, the second element was confirmed as the voluntary spreading of the rumour started with efforts from 4chan.org platform and included the presence of social bot operation during election day amplifying the dissemination of such disinformation.

After an exhaustive explanation of methodology and methods used, the paper characterises MacronLeaks' bots, which based on authors' classification model represent 18% of roughly 100.000 users involved in this disinformation campaign. Despite recent literature examines that automated activities of social bots are considerably easy to detect due to its high and incessant volume of posts, re-tweets, etc. in the case here in analysis, **social bots' activities** presented a rather similar activity to human users with lower volume of tweets generated. On this evidence, the author suggests that this social bots' "under the radar" activity could represent a new "strategy to avoid detection and suspicion form the platform**".**

Finally, by means of new technologies such machine learning, is possible to conclude that users who engaged with MacronLeaks disinformation campaigning were mainly foreigners with propensity to engage with alt-right matters, rather than "French users with diverse political views" and actually the ones eligible to vote. To reach this conclusion, the profile of users engaging with MacronLeaks and those not involved in such disinformation campaign were examined and most words present in the profiles of the first, were from English speaking American such MAGA (Make America Great Again).

In conclusion, the paper revalidated results from previous academic contributions sustaining the existence of a "black market of reusable political disinformation bots", yet the study goes further on this argument and add the new discovery of identifying bots already present during 2016 US presidential election campaign and supporting alt-right positions, but inactive since then. Secondly, the paper also concludes that regarding audience of MacronLeaks campaign, it was mainly composed by "English-speaking American alt-right community, rather than French users", potential voters, which also explains the limited success of this disinformation campaign.

As next steps, the author will concentrate the analysis of computational political propaganda phenomena in different types of elections aiming to understand how online social media might be manipulated and in case of success of such attempts, will also try to examine quantifiable consequences.

4.3.16. Foreign influence operations in the EU (Ref. no. 58)

Reference title: Bentzen. 2018. Foreign influence operations in the EU

Key words: *foreign influence, disinformation*

The briefing examines foreign influence by different actors and the techniques they used in the past.

The briefing aims to map different techniques that were used by foreign actors and how to tackle it.

In terms of methodology, the paper gives an overview of cases and lessons learned.

The paper discusses in four parts foreign influence operations in the EU. The first part, "Projecting power: the soft and the sharp approach" describes the success of soft power as opposed to military power, focuses on communication via public diplomacy. Having had limited success with their soft power efforts, both Russia and China, recognise the potential for reaching their goals by making democracy, human rights and fundamental freedoms appear less attractive through sharp power. This can be seen as 'forced attraction' based on coercion, as opposed to soft power, which is based on attraction and persuasion. Sharp influence efforts for undermining are not new, but the information disruption toolbox, which includes a number of often overlapping covert and some overt instruments, keeps growing.

The second part: "Active measures then and now: the case of the Kremlin" describes that Russia started with its disinformation campaign in influence operations during the Soviet era. Some of the tools they used were: active measures, disinformation, agents of influence, reflexive control, forgeries, propaganda and controlled international front groups. While narratives may differ from country to country, analysts agree that Moscow seeks to undermine unity, destabilise democracies and erode trust in democratic institutions. Moscow's influence operations are often outsourced to an 'adhocracy' of oligarchs, trolls, criminal networks and hackers to minimise or delay the risk of exposing the involvement of the Kremlin.

The third part: "European response to disinformation campaigns" describes that striking a balance between countering online disinformation to defend democracy while at the same time protecting freedom of expression appears to be the key challenge facing the EU. A number of EU Member States have responded to recent disruptions in the information sphere by updating and/or increasing their counter-disinformation efforts. The debate on legislative responses in MS reflects the ethical dilemma of protecting the information ecosystem without compromising fundamental rights.

The last part: "Focus on evolving tools and actors" discusses that new artificial intelligence-driven techniques such as deep fakes are on the rise. At the same time, existing tools are (re-)activated. Turkey has repeatedly mobilised its diaspora for political gains. Russia has long used ethnic Russians abroad as an influence tool and a pretext for military action. China has expanded its global information strategy, by increasing its efforts to influence political and economic elites, media, public opinion, civil society and academia in liberal democracies.

In conclusion, with an increasing number of state and non-state actors attempting to impact and/or undermine decision-making in the EU, paired with the rapid evolution of means and methods, a growing number of MS, sectors and policy areas will likely be affected by these developments.

As a way forward, a multifaceted response is needed to the challenges of foreign disinformation and these evolving foreign influence operations call for a broader European and interdisciplinary approach.

4.3.17. The digital transformation of news media and the rise of disinformation and fake news (Ref. no. 62)

Reference title: Martens et al. 2018. The digital transformation of news media and the rise of disinformation and fake news: An economic perspective

Key words: *disinformation, fake news*

The paper examines the digital transformation of news markets and the impact on the quality of news. It also compares various definitions of fake news and looks into consumer trust and quality perceptions of various sources of news.

The paper aims to give an overview of the relevant economic research literature with regard the digital transformation of news markets and the impact on the quality of news.

In terms of methodology, both literature reviews and survey data are carried out.

The paper, discusses in seven chapters:

Chapter 2 in the report presents a brief overview of a variety of definitions of fake news, ranging from various forms of disinformation and, more generally, quality variations in news. a narrow definition based on verifiably false news to a broader definition that encompasses

Chapter 3 presents some recent empirical evidence, mostly from survey data, on consumer perceptions of the quality of news. Traditional print and broadcasted news remain the most trusted sources. Despite the much wider availability and accessibility of online news, user trust in online sources of news, is lower and differs considerably by age, education and country.

Chapter 4 explores how digitization has transformed the news media landscape and affected production, advertising, distribution and quality of news. It has transformed the traditional business model into a multi-sided market or platform with at least three interacting sides: news publishers, readers and advertisers. This has shifted market power and revenue streams from news publishers to platform operators who have the data to match readers, articles and ads in a more efficient way, compared to offline newspapers that could only do bulk targeting of a bundle of articles and ads on a wider audience.

Chapter 5 presents some empirical studies on the role of social media networks in the propagation of news, on the reach and consumption of false news articles and on the impact of false news on political choices.

Chapter 6 explores possible causes of market failures in online news markets that would require regulatory intervention in order to restore social welfare.

Chapter 7 explores possible private sector and public policy responses to online news quality concerns.

In conclusion, platform operators are best placed to take corrective measures. Fact-checking is a good tool to identify false news but its effectiveness to reduce propagation may be limited. Strengthening media literacy may help consumers to better assess the quality of news articles but also shifts the burden

of quality control from distributors to consumers. There is a long history of government interventions in news markets through competition policy tools, state aid and regulation. Most of the potential quality problems in online news markets seem to be associated with distribution and advertising mechanisms, not with a lack of quality news producers.

As a way forward, the subject is entirely new for researchers and probably still has a long way to go in order to get better insights in the phenomenon of fake news.

4.3.18. Disinformation and Propaganda - Impact on the Functioning of the Rule of Law in the EU and its Member States (Ref. no. 68)

Reference title: Bayer et al. 2019. Disinformation and Propaganda - Impact on the Functioning of the Rule of Law in the EU and its Member States

Key words: *disinformation, propaganda, social media, E-Commerce Directive, ePrivacy Regulation*

The study assesses the impact of disinformation and strategic political propaganda disseminated through online social media sites and examines effects on the functioning of the rule of law, democracy and fundamental rights in the EU and its Member States.

The aim of the Study is, to formulate recommendations on how to tackle this threat to human rights, democracy and the rule of law and specifically addresses the role of social media platform providers in this regard.

The Study analyses how new technology has transformed the operation and structure of the democratic public sphere in general, and in particular explores the recently experienced events of disinformation and propaganda campaigns in the light of interference with democratic processes through the manipulation of public opinion, as well as the international and national legislative and self-regulatory initiatives

The Study explores the legal framework of social media platforms, including their place and assumed responsibility in the legal order, among various information-society service providers. It is found that social media service, which emerged after 2000, is not defined and its liability is not set out consistently by the relevant legal instruments. These include the E-Commerce Directive, the Audiovisual Media Services (AVMS) Directive, the ePrivacy Directive and the proposed ePrivacy Regulation, the Code of Conduct on countering illegal hate speech, the Commission Recommendation on measures to effectively tackle illegal content online, the Communication from the Commission on tackling online disinformation, the European Council decision of March 2018 and the Proposal for a Regulation on preventing the dissemination of terrorist content online. Based on these documents, the study uses the term 'platform providers' to designate those services that facilitate, organise and amplify the transmission of third-party content, through actions of their registered users. While platforms are ubiquitous also in other business sectors, social media is a subcategory of theirs. In accordance with many leading international actors, including the UN, Organisation for Security and Co-operation in Europe (OSCE) and Council of Europe, this study represents the position that platforms should not be made liable for third-party content.

In conclusion, disinformation and propaganda are symptoms of deeper structural problems in our societies and media environments. Rather than targeting the content itself, the vulnerabilities that these narratives exploit should be identified and addressed. The recommendations are divided into two sections: strengthening democratic resilience and adapting media policy. The first section includes imminent actions relating to the coming EP elections, regulation of political and public issue advertising, data protection, civic education, mainstreaming science in policy-making and further research. The second section includes strengthening pillars of trust in the media and the obligations of platform providers.

As a way forward, all recommendations are directed towards one common objective: to safeguard democracy, the rule of law and respect for human rights. This should provide the basis for the competences of EU legislation. Given the cross-border dimension of the problems addressed, the recommended measures need to be adopted at the EU level in order to achieve the objectives.

4.3.19. Open data analysis - European Parliamentary Elections: Comprehensive Report (Ref. no. 83)

Reference title: Rapid Response Mechanism Canada (RRM Canada). 2019. Open data analysis – European Parliamentary Elections: Comprehensive Report

Key words: *European elections, foreign interference, divisive narratives, narratives competition*, *manipulating Search Engine Optimization, de-contextualisation*

The repot analyses foreign interference on run-up 2019 European Union Parliamentary elections (EU elections) and outlines important findings on used tactics.

The report main objectives are: identify efforts of artificial amplification of false information that might influence legitimacy and fairness; find main issues which are considered highly divisive and intentionally exploited during EU elections and using examples from UK, Italy and Ireland, with the aim of identifying cross-border narratives susceptible of being used in different contexts and, finally, find relevant tactics used by foreign actors with harmful purpose.

The report suggests an important discovery regarding the transition from an information warfare to narrative competition[90], where divisive narratives spread are immigration or Muslims in Europe, which weaken social cohesion, amongst others. In continuation, the report presents two examples of such phenomena. The first example is related to Migration/Immigration and is based on official news on New York Post regarding a high number of migrants occupying French

[90] RRM Canada reports' definition: "Competition for the way an issue is framed within public discourse, with each framing looking to become the dominant method of conceptualizing said issue, is referred to as "narrative competition".

airport[91]. This event and news content was posted by national and transnational alternative and Kremlin-affiliated news sites and blogs, then shared and reproduced divisive content which later suspicious sites by means of manipulating Search Engine Optimization[92] artificially amplified such content just days before 2019 European elections, via networks of unreliable websites and unauthentic Twitter and Reddit accounts. In addition, this scalation and dissemination of information playing on anti-immigrant and making use of inflammatory language, frequently referred and linked to the original content giving the impression of validation of the content. The second example is related to health and reproductive issues and occurred in Ireland, where national and international non-state actors used factual information from public Health Service of Ireland which was then manipulated into divisive narrative about abortion. Such information by means of coordinated activity was disseminated and target vulnerable audience at local and international level.

The report main findings: no relevant evidence of foreign interference has been identified neither by state-based nor by non-state actors within the cases studied**.** Similar tactics used by Internet Research Agency[93] (IRA) in 2016 US presidential elections were identified in national and transnational actors**.** The report also identified disinformation or "de-contextualisation" tactic, which consists on the use of authentic and factual information intentionally "manipulated and distorted by means of misrepresenting its context or content". As the report states, these tactics allow the creation and dissemination of divisive narratives which weaken trust in democratic institutions and affect social cohesion stability.

Another finding from report is that main untruth and divisive content issue-related that was strategically disseminated can be comprised in the following topics: "immigration/migration, antireligious sentiment (Muslim and Jewish), nationalist identity, women's health, gender-based harassment and climate-change". This was also verifiable either by national or international non-state actors.

In conclusion, the report verified that in the contest of EU elections there was no relevant state-based foreign interference observed, thought indicated that digital systems contain ideal conditions for exploitation by foreign malign actors.

4.3.20. Progress Report - November 2019 (Ref. no. 86)

Reference title: Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation. 2019. Progress Report - November 2019

[91] https://nypost.com/2019/05/19/footage-shows-hundreds-of-migrants-occupying-french-airport-terminal/

[92] RRM Canada reports' definition: Search engine optimization is the process of affecting the online visibility of a website or a web page in a web search engine's unpaid result. It is a measurable, repeatable process that is used to send signals to search engines that a webpage is worth showing in Google's index. Though this process should occur organically by users visiting a website, this can be manipulated by multiple tactics to give an inauthentic SEO score thus artificially amplifying content

[93] Russian "troll farm" identified as having performed coordinated efforts to manipulate 2016 US presidential elections - https://www.ft.com/content/55a39e92-8357-11ea-b872-8db45d5f6714

Key words: *disinformation, cyber-security, cyber-attacks, political advertising, transparency of online political advertising*

This report presents a first assessment of the progress reached on the seven recommendations of the first Interdepartmental Group (IDG) Report, since its publication in July 2018. IDG has been stablished by the Irish government after observing issues arising from recent experiences in other democratic countries regarding to the use, and misuse, of social media by external, anonymous or hidden third parties.

In terms of methodology, the report lists all seven recommendations progress and next steps planned to each recommendation.

The report details the developments made on the seven recommendations derived from the first report. These seven recommendations aim to form the basis for a multi-faceted, whole of government approach to safeguarding of the electoral process from disinformation and security risks.

The seven recommendations indicated in the first and in this second progress report are: expedite the establishment of an Electoral Commission as outlined in the Programme for Partnership Government; advance the modernisation of the voter registration process; regulate transparency of online political advertising; reform of legislative provisions concerning the funding of election and referendum campaigns; support the EU Commission's work in tackling online disinformation; continue to advance national level media literacy initiatives and enhance cyber security measures around the electoral process including the possibility of the National Cyber Security Centre (NCSC) providing advice to political parties.

Moreover, the report acknowledges that while Google, Facebook and Twitter have made important efforts to support the integrity of elections by the provision of publicly available advertising libraries. However, much more is required to facilitate effective media monitoring of digital political advertising and campaigning.

In conclusion, the report proves that risks to the electoral process in Ireland are relatively low but that the spread of disinformation online and the risk of cyber-attacks on the electoral system pose more substantial risks. Moreover, the report outlines a proposal for regulating transparency of online political advertising, at national and at international level (EU).

4.3.21. First Annual Self-Assessment Reports on the Code of Practice on Disinformation (Ref. no. 96)

Reference title: European Commission. 2019. First Annual Self-Assessment Reports on the Code of Practice on Disinformation

Key words: *Code of Practice on Disinformation*

This document presents an overview of the first annual reports on the Code of Practice on Disinformation, submitted by its signatories Google, Facebook, Twitter, Microsoft and Mozilla and the trade association detailing policies, processes and actions undertaken to implement their respective commitments under the Code.

In terms of methodology, the document provides information on how the Code signatories implemented its five pillars, namely:

Pillar 1: Scrutiny of ad placements; Pillar 2: Transparency of political and issue-based advertising; Pillar 3: Integrity of services against inauthentic accounts and behaviours, Pillar 4: Empowerment of consumers; Pillar 5: Empowerment of the research community

In particular, the document points out the specific actions that the Code signatories undertook within each of these pillars according to their reports. For instance, in pillar 2, political and issue-based advertising, Facebook launched its political ads transparency tools globally in March 2019. These tools aim at clearly identifying the ad funding source, as political ads on Facebook and Instagram must be clearly labelled with a "Paid for by" disclaimer. Facebook's identity confirmation and authorisation system aims at preventing abuse and foreign interference. However, this system raised some complaints by European-wide political organisations ahead of the EU elections, because it seems that Facebook's definition of political ads is wider than those of the other platforms. It covers ads made by, on behalf of or about a current or former candidate, a political party, action committee or advocates for the outcome of an election to public office; ads about any election, referendum or ballot initiative, including "get out the vote" or election. In addition, Facebook has an Ad library, where it stores all ads, including non-political ones, and one can perform a customised search throughout them. Similar approach on the ad policy[94] has been undertaken by Google. Twitter applies its global policy on political content. This global policy permits political ads in all countries but Cyprus, France, Hungary, Latvia, Lithuania and Portugal. Twitter's political ads policy for the EU elections includes a certification process, which requires that political advertisers be established in the EU in order to place political ads in any EU Member State. The objective is to ensure that only EU-based individuals can advertise political campaign content.

In addition, as regards to pillar 5 Empowerment of the research community, in September 2019, Facebook created a Deepfake Detection Challenge with the aim of producing technology to better detect when artificial intelligence has been used to alter a video and mislead viewers. Google reported on its partnership with the International Fact-Checking Network (IFCN), which has focused on training more fact-checkers.

In conclusion, the document points out the positive actions of the Code signatories in all the 5 pillars**,** such as efforts to disrupt advertising and monetisation incentive that contribute to the dissemination of online disinformation in the EU; deployment of policies and systems to ensure transparency around political advertising; provision of tools that enable consumers to understand why they are seeing advertisements; supporting media literacy skills, putting in place policies and tools intended to provide researchers and the fact-checking community with access to platform data.

However, the document also highlights the areas of improvement, such as deployment of concrete actions to improve transparency in the online advertising ecosystem; more harmonised approach in scoping the definition of political ads; correct labelling of all the political ads served on the platforms during the elections, to increase the reliability of the political ads archives as well as the reporting provided on amounts spent on political advertising; provision of more granular information to better assess malicious behaviour specifically targeting the EU and the progress achieved by the platforms to counter such behaviour; developing and implementing trustworthiness indicators in collaboration with the news ecosystem; more detailed reporting to assess the relevance and

[94] https://support.google.com/adspolicy/answer/6014595?hl=en&ref_topic=1626336

impact of the consumer; making consumer empowerment tools available in all EU Member States; provision of data and search tools to the research community in a less episodic and arbitrary manner to respond to the full range of research needs.

4.3.22. Tackling COVID-19 disinformation - Getting the facts right (JOIN (2020) 8 final) (Ref. no. 102)

Reference title: European Commission. 2020. Tackling COVID-19 disinformation - Getting the facts right

Key words: *COVID-19, disinformation*

The Communication focuses on the immediate response to disinformation around the coronavirus pandemic, looking at the steps already taken and concrete actions to follow, which can be quickly set in motion based on existing resources.

The aim of the Communication is to increase the knowledge, as knowledge gaps have proven to be an ideal breeding ground for false or misleading narratives to spread.

The Communication discusses that the COVID-19 'infodemic' has demanded a rapid response from the EU and its Member States. Disinformation can have severe consequences: it can lead people to ignore official health advice and engage in risky behaviour, or have a negative impact on our democratic institutions, societies, as well as on our economic and financial situation. The crisis has opened the door to new risks, for citizens to be exploited or be victims of criminal practices in addition to targeted disinformation campaigns by foreign and domestic actors seeking to undermine our democracies and the credibility of the EU and of national or regional authorities. Combatting the flow of disinformation, misinformation and foreign influence operations, including through proactive and positive communication, calls for action through the EU's existing tools, as well as with Member States' competent authorities, civil society, social media platforms and international cooperation, enhancing citizens' resilience. This work must be done in full respect of freedom of expression and other fundamental rights and democratic values.

Since the beginning of the COVID-19 crisis, clear and accessible communication and accurate information have been central to protecting citizens' health. Aside national information channels, the EU has played a role in this through its institutions, multipliers and networks in the Member States, in its neighbourhood and beyond. The work has included effective pro-active communication efforts to promote verifiably reliable health information, inform citizens and third-country partners about the EU's activities to tackle the crisis, as well as to raise awareness of the risks of disinformation. In March 2020, the Commission launched a specific webpage addressing false claims related to COVID-19, promoting content that is authoritative and helping separating facts from fiction, for example to counter narratives about the lack of solidarity in the EU.

As a way forward, the Commission and the High Representative will quickly set in motion the actions proposed in the Communication, building the ground for a longer-term approach as part of the European Democracy Action Plan, which should be presented towards the end of 2020, as well as of the forthcoming Digital Services Act.

In conclusion, the EU acted to respond to the threat posed by disinformation, misinformation and foreign influence operations in the COVID-19 crisis. However, the scale of the potential impact on the health of citizens and the stability of our societies, and the gaps it has revealed, call for continued efforts to step up this work. The COVID-19 crisis has become a test case showing how the EU and its democratic societies deal with this challenge. Based on the challenges identified, lessons learned so far and the proposed short-term solutions, EU society and its democratic oversight could in the longer-term become stronger and more resilient and better prepared for the challenges of the future.

4.3.23. Disinformation as a Global Problem – Regional Perspectives (Ref. no. 106)

Reference title: Lim. Disinformation as a Global Problem – Regional Perspectives. 2020

Key words: *Disinformation*

The study focuses on disinformation in the European Union (EU) and Southeast Asia (SEA).

The aim of the study is to examine the characterisation and context of disinformation, provide an overview of its creators and its circulation, and round up with a discussion on foreseeable trends.

The methodology used was open-sourced research, and published frameworks were used to discuss the findings. This approach allowed broad observations to surface and provides an initial understanding of how disinformation is present in the EU and SEA and the conditions that enable it.

The study discusses that in the aftermath of suspected electoral interference in the 2016 US presidential elections and in several European elections in 2016 and 2017, much has been written about disinformation, its definitions, history, manifestations outside of elections and motivations.

Generally, the assessed intent is to undermine confidence in legitimate institutions and democratic processes and deepen societal fault lines through entrenching views/beliefs and subverting a society's values. A range of tactics is used. They include creating and capitalising on areas of vulnerability and instability, exploiting political differences and normalising debate on sensitive national issues that have had long-standing scientific consensus. Disinformation has been used somewhat interchangeably with information manipulation, information disruption and fake news.

At the heart of disinformation is falsification and obfuscation. To prevent attribution and for plausible deniability, perpetuators hide behind covers, i.e. false identities, false personas or intermediaries. Nevertheless, these actors can be categorised.

There is a need for multi-faceted solutions to the many dimensions of the problem and a need to scope the issue to better identify the stakeholders involved and the processes required to respond at the structural, societal and governmental levels.

In conclusion and as a way forward the study makes a note of an increasing sophistication in disinformation and sharp power tools will be abled by advances in technology, most notably AI. Also, a key development to watch is the possible bifurcation of the internet in the next decade, one led by the US and the other by China. Disinformation and the use of sharp power is ultimately a national security problem. Any assessment of disinformation and sharp power must be taken and assessed together with developments in other domains. The authors finally expect a stronger, collective responses from governments and civil society to disinformation and sharp power.

4.3.24. Assessment of the Implementation of the EU Code of Practice on Disinformation (Ref. no. 109)

Reference title: European Regulators Group for Audiovisual Media Services. 2019. Assessment of the Implementation of the EU Code of Practice on Disinformation

Key words: *Code of Practice on Disinformation, social media platforms, measures, disinformation, self-regulation*

The report analyses the standard terms of service and the specific policies and tools adopted by the online platforms to implement the commitments of the Code in the first year of implementation of the Code (October 2018 to October 2019).

The report aims to support the European Commission's evaluation of the Code of Practice's effectiveness.

The report discusses that there is a consensus among stakeholders that the Code of Practice is needed. Since disinformation continues to be a widespread problem, the Code, its aims and activities are considered to be highly relevant.

Furthermore, stakeholders consulted for the study also agreed that disinformation is a topic where the EU has an added value and where it should continue to lead and coordinate action. Despite differences in stakeholder views with regards to the effectiveness of self-regulation, there is widespread acknowledgement that the Commission is right in pursuing a dialogue with the social media platforms. There is also acknowledgement that the Code constitutes a first and crucial step in the global fight against disinformation. In this sense, the Code shows European leadership on an issue that is international in nature.

The study identifies a range of achievements. Firstly, the Code has established a common framework under which to agree on and implement activities to tackle disinformation. In doing this, the Code has set a foundation on which further activities can be built

Secondly, the discussions facilitated by the work of the Code have also contributed towards a specific set of actions and measures at EU and national levels and it has improved cooperation between policymakers and the Signatories to combat disinformation:

For instance, the Code has established a platform for negotiation that has produced concrete results in the form of regular monitoring of Signatory activities and continuous action to combat disinformation activities. In addition, the Code has also led to increased reflection among Member States with regards to activities to understand and combat disinformation.

The main criticism of the Code relates to its self-regulatory nature, lack of uniformity of implementation – evidenced by the unevenness of progress made under the specific Pillar – monitoring, and lack of clarity around its scope and some of the key concepts.

First, it is a voluntary document, and as such there are no means to enforce the commitments of the Signatories nor do the 13 signatories cover all relevant stakeholders.

Second, the study shows that there remains a need for a common understanding of key concepts. To combat this lack of clarity and foster a harmonised approach, it is important that the action that are agreed upon are as concrete as possible to facilitate the definition of intended results and key performance indicators and support implementation and monitoring.

In conclusion, the Code remains relevant, it has led to positive results, and it provides value added at a European level.

As a way forward the effectiveness of the Code can be strengthened with (i) continued efforts to debate the Code's strengths and weaknesses with the Signatories, non-Signatories and wider stakeholders; (ii) a mechanism for action in case of non-compliance of the Code's Pillars; (iii) further support to evaluation and monitoring of the Code and (iii) strengthening the practical implementation of the current requirements of the Code, which entails that signatories should implement activities to the same standard across Member States.

4.3.25. The effects of campaigns on participation in political decision-making (Ref. no. 116)

Reference title: European Economic and Social Committee. 2020. The effects of campaigns on participation in political decision-making

Key words: *disinformation, campaigning, decision-making, social media, media literacy, media freedom and pluralism, political advertising*

This exploratory opinion was requested by the Croatian presidency to the European Economic and Social Committee (EESC) and **presents** a set of recommendations such as the improvement of self-regulation in the field of online disinformation.

The opinion describes first the opportunities to enhance Europeans' informed participation in elections by means of a more effective public information campaigns or by increasing investment in media freedom and plurality and in journalism, where EU should continue to encourage self-regulatory measures and bodies such as ethical codes and press councils with the aims to reinforce high standards of journalism, including in digital and social media.

The opinion also refers to the need to respond to opportunities and challenges posed by digital and social media. It is a fact that digital and social media facilitated the access to a greater range of information and views, which are more rapidly available and enables citizens to participate more easily in the democratic debate. However, there is a greater concentration of ownership among social media platforms than among the traditional print and broadcast media which commercially-driven secret algorithms serve to significantly filter the information available user's accounts. Moreover, the arrival of social media has led to a creation and dissemination of disinformation (e.g. by means of fake accounts) that might influence voters' behaviour. Regarding the Code of Practice to tackle online disinformation and signed by online platforms, the opinion addresses the conclusions of the first annual self-assessment report and report by the European Regulators Group for Audiovisual Media Services (ERGA)on Code of practice implementation. The findings indicate that not all of the political ads available in the archives of the ad libraries were correctly labelled as political advertising nor disclose enough data to ensure greater transparency of political campaigning and advertising, including its financing sources and linkages to special interest groups. Additionally, no common standards have been adopted by the signatories of the code to allow researchers and journalists to access personal data while respecting users' right to privacy and consent.

The EECS opinion also indicates the need of improving Europeans' media literacy and civic education where media literacy for all generations in society, as well as training by and for journalists should be strongly promoted and financially supported by the EU across the EU Member States and in a regular basis.

Encouraging European political parties to be citizen-oriented and accountable is also addressed by the EESC as an important contributing factor for integration within the Union. In this context, further regulatory action should take into account the current policy debate and policy proposals, including a range of policy ideas on developing European parties so that they are closer and more accountable to the European public, for example through declarations by national parties of their intended European party affiliation, transparent fundraising and campaigning and accountability for political content that blatantly undermines EU common values.

In conclusion, the opinion presents several recommendations with impact on a broad funding on education on EU values, institutional affairs and citizenship as main catalyst to European democracy such as the development of a European Democracy Action Plan that strive for more initiatives "to achieve free and plural media and quality independent journalism" or the creation of an High-Level Expert Group on "Teaching Europe" which could for example provide policy proposals and recommendations for discussion by education ministers, which could lead to Council conclusions.

4.3.26. Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives (Ref. no. 118)

Reference title: Joint Research Centre. 2020. Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives

Key words: *disinformation, hostile narratives, disinformation campaigns, Italy, France, Spain, case studies*

This report analyses how disinformation campaigns have evolved into more complex hostile narratives.

In terms of methodology Italy, France, and Spain were taken as case studies to prove what has been observed and determined from analytical and numerical research.

The paper discusses that during the last years, malicious actors have been able to rely on much more sophisticated and organized disinformation campaigns in an attempt to manipulate citizens' perceptions. Technological advances have provided producers and sharer of distorted information with new powerful means to reach an ever-wider audience. One of the reasons this system of propaganda and disinformation is so effective and successful is that it deceives ordinary citizens into sharing false stories within their own circle of friends and acquaintances, while platforms' algorithms have the capacity to pick these messages up very quickly and amplify it on an unprecedented scale. Most of this content is not designed to channel people into a particular direction, but to create confusion and erode the trust in our media, institutions and eventually, democracy itself. Hostile narratives target feelings and emotions and touch upon specific social vulnerabilities. They are made of true and false information, where the narration of facts counts more than the facts themselves. They rely on negatively charged emotions, like fear or anger, in order to lower the means of rational self-defence and trigger self-survival instincts, creating a psychological condition that makes the brain respond positively rather than negatively to bigoted statements and divisive rhetoric. It should be said that public figures and the media in recent years have played a key role in disseminating false and unsupported information. There has been a dramatic rise in the number and type of news programs available, including a troubling number of partisan programs that often feature false or exaggerated information.

In the last decades, foreign interference has been pushed by the belief that by breaking the Euro-Atlantic link, the West would end as a strategic entity. Russian military interventions in Georgia in 2008 and in Crimea in 2014, China's Massive Belt and Road Initiative in Eurasia and the mosaic of sovereigntist and populist parties that have revamped anti-Americanism and anti-globalism, combined with sudden asymmetric cyberwarfare, can describe the most formidable and dangerous challenge that democracies are facing since the fall of the Berlin Wall.

This report highlights how hostile narratives target citizens' vulnerabilities exploiting fear mongering using algorithmic content curation. It also includes case studies that will describe how different disinformation campaigns have been used in Italy, France and Spain. It provides examples on how hostile disinformation narratives were employed in France and Italy.

In conclusion, it is wrong to assume that disinformation is only the fault of 'modern' technologies, like algorithms. Online social networks and platforms indeed amplify, sometimes distort, a polarization that already exists in society. A definitive solution to hostile narrative is complex and there is no silver bullet for this problem.

As a way forward, a multi-sector approach is needed, from regulating data collection and micro-targeting, reduce amplification of misinformation content, to dealing with citizens radicalised by a prolonged exposure to hostile narratives. To reduce the impact of disinformation and misinformation on our society, a more complex and heuristic approach, which involves tech players, media, public institutions, and political actors, is essential.

4.3.27. Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda (Ref. no. 119)

Reference title: Joint Research Centre. 2019. Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda

Key words: *disinformation, data-driven, propaganda*

The report analyses citizens' vulnerabilities to disinformation and hostile narratives, taking the 2018 Italian General Election as a case study.

The report discusses that disinformation strategies have evolved from "hack and dump" cyber-attacks, and randomly sharing conspiracy or made-up stories, into a more complex ecosystem where narratives are used to feed people with emotionally charged true and false information, ready to be "weaponised" when necessary. Manipulated information, using a mix of emotionality and rationality, has recently become so pervasive and powerful to the extent of rewriting reality, where the narration of facts (true, partial or false) counts more than the facts themselves. Every day, an incredible amount of information is constantly produced on the web. Its diffusion is driven by algorithms, originally conceived for the commercial market, and then maliciously exploited for manipulative purposes and to build consensus.

The report argues that today's society vulnerability to disinformation operations is not only the result of the threats posed by hostile actors or psychometric profiling - which can be seen as both exploiters and facilitators - but essentially due to the effect of three different factors: (1) Information overload; (2) Distorted public perceptions produced by online platforms algorithms built for viral advertising and user engagement; and (3) The complex iteration of fast technology development, globalisation, and postcolonialism, which have rapidly changed the rules-based international order.

As a way forward, building up on the existing initiatives taken by the European institutions and member states against disinformation, a set of three mutually reinforcing policy options is proposed, addressing: monitoring hostile narratives, regulating 'Personalisation Algorithms', and authenticating cryptographic content.

In conclusion, in rapidly and dynamically evolving environments increasing citizens' resilience against malicious attacks is, ultimately, of paramount importance to protect our open democratic societies, social values and individual rights and freedoms.

4.3.28. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement" (Ref. no. 128)

Reference title: European Commission. 2020. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement

Key words: *disinformation, Code of Practice*

The document sets out the key findings of the EC services' assessment of the implementation and effectiveness of the Code of Practice on Disinformation during its initial 12-months period of operation.

The document aims to provide an overview and an assessment of the implementation and effectiveness of the commitments subscribed to by the signatories of the Code.

The document discusses that that the Code has proven a very valuable instrument and has provided a framework for a structured dialogue between relevant stakeholders to ensure greater transparency and accountability of platforms' policies on disinformation. It has also prompted concrete actions and policy changes by relevant stakeholders aimed at countering disinformation.

In general, the signatories have put in place policies aimed at: reducing opportunities for advertising placements and economic incentives for actors that disseminate disinformation online; enhancing transparency of political advertising, by labelling political ads and providing searchable repositories of such ads; taking action against and disclosing information about malicious actors' use of manipulative techniques on platform services, to artificially boost the dissemination of information online and enable certain false narratives to become viral; setting up technological features that give prominence to trustworthy information, so that users have more instruments and tools to critically assess content they access online, and engaging in collaborative activities with fact-checkers and the research community, including media literacy initiatives.

In order to ensure a complete and consistent application across stakeholders and MS, the Code should be further improved in several areas by providing commonly-shared definitions, clearer procedures, more precise and more comprehensive commitments, as well as transparent KPIs and appropriate monitoring. Participation should be broadened to include other relevant stakeholders, in particular from the advertising sector.

In conclusion, the lack of access to data allowing for an independent evaluation of emerging trends and threats posed by online disinformation, as well as the absence of meaningful KPIs, are fundamental shortcomings of the current Code. The EC and public authorities are still relying on the willingness of platforms to share information and data. Therefore, a more structured model for cooperation between platforms and the research community should be developed.

A structured monitoring programme may constitute a pragmatic way to mobilise the platforms and secure their accountability. The programme for monitoring disinformation around COVID-19 will be an opportunity to verify the adequacy of such an approach and prepare the ground for further reflection on the best way forward in the fight against disinformation.

As a way forward, the information and findings will support the EC's reflections on policy initiatives, including the European Democracy Action Plan (EDAP), as well as the Digital Services Act, which will aim to fix overarching rules applicable to all information society services.

4.3.29. Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity (Ref. no. 133)

Reference title: Garnett, James. 2020. Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity

Key words: *integrity, trust, disinformation, equality, electoral law, cyber elections*

The report analyses the opportunities for state actors to incorporate technology into the electoral process to make democratic goals more realisable. It also poses major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals such as political equality and popular control of government.

The study aims to argue that this new era of technologies requires proactive interventions into electoral law and the rewriting of international standards to keep pace with societal and technological change.

As a methodology, the authors used recent reports (from 2016 till 2019) of the use and mis-use of technologies during elections in the USA and Europe.

The report discusses the new era of cyber elections. New technologies have always been integrated in people's daily life, so also into the elections cycle. The elections cycle is way more than just the election day itself, also includes all sorts of organisational and preparatory tasks where the newest technologies are used.

The era of cyber elections is marked by five core characteristics: (a) the new ontological existence of the digital, (b) new flows of data and communication, (c) the rapid acceleration of pace in communications, (d) the commodification of electoral data, and (e) an expansion of actors involved in elections.

Electoral integrity is evaluated based on key factors of democracy. The key factor of democracy is that it is ruled by the people, with voting right for domestic people, as well as for the people living overseas. There are three principles that are necessary for democracy, and all three could be affected by the deployment of technology. These principles are: (1) opportunities for deliberation, (2) Equality of participation in elections, and (3) electoral management delivery.

Deliberative opportunities. Citizens need full opportunities to formulate their preferences. Now a days the social media have broaden up the possibilities for deliberation and debate. The downside is that it also made it easier to advertise online disinformation and hate speech, as well as to make use of microtargeting techniques. There are also less financial borders which increases inequality between the candidates.

Equality of participation. Political equality is central to the practice of elections. Already on the process of registering for elections an equal treatment of citizens is important. Some political parties don't see a benefit in facilitating registering and voting in some regions where they expect no big support for their party. Online registration can improve the voters' turnout in more remote regions. As a matter of securing the identity, some countries make us of biometric data, such as a fingerprint, to assist in confirming the identity of a voter. On the other hand, some voters start to distrust the electoral system if more technologies are involved, certainly when speaking of internet voting.

Electoral management delivery and provision of robust laws. Technology can help in making the elections more transparent and give more trust in for example the transport of votes from polling stations to counting station. The trust was increase especially when the automatic counting was used in parallel to manual counting. The use of machines and technologies also results in fewer human errors in the process.

The main question is what laws should be adopted to respond to these technological changes. For this to answer it is important to get answers to some sub questions such as: What technology can be used for what specific process? Who owns the technology and the resulting data? What procedures are in place if technology breaks or is faulty? Additionally, the challenge is to identify laws that can protect democratic space, while also protecting freedom of speech.

In conclusion, electoral integrity now must include the cyber-sphere, specifically how it impacts opportunities for deliberation, the quality of participation, and the professionalism and transparency of electoral management. It may require the revisiting of international standards and handbooks.

Elections are entering a new digital era in which there are new opportunities and threats for the conduct and contestation of elections. Although many of these are not entirely new, perhaps being a continuation of older problems.

As a way forward, the article argues that elections are essential to democratic rule. However, the evaluations of electoral integrity require a new focus in the cyber era, with its expansion of actors, transition, and challenges in running elections. It is argued that interventions to electoral law and new international standards are needed to confront these challenges and safeguard the integrity of elections.

4.3.30. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains" (Ref. no. 136)

Reference title: Huckle, White. 2017. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains

Key words: *Fake News, blockchain, big data, Ethereum, hash functions, cryptography, public-key cryptography, digital signatures, Preservation Metadata*

The document introduces a prototype of an innovative technology for proving the origins of captured digital media.

The document aims to introduce a blockchain-based distributed application, Provenator (intended as the agent noun of the verb form of provenance, which means establishing the origin of something), a tool that helps prove the originator of media sources.

The document discusses that in an era of fake news, when someone shows us a video or picture of some event, how can we trust its authenticity? It seems the public no longer believe that traditional media is a reliable reference of fact, perhaps due, in part, to the onset of many diverse sources of conflicting information, via social media. Indeed, the issue of 'fake' reached a crescendo during the 2016 US Presidential Election, when the winner, Donald Trump, claimed that the New York Times was trying to discredit him by pushing disinformation.

Current research into overcoming the problem of fake news does not focus on establishing the ownership of media resources used in such stories - the blockchain-based application introduced in this article is technology that is capable of indicating the authenticity of digital media. Put simply; by using the trust mechanisms of blockchain technology, the tool can show, beyond doubt, the provenance of any source of digital media, including images used out of context in attempts to mislead. Although the application is an early prototype and its capability to find fake resources is somewhat limited, they outline future improvements that would overcome such limitations. Furthermore, they believe that the application (and its use of blockchain technology and standardised metadata), introduces a novel approach to overcoming falsities in news reporting and the provenance of media resources used therein.

In conclusion, the application has the potential to be able to verify the originality of media resources, the authors believe that technology is only capable of providing a partial solution to fake news. That is because it is incapable of proving the authenticity of a news story as a whole. The authors believe that takes human skills.

As a way forward, the authors have reservations about the possible limitations of technology in combating fake news, they believe the trust mechanisms of blockchains make them better positioned than other technologies for proving the authenticity of media resources. Indeed, organisations are investigating using blockchains for purposes such as transparency and publicly auditable content ranking.

4.3.31. Disinformation and Digital Media as a Challenge for Democracy (Ref. no. 155)

Reference title: Terzis et al. 2020. Disinformation and Digital Media as a Challenge for Democracy

Key words: *disinformation, fake news*

The book discusses diverse academic and professional comments from all over the world, touching upon topics that range from the theoretical approaches to and the conceptualisation of disinformation, to the experiences of dealing with disinformation, to the solutions for dealing with disinformation and their critique.

The book aims through a collection of expert analyses, to deepen the understanding of the dangers of fake news and disinformation, while also charting well-informed and realistic ways ahead.

The book is motivated by some recent troubling developments in public discourse, namely the developments in information, misinformation and disinformation practices. From the beginning of history, various and diverse means or channels of communication have been used to inform, misinform (unintentionally) and disinform (deliberately). However, in recent decades, the emergence and development of new information and communications technologies (ICT), combined with the ever-increasing digitalisation and globalisation of almost every aspect of modern life, among others, have opened up new and uncharted avenues to that end. This book therefore focuses on disinformation practices occurring with the help of digital media as these practices bring to the fore profound negative ramifications for the functioning of a democratic polity.

In conclusion and as a way forward, it is not too late to find public policy solutions which can restore information technologies to their original role of facilitators of democracy rather than their undertakers. But the timeframe is closing, and these solutions are needed sooner rather than later.

4.3.32. Balancing Act Countering Digital Disinformation While Respecting Freedom of Expression (Ref. no. 156)

Reference title: Broadband Commission for Sustainable Development. 2020. Balancing Act Countering Digital Disinformation While Respecting Freedom of Expression

Key words: online disinformation, disinformation responses, freedom of expression, disinformation techniques.

The targeted analyses and recommendations address the life cycle of online disinformation: from production to transmission, reception and reproduction.

They are aimed at different audiences such as legislators and policy makers (counter disinformation campaigns, electoral-specific responses, the Freedom of Expression Assessment Framework); Internet companies, producers and distributors (content curation, technical and algorithmic, advertisement policy, demonetisation responses); Journalists, investigative researchers and fact checkers; Universities and applied and empirical researchers; Target audiences (educational, ethical and normative, empowerment and credibility labelling responses).

In terms of methodology, the findings are organised into a typology of 11 different categories of responses to disinformation – ranging from identification and investigatory responses, through to policy and legislative measures, technological steps, and educational approaches. For each category of response, the

analysis provides a description of work being done around the world, by which actors, how it is funded and who or what is targeted. The report further analyses the underlying assumptions and theories of change behind these responses, while weighing up the challenges and opportunities. Each category of response is also assessed in terms of its intersections with the universal human right of freedom of expression, with a particular focus on press freedom and access to information. Finally, case studies of responses to COVID-19 disinformation are presented within each category.

In particular, the report provides a 23-step tool developed to assess disinformation responses, including their impact on freedom of expression. It also produces a framework for capturing the complete disinformation life cycle - from instigation and creation, to the means of propagation, to real-life impact, with reference to 1. Instigators 2. Agents 3. Messages 4. Intermediaries and 5. Targets/Interpreters. It then assesses the 11 response types under four categories – (i) Identification responses (Monitoring and fact-checking and investigative); (ii) Responses aimed at producers and distributors through altering the environment that governs and shapes their behaviour (legislative, pre-legislative and policy responses, national and international counter disinformation campaigns and electoral responses); (iii) Responses aimed at production and distribution mechanisms (curatorial responses, technical and algorithmic responses and demonetisation responses); and (iv) Responses aimed at the target audiences of disinformation campaigns (normative and ethical, educational and empowerment and credibility labelling responses). These responses to disinformation are shown to often be complementary to each other. However, sometimes one type of response may work against the other. For instance, when internet communications companies do not remove disinformation-laden attacks on journalists on the grounds of 'free speech', they may undermine press freedom and journalism safety, and work against the role of independent journalism as a counter to disinformation. For each response a definition is provided, it is explained who and what is targeted, who they try to help, who funds them across different countries, how they are evaluated, what are the specific challenges and opportunities they present and what are the recommendations put forward.

In conclusion, the report points out that disinformation cannot be addressed in the absence of freedom of expression concerns, and it explains why actions to combat disinformation should support, and not violate, this right. It also underlines that access to reliable and trustworthy information, such as that produced by critical independent journalism, is a counter to disinformation.

As next steps, the report puts forward a number of important cross-cutting recommendations for action but also recommendations addressed towards each group of stakeholders. Among others, it recommends encouraging global multi-stakeholder cooperation, donor investments in countermeasures to disinformation, promotion of privacy-preserving equitable access to key data, investments in independent research. In addition to that, intergovernmental and other international organisations could increase technical assistance to Member States to develop regulatory frameworks to address disinformation in line with freedom of expression. They could also collaborate with states and NGOs towards media literacy campaigns and training. Individual states could review and adapt their responses to disinformation using the 23-step framework for assessing law and policy. They could also increase transparency and proactive disclosure of official information and data. Recommendations are also provided for electoral regulatory bodies, national authorities, political parties, law enforcement agencies and the judiciary, Internet communications companies, the media sector, civil society and researchers.

4.3.33. The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms (Ref. no. 198)

Reference title: Persily. Kofi Annan Foundation. 2019. *The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms-annotated*

Key words: *Remote electronic voting, internet, review, state-of-the-art. Disinformation, hate-speech*

The report elaborated on the concern that that the most democratic features of the internet are, in fact, endangering democracy itself. This paper lists the main dangers, how to best counter them and who should do the counter measures.

The study aims to identify and frame the challenges to electoral integrity arising from the global spread of digital technologies and social media platforms, and to inspire for the development of policy measures that address these challenges.

As a methodology, this study unites the most distinguished leaders from the tech sector, academics and of political life to answer one simple question: How can we mitigate the risks of the digital age to our elections while harnessing the opportunities and ultimately strengthen democracy worldwide.

The report discusses the issues and challenges of the new technologies related to the elections. Critics however point out that new media merely serve as a mirror reflecting the social ills of the time, but not necessarily creating them. The problems allegedly created by the internet well precede its development. Polarization has deep roots and has been growing for some time. "Fake news" is as old as news, and hate speech is as old as speech.

The unique dangers of the new digital communication revolution fall into several categories: Velocity (an increase in speed of online communication); Virality (the kinds of speech, strategies, and candidacies most likely to succeed in a regime are those that appeal to emotion, especially to outrage); Anonymity (it can gives rise to a range of unaccountable anti-democratic speech); Homophily (people live in some kind of filter bubbles, and information cocoons); Monopoly (there is an unprecedented power of the new big tech companies. Their rules for speech and the decision-rules embedded in the algorithms for search and newsfeed are, in many respects, more important than formal law for governing the information ecosystem.); and Sovereignty (the World Wide Web enables foreign entities to propagandise well beyond their borders with great ease).

As a combating agent, For the most part, the sources of reform are governments regulation, the platforms self-regulation, or civil society. Most reforms, however, do come with costs to speech, given that the alleged dangers come in the form of online communication and association. These reforms fall into several categories: deletion, demotion, disclosure, delay, dilution and diversion, deterrence, and digital literacy.

In conclusion, with those caveats in mind, though, the new forms of communication enabled by the internet have specific, democracy-endangering effects. The tasks of this Commission are to identify and tackle those challenges, while recognising the benefits of internet freedom, and proposing reforms that minimise the costs to such freedom.

As a way forward, the problems and solution technologies of today are not necessarily going to be the ones most important in the near future. The next generation of online challenges to democracy is quickly coming into view. The list of expected challenges would include: encrypted peer-to-peer platforms; deepfakes; home assistants, wearables, and the internet of things; professionalisation of election interference.

4.4. Campaigning

4.4.1. Study on the use of Internet in political campaigns (Ref. no. 06)

Reference title: Committee of experts on media pluralism and transparency of media ownership. 2018. Internet and electoral campaigns - Study on the use of internet in electoral campaigns

Key words: *political campaign, Internet, political advertising, new digital techniques*

This study analyses the key concepts of fair, clean and clear elections and explains the context and evolution of internet advertising for political objectives.

In terms of methodology, the study begins with an introduction on the potential benefits and issues that may arise out of the use of Internet for political campaign. It then explains how political campaigns are regulated, what are the objectives, standards, principles and broadcasting regulations they should abide by. Furthermore, the study shows how political campaigning activities have changed in the recent years in terms of spending, usage of Internet sources, in addition to broadcasting, and deployment of new digital techniques, which could be associated with certain problems. In conclusion, the authors come up with a list of recommendations to existing policies of Member States on the organisation and regulation of elections.

The study provides an overview of the broadcasting/mass media regulation of political campaigning in the EU to highlight that this is heavily regulated everywhere in the EU, unlike online campaigning. It warns that new internet technologies pose challenges for established institutions and principles of regulation of election communications such as freedom of association, spending limits, and regulation of political advertising. The fact that new intermediaries and platforms now occupy important gatekeeper positions, once occupied by journalists, but have not adopted the ethical obligations of the media, represents a threat to elections and potential for corrupt practices to emerge.

In particular, the study's findings show that in recent years political parties have significantly shifted their campaign spending from broadcasting channels to digital channels. The study examines some of the new digital marketing techniques and their application in politics, in particular, "push vs pull advertising" and "message targeting". The study points out that push advertising involves agency from the user and is primarily associated with search engines and ads triggered after the user searches for a product or service. On the other hand, pull advertising involves less agency from the user and ads are displayed to them unsolicited, while the user carries out regular activities online. The study explains that with the increasing sharing of data across platforms, the lines between

push and pull advertising are blurred. For example, Facebook ads can be targeted not just according to data volunteered and in circulation in the Facebook ecosystem but also based on users' browsing history on other websites. Similarly, an advertiser (a political party for example) can upload lists of their users into Facebook and use the platform to advertise to them and similar users. Search advertising can also take advantage of data from users who have performed an action away from the search engine results page, for example a user who has visited a website and did not purchase or sign up can be 'remarketed' to. In addition, the study finds that political parties have shifted from methods targeting large audiences to using more precise tools and sophisticated data-mining techniques to target smaller groups of individuals. Although for political parties, message targeting may optimise electoral campaigns' resources, it hides certain threats, specifically because it is aimed primarily at swing or undecided voters, therefore the rest of the public is deprived of information and this creates inequality and reduced choice.

Furthermore, new digital techniques may pose a number of problems. For instance, online media may undermine the applicable rules on electoral campaigning, especially broadcast advertising, since large groups of peoples switch easily from TV to Internet channels. Also, digital technologies may lead to transparency issues - gaps in the amount of digital spending and how it is reported. Political parties may start campaigning on wedge issues, such as immigration and welfare, which are highly divisive in a public forum, but are able to mobilise voters. Other problems include political redlining – bypassing certain groups of individuals from the messaged targeting, disinformation issues, privacy and data protection issues, difficulties to track the sources of campaign financing, specifically when it includes online donations and crowdfunding. Last but not least, issues may occur with intermediaries being able to facilitate political parties to disseminate or impede information, if their business/ideological interests align.

In conclusion and as next steps the study recommends that 1) national data protection bodies should scrutinise the use of personal data for message targeting services; 2) intermediaries should develop codes of conduct that make explicit their respect for fundamental rights and strategies for their effective enforcement; 3) national governments should adopt rules on online electoral campaigning and increase transparency and monitoring of digital spending; 5) self-regulatory bodies should be encouraged to collaborate with online intermediaries to prevent deliberate mis- and disinformation and check facts independently from the state.

4.4.2. Social media and election campaigning (Ref. no. 59)

Reference title: Davies. 2014. Social media and election campaigning

Key words: *elections, election campaigning; social media, microtargeting*

The briefing examines how social media can provide a way of increasing citizen involvement in political life, especially during election campaigns.

The briefing aims to give an overview on how social is used by politicians, especially during campaigns.

In terms of methodology, cases, studies and expert's views are used to give an overview of how social media is used by politicians and what the effect can be.

The paper discusses that social media can be used in election campaigns in various ways. Firstly, in political communication, the internet and social media have become important alternative sources of political and campaign information. More than half of European internet users now think social networking services (SNS) are a good way of keeping up to date on, or having a say in, political affairs. Social media allow candidates to communicate directly with citizens, keeping control of the content, distribution and timing of their messages, as well as reducing their dependence on traditional intermediaries such as journalists. User-generated content supporting a party or candidate is another way to bypass traditional mass media. Social media can also serve as an indirect influence on the stories that mass media present and provide a way for politicians to monitor what is happening in the public sphere during an election campaign.

The second way is in campaign organisation. Social media can be used as a means to direct political messages to certain target groups and assist with much more refined targeting of voter groups. Voter data (partly collected via social media) can be used to 'micro-target' messages sent to particular groups of users during the campaign. One of the main changes in campaigning with the advent of the Internet has been the use of social media's online capabilities to communicate and organise events that take place 'offline', i.e. in the real world.

The third way is that social media can cause multiplier effects. Perhaps the most important aspect of social media is the 'network' effect produced when someone who has seen a video, visited a page or read a tweet passes on the same message or a reference to all of their friends or followers. These 'second degree' networks (i.e. followers of followers) may represent weak social ties but can be very large. The extreme case of this network effect is that of a campaign item which 'goes viral'.

The last way is the effectiveness of social media, the fundamental question in the EU context is whether social media are effective in mobilising those who are engaged online to become engaged 'offline' (i.e. in the real world) and thereby to reduce democratic deficits.

In conclusion, the influence of social media use in elections may be different in countries with different size populations and with different political and electoral systems. Nevertheless, even motivating a small percentage of the population can (at least in some electoral systems) make a considerable difference to the result of a party or an individual candidate. Certainly, an upward trend in citizen participation in EU elections due to any media, social or not, would be taken by many as a good sign.

As a way forward, it will take some time, and further elections, before a clearer picture emerges.

4.4.3. Technology and social polarisation (Ref. no. 60)

Reference title: Boucher. 2019. Technology and social polarisation

Key words: *technology, social polarisation*

The briefing examines two studies**,** one study approached the question with reference to trends in the production and consumption of news media, while the other focused on trends in political campaigning and communication strategies.

The briefing aims to give policy options to tackle social polarisation.

In terms of methodology, two studies are briefly explained and at the end a set of policy options are giving.

The paper discusses two studies. The first study focuses on European news media and polarisation. This study considers the effects of technology on news production and consumption across Europe and their potential to lead to more polarised societies. One of the key messages is how little we understand about the mechanisms that link news production and social polarisation, because evidence is patchy, and findings are not always transferable between European countries. The internet has created more consumer choice, to the point where most people select their own news sources based on their ideologies and preferences. For Europeans, their position on the left-right political spectrum is the strongest predictor of news choices, although their level of populism can also play a strong role. An important demographic is identified in users that rely heavily on social media for their news, raising concern about 'filter bubble' effects, where users' information exposure is limited to a narrow field of perspectives that align with their pre-existing views. The authors highlight that individuals' basic interest in politics and the news might be a more important factor than the ideologies that drive their choices, as the high-choice media environment means that some users may opt-out of news consumption entirely. Such news aversion could be a worrying trend if healthy democracies rely upon citizens understanding their political system.

The second study discusses political campaigns and polarisation. This study considers polarisation in the context of political campaigns and communications. It highlights a trend towards more emotionally charged content – particularly negative material that provokes fear, hatred or disgust – in political communications. Emotion has always been part of the political strategist's toolkit but is particularly effective in the context of social media campaigns where they tend to generate more clicks, more data and more revenue. In other cases, polarisation has been the deliberate aim of manipulative political campaigns by hostile foreign and domestic political actors. These make use of a range of strategies including automated bots and 'dark ads' to amplify disagreement, provoke hostility between different groups and despite these worrying developments, these technical and social trends might also have some positive effects. First, some degree of polarisation can be healthy for political systems, encouraging wider democratic participation and deeper democratic engagement. Second, social media can help bring large numbers of people together around socio-political movements.

In conclusion, both studies present policy options that could help to foster healthier digital environments and mitigate trends towards social polarisation. In total there are five policy option which target: 1) citizens' news consumption; 2) digital divides; 3) political communications; 4) news producers and major platforms; 5) governance institutions.

4.4.4. Polarisation and the use of technology in political campaigns and communication (Ref. no. 61)

Reference title: Neudert, Marchal. 2019. Polarisation and the use of technology in political campaigns and communication

Key words: *elections, political campaigns, polarisation, algorithms, big data, artificial intelligence (AI), deepfakes*

The study examines how digital technologies can be mobilised by political actors, campaigns and movements to motivate action or influence political opinion.

The study aims to formulate principles and policy options for fostering a better relationship between digital technology and public life.

In terms of methodology, an in-depth analysis of the technological affordances that enhance and undermine political decision-making, both now and in the future was carried out.

The study discusses the relationship between digital technology and polarisation in contemporary Europe. It does so by first reviewing two core mechanisms through which social media could be polarising European publics: inadvertently, through design choices and incentives that potentially narrow the diversity of information accessed by individuals while facilitating the dissemination of divisive and emotionally-charged content; and deliberately, through the exploitation of loopholes in an attention-driven media ecosystem to stoke divisions and manipulate users.

Then three counter-trends are outlined, whereby technology has and could continue to facilitate a better relationship between European publics and civic life, starting with social media as a catalyst and focal point for political activism, mobilisation and organising. Then they touch on the powers of digital nudging, its effects on giving, civic debate and voting practices, paying special attention to how purposeful design and positive social nudging can help create healthier online environments and incentivise political engagement. Finally, they survey how advances in artificial intelligence, although still in their infancy, offer new opportunities to bring about better accountability and transparency in online information environments.

In the last section of this report, they sketch out how these trends may continue in the future. They note that as individuals increasingly retreat to private spaces to access and discuss political news and information, new challenges will emerge for policymakers to monitor and remedy the spread of misleading, false or polarising information. Beyond that, many of today's political manipulation tools are likely to sharpen with time as they benefit from technological advances in artificial intelligence and increasingly embedded communication cultures. This could take the form of increasingly sophisticated conversational interfaces and 'deepfakes' for example – an image synthesis technique already used to create hoaxes and falsehoods involving politicians. Yet as technology becomes more and more politicised and regulatory efforts are ramped up to address these new threats, we caution against short-sighted legal action, which if taken precipitously, could have chilling effects on democracy itself.

In conclusion, effectively tackling polarisation revolves around three axes: accountability and transparency, user activation and contextual literacy, and greater investment in digital infrastructures.

As a way forward, they expect that these mechanisms, from targeted messaging to digital political strategies and computational tools, to evolve, reflecting technological progress, and changes in communication cultures.

4.4.5. Political advertising and media campaign during the pre-election period: A Comparative Study (Ref. no. 84)

Reference title: Glavaš, Organisation for Security and Co-operation in Europe. 2017. Political advertising and media campaign during the pre-election period: A Comparative Study

Key words: *political advertising, campaign, pre-election, Montenegro*

The article compiles a comparative analysis of the legal frameworks in seven OSCE and Western Balkan region countries related to the political advertising and media campaign during the pre-election period.

The article aims to improve the quality of media legal framework regulating political advertising.

In terms of methodology, the regulations are compared in between the Western Balkan Countries (Albian, Bosnia and Herzegovina, Nord Macedonia, Montenegro, Kosovo, Serbia), and Turkey, or the WBT countries. After which recommendations are proposed for the Western Balkan Countries and Turkey in general and additionally with focus on Montenegro. Comparison is also done with European countries (Denmark, Finland, Germany, France, Italy, the Netherlands, Spain, and the UK).

The paper discusses the regulations around political advertising, in the countries and came with the following recommendations.

Western Balkans countries and Turkey should keep the current legal and regulatory provisions that define the beginning of the election campaign and the election silence. Some variances in legal stipulations are in no way in collision with the internationally accepted standards.

The obligation to report elections in a fair, balanced and impartial manner should apply to both public service and private broadcasters. Publicly funded broadcasters should provide a complete and impartial picture of the political spectrum in the coverage of an election. Private broadcasters should have this obligation as well, since they are using the limited public good (frequencies) which should go with at least a certain level of responsibilities towards the public.

The effectiveness of the silence rules for the opinion polls is sometimes questioned, given that the public may obtain the poll results, not necessarily from the media to which the restrictions apply, but by other means, such as by accessing the Internet or from foreign newspapers or broadcasters. Given this fact, it is considered that too restrictive rules in this area should be avoided, and that the duration of the prohibition to publish the opinion polls should not be excessive.

If paid advertising is allowed it should be subject to some rules: primarily, that equal treatment (in terms of access and rates) is given to all parties requesting airtime. In addition, the public must be aware that the message does not represent an organic, editorial part of the content, but has been paid for. It may also be considered important to set limits on the amount of paid advertising that can be purchased by a single party. There are no strict regulations to specify

whether it is desirable to set any precise limits on the amount of paid advertising, as it is considered that the decision on this matter should be taken at the national level.

Free political advertisement should be according to one of three principles: (1) principle of equal access, (2) principles of proportionally, and (3) a principle of mixed access. A negative side effect is that extremist views might help the propagation of ideas which are harmful to democracy and/or create a kind of congestion of the communication channels which might hurt major political parties in delivering their messages to the audience. When airtime is made available to parties, it should be granted in a fair and non-discriminatory manner and on the basis of transparent and objective criteria.

The regulatory acts on conducting the election campaigns in the WBT countries should include more precise stipulations on the right to reply (in the printed media), if possible, within the Election Law. This stipulation should allow for a specific procedure to guarantee an urgent right of reply, including on the reflection day/ the election silence if the right of reply cannot otherwise be exercised.

In conclusion, the regulatory framework in WBT area, with provisions on equal treatment of political parties by the media during the election campaign, is on general terms aligned with the desirable/recommended international standards. In the absence of the one defined set of rules and unambiguous guidelines most of WBT countries have adopted solutions and definitions that have proved their validity and resilience in the countries with a history of dozens of free and fair elections. Nevertheless, in practice there are generally shortcomings which indicate that the frameworks are insufficient.

As next steps, some direct recommendations are given for Montenegro: Election broadcasts should be monitored and regulated by an independent, impartial body; Consideration could be given to amending the election law to clearly define when the official campaign period starts and ends; Effective supervision of media compliance with the law during the electoral campaign could be strengthened by a proactive independent body authorized to decide on complaints and take prompt and effective action against infringements of the law; The existing legal framework for the media would benefit from a revision to clearly define a political advertisement; Political parties could consider agreeing on and adopting a Code of Ethical Conduct during the election campaign.

4.4.6. Protecting the Debate: Intimidation, Influence and Information (Ref. no. 92)

Reference title: Electoral Administration Team of the Cabinet Office in London. 2018. Protecting the Debate: Intimidation, Influence and Information

Key words: *disinformation, intimidation*

The article compiles a response to electoral recommendations and issues raised in the committee on standards in public life's report on intimidation in public life.

The article aims to bring some clarity on the issue of intimidations on election candidates, campaigners and voters, and have a view on the impact, with the suggestion of creating a new electoral offence.

In terms of methodology, public consultation was held to get the opinion on three specific recommendations related to intimidation of election candidates and voters.

The paper discusses the following three recommendations and issues. They are aimed at improving political debate and helping electors to make an informed decision.

As a first recommendation, the Government should consult on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners, allow for appropriate electoral sanctions and to make clear that this kind of abuse will not be tolerated. Intimidations of this kind have an impact on individuals but also on the democratic process. For electoral offences, the sanctions should be as well criminal (fine or imprisonment) as civil (eliminated form voting).

The second recommendation tackles the consolidation and clarification of the electoral offence of undue influence. The offence of undue influence is designed to prevent intimidation of the elector, this considers (a) providing clarity of the offence; and (b) intimidation at polling stations.

And as a third, the government should extend electoral law requirements for an imprint on campaigning materials to electronic communications. Digital campaign techniques at elections include increasingly sophisticated use of data and more personalised and targeted messaging. The Government is committed to ensuring transparency for voters, for them to be able to make an informed choice on the arguments presented.

In conclusion, this consultation and discussion paper demonstrated the widespread impact that these electoral offences (intimidations) are having on the elector making an informed decision at the ballot box, based on choice, policy and principle.

As next steps, it is hoped that political parties will be encouraged to lead the way in creating a healthy political culture in which everyone can participate, and persuade those in public life to take responsibility for the tone of the debate during the election period, rather than on misinformation or abuse. Also, election rules must keep up with technology to maintain the transparency of our electoral system and to allow for an informed and transparent debate.

The Government considers that these three measures should allow electors to make their choice at the ballot box based on quality, effective and informed discussion, free from abuse, intimidation and misinformation and with a range of candidates from which to choose.

4.4.7. Report on the 2019 elections to the European Parliament (Ref. no. 103)

Reference title: European Commission. 2020. Report on the 2019 elections to the European Parliament

Key words: *elections, social media, transparency, campaigns, disinformation, digital campaigning*

This report examines the 2019 European elections. It addresses and analyse on different aspects of the European dimension of the elections such as the participation of voters, data protection aspects or impacts of disinformation.

In terms of methodology, the report analyses and presents mains findings, but is completed and accompanied by a Commission Staff working document, which follows the same structure as this Report in detailing its findings.

The report starts by listing the regulatory efforts from EU before 2019 European elections, following the evidences of online interference techniques, including cyberattacks and circumvention of traditional electoral safeguards such as funding rules. Therefore, the Commission published a package of measures ('the electoral package') designed to addressing these challenges. The package promoted a comprehensive approach and mutual support among competent authorities, supported by the establishment of elections networks at national and European level. Following this package, the Commission took initiative also on disinformation with the code of practice on disinformation and the action plan against disinformation, including the Rapid Alert System and the analytical and awareness-raising activities of the European External Action Service (EEAS) Strategic Communication (StratCom) Task Forces – contributed to securing the integrity of the electoral process and voters' confidence in it.

The report also develops the mapping of Member States rules and practices where it shows that MS have in common rules on transparency donations of and/or prohibit anonymous donations; ban foreign funding of political parties and campaigns, though some only limit its amount or impose disclosure requirements and also have rules on silence periods. On the other side, there are several matters where differences emerge between MS such as half of the Member States require transparency for paid political adverts and communications, only few MS have specific rules on social media.

The report reached important conclusions, such as that young and first-time voters drove turnout figures to the record high. This document also concludes that 2019 election campaign was the most digital to date, where almost half of EU citizens used and relied on online news as their main source for information about national and European politics. Nevertheless, the Member States have different rules regarding digital campaigning, including on paid-for political content online. Although European citizens expressed increased satisfaction with free and fair elections in the EU, additional work is essential to protect democracy from several threats such as foreign interference and manipulation.

As a way forward, the report reflects on further work and progress to be made on the democratic participation of women, citizens with disabilities, younger citizens and other groups. Moreover, there are still mobile EU citizens that encounter difficulties voting in certain Member States.

4.4.8. Suspicious Election Campaign Activity on Facebook (Ref. no. 108)

Reference title: Davis, Livingston, Hindman. 2019. Suspicious Election Campaign Activity on Facebook

Key words: *election campaign, social media, far right parties, artificial promotion*

The report analyses the political parties' presence on the social platform: Facebook. It follows the political parties' online activities in Germany, in the months leading up to the May 2019 European parliamentary elections. It deducts that the far-right populist parties are more present than any other party.

The article aims to explain how several factors contribute to this phenomenon.

As a methodology, 6,817 political pages have been examined representing all the major and several minor parties in Germany. Also, nearly 220 million interactions were examined within these pages and their content from October 2018 to May 2019. These include profile-to-page (like, follow), page-to-page (follow), and profile-to-post (like, share, comment) interactions. The study was conducted in accordance with the George Washington University's guidelines on social media research.

The report discusses the findings that the far-right political party in Germany 'Alternative for Germany' (AfD) dominated German Political Facebook.

AfD content was promoted by a dense network of suspicious accounts. The AfD party had on Facebook about 1,663 pages it maintained. This is more than all the other parties combined. Its content was shared between five and seven times more than all the other parties combined, and it produced 1.2 times as many individual posts than the other parties combined.

As a content strategy, the AfD has similar content on different pages, for which these pages often repost the same photo dozens of times, from up to hundreds of active pages.

The party makes use of artificial promotion in favour of AfD. A network of roughly 200,000 accounts were identified that like or promote AfD pages and content. These accounts are densely networked and often engage in what appears to be coordinated behaviour. Suspicious accounts were identified with the following criteria: multiple changes of name or location, misleading names, stolen photographs, dubious linking of posts, and different profiles using the same picture.

The authors, during the study, have detected several suspicious page followers. There are two types: the first ones are page promoters, which follow hundreds of AfD pages, but otherwise inactive accounts. The other type also has German followers on itself.

In conclusion, a large network of suspicious accounts was active in promoting AfD Facebook pages in the lead up to the 2019 European Parliament elections. This shows the possibilities of (mis)using the social media platform for political purposes.

As a way forward, in the aftermath of the 2016 U.S. election, Facebook has reportedly devoted energy and resources in an attempt to reduce fraudulent behaviour on its platform. Data from the 2019 European Parliamentary elections, however, raises questions about the effectiveness of Facebook's efforts to date, and their strategy in the future.

4.4.9. AI in the election industry demands transparency (Ref. no. 115)

Reference title: Esposito, Tse, Entsminger, Jean. 2020. AI in the election industry demands transparency

Key words: *artificial intelligence, election industry*

The article focuses on the use of artificial intelligence (AI) in the prediction of elections results.

The article discusses that over the last campaigns, the prediction industry has been increasingly turning to machine learning to drive forecasting. Some companies such as MogIA and BrandsEye showed success at predicting the 2016 US elections by leveraging alternative sources of data such as tweets, despite more well-watched sources such as BBC and FiveThirtyEight failing to effectively predict. Others such as Cambridge Analytica directly, or the research of Alto Analytics, show the power of shaping political preferences. Concern, however, should not only be with whether the predictions are accurate, but how AI and the decisions that can come with its design, reshapes the role of prediction in public discourse. Many attempts at prediction tell us more about the people trying to predict than the world they are trying to understand. Prediction tells us how these people, and at some points the prediction industry at large, see the problem, how they find data, how they ask and frame questions, and how they understand what will convince and persuade members of the public. AI systems are extensions of the mental models of the production team, they are expressions of their assumptions and biases, as much as the inevitable biases of their data. No one wants biased data, but real-world data is inevitably subject to inconsistencies. However, it's not enough to simply acknowledge such mental models, steps need to be made to ensure that cognitive diversity is reflected across the design and use chains—lest AI simply reflect our varieties of ignorance. Following the prediction industry can have a potentially agenda shaping effect: directing the news and reporting environment on who to listen to, determining who among the candidates is worth the attention, or worse, how the public argues and investigates the key issue items for the election, and what people find worth referring to when trying to persuade one another.

As a way forward, the debate around AI, public information, and the fairness of our democracy will continue. Part of this debate should begin with improving, or demanding, transparency and the responsible design and use of AI in media outlets and the prediction industry. Efforts could include audits of prediction algorithms, their application, and initiatives to improve the validity of data collection and use. There is a need to have higher standards for any industry dedicated to shaping voter perspectives.

In conclusion, when used appropriately, AI can be a powerful tool to empower public conversations and strengthen the quality of political debate—but it requires taking a hard look at whether or not AI is needed at all. Algorithms should not be surrogates for historical decisions. Democracy without the possibility of public persuasion no longer counts as democracy. Each generation rediscovers the past for themselves, and how we use and understand AI in electoral races will be a fundamental reflection of the common public consciousness of our time.

4.4.10. Lessons Learned: Social Media Monitoring during Humanitarian Crises (Ref. no. 175)

Reference title: Democracy Reporting International. 2020. Lessons Learned Social Media Monitoring during Humanitarian Crises

Key words: *Social media monitoring, online disinformation, hate speech, elections*

This document provides an overview of social media monitoring (SMM) analyses conducted in Austria, Portugal, Poland, Romania and Croatia.

The document aims to provide examples for teams deciding on what to monitor, how to assemble a team and other critical questions.

The document discusses that five cases from elections in Europe between 2019 and 2020 indicate that the field of SMM is still experimental. Applied research on the role of social media during elections is important to complement academic and more long-term research on phenomena like the effect of disinformation and hate speech on political behaviour, and for its potential to capture current developments and hold tech companies more accountable. Also, accessing data while events unfold helps to preserve data that might be deleted afterwards. Since this is a new field, there is not one single type of organisation, team makeup or methodological approach required for social media monitoring.

Based on the lessons learned from the five projects, future social media monitoring efforts could benefit from action by specific stakeholders:

The government should require companies to provide reasonable access to CSOs when monitoring a public space and invest more in social media monitoring projects at the local level.

Social Media Companies should also invest more in social media monitoring projects at the local level, provide access to deleted data for researchers and provide access to additional aggregate metrics related to user engagement (e.g. clicks). Data access stability for researchers should be improved and the quantity data that researchers are permitted to download should be increased. The Facebook Ad Library should be expanded in order to hold candidates accountable during elections.

CSOs and Universities are recommended to publish a guide or tool to ethically use, save and publish social media data for research. They should also build a repository of sample studies to help organisations get started and train or collaborate with journalists to conduct this type of work.

As a way forward, DRI is also working on other tools to address the challenges faced by social media monitoring teams.

4.4.11. Social media monitoring: Early Parliamentary Election Campaign (Ref. no. 216)

Reference title: *Wahlbeobachtung.org. 2020. Social Media Monitoring Early Parliamentary Election- Final Report*

Key words: social media platforms, monitoring, Facebook Ad library, campaigning, political advertising, interactions, political parties, spending, regulation.

The report examines online campaigning on social media platforms in Austria.

It aims to provide the results from the media monitoring project at the occasion of the Austrian early parliamentary elections on 29 September 2019. The monitored social media are Facebook, Twitter and YouTube.

In terms of methodology, advanced supervised and unsupervised algorithms were used to conduct an analysis of the text that was posted to Facebook and Twitter during the campaign. The research concentrated on a representative sample of the accounts of key political parties and contestants as well as selected media, journalists and social influencers. The generated data was visualised and transferred to an interactive tool, accessible as data4good by VDSG for further analysis. YouTube videos were selected on the basis of the same keywords to gather information about political contents. The technical team of FDV DAPP applied string-lines in a structured-coded internal script to collect information through the platforms' API. The contents of the 25 weekly most-watched videos were double-checked to verify that they fit the sample.

In particular, the report finds that during the 2019 European Parliament elections the Facebook activity of the FPÖ party and the SPÖ party and their high number of followers make them the two most dominant political parties among those engaging in online campaigning. Also, they are the ones that spent the most on Facebook political advertising. The report points out that such investments are not surprising, given the importance of social network services in everyday life. It acknowledges that the best-known way of looking at the use of social media during elections is fact-checking. Several different aspects of online phenomena can be monitored around elections, e.g. political advertisements, bots and trolls, hate speech, and strategic disinformation, or fake news. The monitoring of hate speech and fake news can require a lot of human resources; in some countries it is done by specialised organisations. Disinformation can come in various forms, including narratives to harm the integrity of the electoral administration. Like bots and hate speech, it is difficult to monitor, and there are limits to the use of technology to detect or prevent it. Deep fakes are expected to take disinformation to yet another level in the future.

The algorithms used in the project analysed among others the percentage of reactions (emojis), expressed for specific politicians. The mostly used reactions was 'love'. In addition, with regard to Facebook Ad Library, the report points out that it falls far short of its potential, because it does not allow selecting a time period of interest (only defined periods are possible such as past week, past 30 days, past 90 days); it does not allow determining when a purchased ad stopped running; it does not provide a precise information about payment but a bin only, which are very large and it is not possible to determine how much money was spent on various demographics. Finally, user interactions information (likes, shares, comments) is not included Facebook Ad Library. Therefore, the report concludes that the ad library is currently useless as a way to track political messaging.

The report explains that in Austria no special law or government regulation is yet in force to regulate social network services. Campaign and party finances are regulated but no supplementary instructions about online campaigning have been released. The Court of Audit, as well as several civil society groups, have

highlighted the insufficient disclosure requirements and inadequate oversight. The Austrian legal framework to protect the freedom of expression and information in respect of the EU's General Data Protection Regulation (GDPR) protects only corporate media, but not citizen journalism on social media. While social media monitoring involves the collection, storage, and processing of a large volume of data, the GDPR requires a legal basis for the processing of personal data, which currently does not sufficiently exist in Austria.

Last but not least, the report outlines the problem with access to data from social network providers as a main hurdle in monitoring social media. YouTube is the best API to work with as it grants access to every video ever published on the platform. Obtaining access to Twitter data is also simple and straightforward. Facebook, however, has been constantly reducing data access in the last two years.

In conclusion and as next steps, the report finds that in order to effectively promote a level playing field and transparency in campaigns, to protect the privacy of citizens and to safeguard electoral processes against potential manipulation and disinformation, the EU and its Member States such as Austria should provide clear regulations, coherent implementation and independent oversight of political campaigns in social media and online platforms. To enhance effective electoral campaign oversight and better detection and analysis of disinformation campaigns, social media platforms should provide meaningful access to data for election observers and researchers in line with personal data protection rules.

4.5. e-Voting

4.5.1. Digital technology in elections - Efficiency versus credibility? (Ref. no. 20)

Reference title: Russell, Zamfir. 2018. Digital technology in elections - Efficiency versus credibility?

Key words: *digital technology in election, election fraud, e-voting, issues*

The article examines the different digital solutions in countries over the world and highlights the issues they encountered with it.

The article aims analyse the advantages and disadvantages of the use of digital solutions in the election process.

In terms of methodology, the paper summarises phases of the electoral process followed by a view on the issues, risks and possible solutions of practical use of the digital solutions.

The paper discusses that digital technology offers multiple benefits at all stages of elections. The first stage: "Registering voters", is about creating accurate and manageable voting registers. Due to lack of identification documents it is seen that some of the least developed countries become leaders in the use of biometric technology in elections. In the second stage "voters' identity verification" the identity is verified based on up to date registers. Some countries use a special voting card, others use fingerprints. Compared to finger inking, biometric identification provides a secure and discreet means of preventing multiple

voting. During the “vote casting” phase attention has to be put on the illiteracy of voters in some regions, and safety measures in the voting machines themselves. For the vote counting phase, digital voting saves time on the counting and reduces the human counting error. In the last phase “Results transmission and tabulation” the transfer and spreading of the voting results can be done way faster with a digital solution.

Certain standards for digital technology in elections has to be respected. Polls (digitally) carried out must comply with the general principles set out in Article 25 of the UN's 1966 International Covenant on Civil and Political Rights. International standards addressing of electronic voting do not yet exist. However, the Council of Europe has its recommendations on standards for e-voting (adopted in 2004, updated in 2017).

Several Problems have been noted by different countries using digital voting systems. In general, digital systems are more used in Latin America and the Middle and Far East. Europe tends to be a bit more reluctant in putting its trust in the digital systems. The main concerns are: reliability, protection, auditability, verifiability, testing, and trust.

Reliability. Digital solutions help but are not infallible. For example: systems are sometimes unable to match fingerprints with registered voters or fail in transmitting the results. These events raising suspicions of fraud.

Protection from electoral fraud. In some cases, digitalisation could even facilitate fraud (hacking, etc). It could manipulate the voting results or create a distrust in the system. A backup system recording votes on paper is advised.

Auditability of electronic voting. When votes are only recorded digitally, there is a risk of irretrievably losing them. A paper-based print or backup is advised.

Verifiability. The system should be transparent enough for voters to understand their vote has been correctly registered, therefore a paper trail is still used. A complete “end-to-end verifiable voting” system is still to be developed.

Testing and certification by independent organisations are a must, and it is even advised to also have tests done by activists.

Trust in the digital system is essential for adopting the procedure by the voters.

Some practical considerations have to be taken. The implementation of these digital solutions can be very (or even too) costly for some developing countries, but should be considered anyway to prevent fraud, or even establish more trust in the voting results. The voting machines should be robust to survive the transportation in some countries (rough terrain, dust, sand). Also, electricity and internet should be provided.

Technological options for electronic voting can be considered. Optical scans to read paper ballots have the benefit that it gives trust and security to the voters that the vote is recorded correctly, and the paper functions as a backup. A “Direct recorded electronic” system is a fully digital system. When not equipped with a (auditable) paper record it lacks trust with the voters.

Internet voting, or i-voting, as applied in Estonia, remains still controversial, but it has an impact on the voting society. It potentially improves the voter turnout, as more people actually participate in the elections. It reduces the total costs of organising the elections. It is a more convenient way of voting.

The main argument against i-voting is the security risks. (Malware, hacking, etc.) According to some, e-voting cannot be made safe, but at least the risk can be reduced to an acceptable level. In the case of Estonia, that voters can check if their vote has been cast as intended. Another problem is that it cannot be checked that that nobody is watching voters as they submit their ballots. The possibility of recasting votes can be a solution.

In conclusion, the use of digital solutions in the electoral process is desired, but attention needs to be given to some issues it brings. A full covering digital solution still needs to be developed.

As next steps, the EU electoral monitoring guidelines emphasise the need for observers to assess the use of technologies such as biometric identification and electronic voting machines.

4.5.2. Potential and challenges of e-voting in the European Union (Ref. no. 28)

Reference title: Trechsel, Kucherenko, Silva. 2016. Potential and Challenges of E-Voting in the European Union Study

Key words: *internet voting; e-enabled elections*

The study describes the opportunities of Internet voting and its challenges, namely with regard to legal constraints, political and social implications, and technological and security challenges.

The study aims to discuss the merits of e-voting as solution and possible pathway to eliminate threats or minimise their effect.

In terms of methodology, the study builds on the latest academic research on the topic and on the, previous technical reports developed by the European Parliament (EP), i.e. the "E-public, e-participation and e-voting in Europe - prospects and challenges" final report, and "The Reform of the Electoral Law of the European Union". Furthermore, it includes empirical evidence from the most recent trials of Internet voting and e-enabled elections and evaluates its implementation while bearing in mind the specificity of EP elections.

The study discusses the potentials and challenges of the implementation of Internet voting in EP elections. The implementation of Internet voting carries the promise of elections with more participants, of strengthened efficiency in the electoral process, and the hope of bringing voters and their representatives closer together. On the one hand, Internet voting offers many potential advantages such as facilitating the voting process, increased convenience to voters, gains in efficiency and the promise of increase in turnout rates in the long run. On the other hand, it also comes with multiple challenges which, if not properly addressed, can undermine the integrity of elections.

Politically, it is fundamental to foster a broad consensus among political elites for the implementation of Internet voting. This calls for a transparent, involved and participated process, where the relevant actors have a voice. Internet voting should also be relatively neutral from the political point of view, that is, the new procedure should not benefit disproportionally given factions of the political spectrum.

Technological and security concerns are often pointed at as the main threats to Internet voting. The most relevant social challenge is the digital divide. Although inequality has been a historical determinant of electoral participation long before computers and the Internet saw the light of day, it is a concern that parts of the population remain excluded from these technologies and that a gap persists between EU countries regarding computer literacy and household Internet usage and availability. The success of Internet voting depends largely on how it is perceived by the people meant to use it: citizens. Therefore, it is fundamental to know what their attitudes towards the implementation of Internet voting are. Listening to citizens' opinions and identifying their main concerns provides policy-makers with the opportunity to design the system in a way as to address these concerns and thus be both responsible and responsive. Unfortunately, there is a shortage of data on citizens' attitudes towards Internet voting at the European level.

In conclusion, the experience from successful cases highlights the benefits of developing a gradual, step-by-step designing and implementation of Internet voting systems. It is also highly recommended to opt for a decentralised Internet voting structure which involves all the MS in the process, with a coordinating role for the EU institutions. Finally, it is recommended to follow a principle-based approach to legal regulation of Internet voting, with a focus on comparative lenses and building on existing cases of updated voting legislation.

As a way forward the Reform of the European Electoral Law is an important contribution to harmonise electoral procedures across all Member States. It is of utmost importance to future Internet voting in EP elections. Internet voting at the EP level could lead to a call for the dissemination of the new procedure at the national, regional and local level, both by citizens and national political actors.

As a way forward, the final Report will be finalised by the end of 2019 and will answer the seven research questions.

4.5.3. What if blockchain technology revolutionised voting? (Ref. no. 37)

Reference title: Boucher. 2016. What if blockchain technology revolutionised voting How blockchain technology could be used for e-voting

Key words: *blockchain, electronic voting, blockchain-enabled e-voting (BEV)*

This article provides a brief explanation on how blockchain technology could be used in electronic voting and what its potential impacts and further developments are.

More specifically, the article explains that the blockchain-enabled e-voting (BEV) would empower voters to record, manage, count and check the votes themselves, by allowing them to hold a copy of the voting record. It points out that BEV would shift power and trust away from central actors, such as electoral authorities, and foster the development of a tech-enabled community consensus. The paper points out two approach to develop BEV systems for e-voting -

one way is to create a new, bespoke system, designed to reflect the specific characteristics of the election and electorate. A second approach that may be cheaper and easier is to 'piggyback', running the election on a more established blockchain, such as that used by the bitcoin. The author points out that the second approach may be more secure for elections with small number of voters, given that the security of a blockchain ledger relies upon the breadth of its user base. Regard taken that BEV have been used for internal elections of political parties, and shareholder votes in Estonia, the author opines that in the near term, BEV's strongest potential may be in organisational rather than national contexts. Furthermore, the article suggests combining BEV with smart contracts to automatically take actions, e.g. election results could trigger the automatic implementation of manifesto promises, investment choices or other organisational decisions.

The article also outlines some concerns - with anonymity, coercion and accessibility - that may be associated with the use of BEV but highlights that these concerns are the same as those that are associated with traditional paper systems. Coercion is a threat for any voting system that offers remote participation (e.g. postal votes). For both BEV and paper elections, the use of private polling booths is the only guarantee against fraud. With regard to accessibility, BEV could complicate matters by presenting citizens with too many access options (e.g. voting at a terminal in a traditional booth or using a personal devices, and/or using different interfaces for citizens who wish to go beyond casting votes and also exercise their right to access data and check that the correct procedures have been followed to all voters is a key concern in all elections. Anonymity is a crucial element of democratic participation, although most national elections are in fact 'pseudonymous', because although it is difficult to discover how the voter voted, it is not impossible because the ballot paper linked with a personal entity via a code on the electoral register. In this sense, the author points out that BEV is also pseudonymous, so it may sometimes be possible to discover how an individual voted. He proposes a solution to enhance trust in the technology by introducing a centralised authority to distribute pseudonyms and keep them secret, however such central power would be in discrepancy with the idea of decentralisation associated with blockchain.

Finally, the paper concludes that the extent to which blockchain technology will flourish in the area of e-voting may depend upon the extent to which it can reflect the values and structure of society, politics and democracy. It points out that when assessing the potential impact of BEV, one must consider that BEV does not just digitise the traditional voting process, but it proposes an alternative with a different set of values and political basis. The BEV process differs from the black-boxed, centralised and top-down authorities' managed elections, since it is managed by the people and it is transparent, decentralised and bottom-up. While participation in traditional elections reinforces the authority of the state, participation in BEV asserts the primacy of the people. In this light, links are drawn between BEV and transitions towards a more direct, decentralised and bottom-up democracy.

4.5.4. Blockchain-Based Electronic Voting System for Elections in Turkey (Ref. no. 46)

Reference title: Bulut et al. 2019. Blockchain-Based Electronic Voting System for Elections in Turkey

Key words: *blockchain, e-voting, electronic voting, internet voting*

The paper describes using Blockchain to eliminate all disadvantages of conventional elections.

The paper aims to suggest a solution specifically for problems of conventional paper elections in Turkey. Despite the solution is specific to one country, it may be taken as a general application, and can be customized to other countries.

In terms of methodology, a technological solution, blockchain, is proposed to tackle the problems coming with conventional paper elections.

The paper discusses that to dissipate problems of both conventional and e-voting elections, e-voting can be improved using Blockchain mechanism. Blockchain has impressive features to overcome troubles of voter's security, privacy and data integrity of votes. Blockchain is an inalterable and an easy confirmable system. Under favour of these qualifications, Blockchain has a significant potential to be an alternative to traditional elections. It brings smart solutions to central authority problem in terms of all blocks having all data in the chain.

In Section II, related works about e-voting and blockchain are discussed. Such as a voting process that relies on citizen's email address, peer-to-peer blockchain based voting system, a database alongside blockchain, blockchain IoT interactions, a one-time ring signature to ensure the anonymity of the voting citizen.

In Section III, general architecture of the proposed blockchain based e-voting election system is explained and modelled with supporting materials. Many aspects should be considered in order to construct a secure blockchain-based election system. The first factor is human for such a system, the proposed system will be consisting of nodes (computers in design) that is closed to human interference. The second issue is saving system from hackers. In a blockchain system, every transaction is related to the previous one. So, changing an accepted transaction is impossible for such a system. Due to the consistency of the blockchain, data will always be consistent, and voting will be reliable.

At the following section, Section IV, proposed system is analysed from different aspects. With using the proposed e-voting system, there will be a system that can be modified for each election easily. Because of the system is designed to consider candidates at the main voting mechanism and data can be provided however it is wanted. Thus, this system is easily generalizable. In this system, the whole voting information are hold at the highest levelled blockchain so, voting information of the whole country can be reached instantly at any time after it is synchronized.

In conclusion, the blockchain based e-voting system, provides a trusted, secure and fast voting system for Turkey. The proposed system is suitable to apply in other countries, whereas integration is hard work, since each country has different laws and election systems change between countries.

As a way forward, the system can be applied to cases, and measurements can be taken to compare if the calculations hold. Synchronization and consensus algorithms can be discussed and improved for better performance and security.

4.5.5. What We Don't Know About the Voatz "Blockchain" Internet Voting System (Ref. no 47)

Reference title: Jefferson et al. 2019. What We Don't Know About the Voatz "Blockchain" Internet Voting System

Key words: *blockchain, voting, voting system, authentication of voters*

This article aims to urge the disclosure of more information on the features and functionalities of the "Voatz" blockchain internet voting system.

In terms of methodology, the article explains that Voatz is a recent start-up company that is operating an Internet voting system intended for public elections, used in West Virginia, US in the recent years. The authors consider that the functioning mechanisms of the Voatz system should be more transparent and clearer to the public, and therefore urges Voatz to reveal some technical details on their system by asking a number of important questions.

In particular, the article points out that the major distinguishing feature of the Voatz system is an elaborate authentication of the voter based on automated facial comparison of a photo of the voter's photo ID to a short selfie video and a back end virtual ballot box in the form of a closed, permissioned blockchain. The process of authentication passes through the Voatz smartphone app, where the voter takes a photo of their driver's licence (back and front) or passport photo page along with a short selfie video. By means of Machine Learning (ML) facial comparison software (owned by Jimio, contracted by Voatz) the faces from the photo and the video are compared, the voter is authenticated, and their name and address are extracted from the photo ID and returned to Voatz as the true identification of the voter. The authors point out that there are a lot of "unknowns" in these procedures and ask questions about the type of dataset used to train the ML, the false negative and false positive errors in facial comparisons, whether a human is always involved after failure in automated facial comparison etc.

A number of data protection-related questions are also asked, as it is not clear who retains the data (Voatz, Jimio, the state or all three?), what data is destroyed, what safeguards are in place to prevent the data from being stolen or sold, where the data is stored etc.

Another group of questions relate to the voter's authorisation, in other words, verification if the voter has the right to vote. The authors ask what access Voatz has to the voter registration database and what prevents Voatz from associating the trove of sensitive personal information about the voter collected during authentication with the information in the voter registration database (party affiliation, voting history, e-mail address, phone number, etc.) to create a valuable and potentially dangerous database usable for identity theft or for illegal political purposes.

The authors also ask questions related to the Voatz app, which is designed so that voters can only vote from recent iOS and Android systems from smartphones (not from desktop or laptop computers). The article asks, for instance, whether the source code for the app can be made available for examination and testing and if not, why. Also, what technical measures are in place to ascertain that the voter is not voting from a counterfeit version of the Voatz app, downloaded from elsewhere than Google Play and designed to behave as malware, possibly changing votes before they are transmitted, preventing voters from voting or transmitting a copy of the vote and the voter ID to a third party.

In addition, the authors request Voatz to shed light on their blockchain servers, contents and order, (what data are stored on the blockchain - only ballots or ballots keyed to voter IDs or phone IDs?); the cryptography system, the decryption of blockchain ballots and their transfer into paper, the measures against double voting, the security audits. Interesting to mention are the questions related to the possibility of the voter to verify whether their vote has been correctly recorded and in if not – to "spoil" it after casting it. In such a case the authors ask how the voter can find their vote on the blockchain (with a unique voter or

phone ID?); how is their choice transmitted to them (via the Voatz app or e-mail?); is "spoiling" the only recourse the voter has; what happens to the "spoilt" votes on the blockchain (marked as cancelled but not removed?), etc.

As regards to certification, the authors counterargue Voatz' idea that they do not need to be certified as they are not tabulating votes. The article claims that Voatz is a part of a complete ballot-capturing front-end voting system that does tabulate votes and are therefore subject to certification in order to be used in any public election.

4.5.6. Study on the benefits and drawbacks of remote voting (Ref. no. 93)

Reference title: Lupiáñez-Villanueva et al. 2018. Study on the Benefits and Drawbacks of Remote Voting

Key words: *remote voting, benefits, drawbacks, Internet voting, remote voting options, barriers, drivers*

The study **examines the barriers** to voting encountered by different groups of citizens and maps the different types of remote voting solutions available in the EU Member States, outlining their benefits and drawbacks.

It aims to contribute to the discussion regarding the benefits and drawbacks of remote voting by examining the landscape of remote voting practice and outcomes in use in Europe.

In terms of methodology, the analysis is based on mixed-methods and data triangulation, which consists of using different sources of data and collection methods such as literature and legislation, in-depth interviews with Member State representatives working on electoral matters - local public authorities, political parties, academia, industry, and non-profit organisations), in order to collect key insights. Based on the information, 15 thematic case studies were formed and grouped into three main groups: case studies which examine aspects of the remote voting process; case studies which detail the experience of remote voting for specific groups; and case studies which provide examples of EU Member State experience of internet voting implementation.

In particular, the study splits remote voting into two main groups – non-electronic and Internet voting. The first one includes 6 options such as postal vote, voting by proxy, voting in person abroad, voting at special polling station within the country, voting at mobile polling station and voting in another district etc.). For each of these options the study examines how the votes are registered, casted and counted in the EU Member States as well as what the drawbacks and benefits are. Regarding Internet voting, the study finds that its impact on turnout is unclear. Several studies in jurisdictions that have tried internet voting report high levels of satisfaction from voters and/or willingness to use the option again. However, the literature examining the impact on voter turnout presents mixed results. Some studies have observed an increase in turnout, while others found no such effect. Moreover, due to the nature of elections, experimental research comparing the impact of a remote voting option with a control condition is difficult to conduct. The study's online experimental task showed that the existence of internet voting sometimes had a positive effect on likelihood to vote, but not in all situations. It is also uncertain whether internet voting would increase turnout, if implemented and its impact on costs is unclear.

In conclusion, the study points out that options for remote voting and how they operate vary greatly from one country to another, depending for example, on the electoral system, the method by which voters are registered, the design of the solution, demographic factors, and the aspects of the voting process (such as ballot secrecy) most valued by the population. This implies that in European elections, citizens vote under different systems. While proposing a common approach to the availability of remote voting for European Parliament elections would reduce the complexity of the current status quo, it would also affect the prerogatives of Member States. It should also be stressed if such an approach implied a reduction of the remote voting options in any particular country this might not facilitate participation and might be undesirable.

Remote voting brings the **benefits** of facilitating the act of voting for several groups of voters such as those who live abroad or in remote areas, people in poor health, and those who cannot leave the place in which they are residing at the time of the election. However, remote voting options may also present issues relating to electoral legitimacy and additional administrative burdens for the state. For example, verifying the identity of the voter and observing the election may be more difficult than in the traditional polling station settings. There is currently little evidence about the impact of remote voting solutions, including the consequences for turnout and costs. Moreover, the outcomes may depend on the context and on how the voting options are designed and implemented. Therefore, expectations for what remote voting solutions can achieve should be managed with caution and backed up with evidence that consider the context in which it was generated.

4.5.7. Some states have embraced online voting. It's a huge risk. (Ref. no. 114)

Reference title: Geller. Politico. 2020. Some states have embraced online voting. It's a huge risk.

Key words: *online voting*

The article discusses that the moving of elections to the internet poses huge risks that the United States is unprepared to handle — endangering voters' privacy, the secrecy of the ballot and even the trustworthiness of the results.

The article describes that the internet is riddled with security flaws that hackers can exploit. So are voters' computers, smartphones and tablets. And the U.S. has never developed a centralized digital identity system like the one in Estonia, a tiny, digitally savvy nation that has held its elections online since 2005.

The logic of the question, "If we can bank online, why can't we vote the same way?" has the following problems:

Elections are different. Elections are unique for two reasons: They are anonymous and irreversible. U.S. elections use secret ballots and polling places designed for privacy. Unlike a banking transaction that goes awry, political and legal factors make elections nearly impossible to reverse.

The internet is a dangerous place. An email that someone in Washington, D.C., sends to someone across town might zip through servers in Dallas or Mumbai, or even through hostile countries such as Russia, with each stop offering an opportunity for a hacker to tamper with it. Even if it were possible to require electronic ballots to travel through servers only in the U.S., no method exists to ensure security at every server along the way.

People's devices may already be compromised. What really keeps experts up at night is the thought of average Americans using their computers or phones to cast that ballot in the first place. Election officials cannot peer into their voters' devices and definitively sweep them for malware. And without a secure device, end-to-end encryption is useless, because malware could just subvert the encryption process.

Hackers have lots of potential targets: Attacking the ballot; Attacking the election website; Tampering with ballots in transit; Bogging down the election with bad data; The insider threat.

Audits have faulted the major internet voting vendors' security. Virtually every audit of an internet voting system has revealed serious, widespread security vulnerabilities, although the ease with which a hacker could exploit them varies.

Internet voting advocates disagree. Mac Warner suggested it would "take a nation-state effort" to figure out how to tamper with each of the state's various ballot formats and break into voters' devices. The vendors, meanwhile, usually argue that hackers could never actually exploit vulnerabilities in their products. Democracy Live argues that its product does not constitute online voting at all because election officials print out the ballots after they arrive over the internet. The company also contends that its system is safe because it is hosted on Amazon's well-regarded cloud platform, which has been approved for use by federal agencies.

What it would take to make internet voting secure. Secure internet voting depends on two major advances: technology that allows voters' computers and phones to demonstrate that they are malware-free, and end-to-end encryption to protect ballots in transit. Solving these problems would require expensive, long-term collaboration between virtually every big-name hardware- and software-maker.

4.5.8. Use of technology in the electoral process: Who governs? (Ref. no. 134)

Reference title: Loeber. 2020. *Use of Technology in the Election Process: Who Governs?*

Key words: *election technology, electoral process, technology ownership, electoral management bodies (EMBs), decision-making*

This article discusses the use of information and communication technologies (ICT) in the electoral process including but not limited to e-voting and i-voting, the reasons for this use and the challenges the electoral management bodies (EMBs) are facing in this regard.

It aims to point out the areas of concern in which little research has been conducted so far, such as election technology ownership and independence of the EMBs.

In terms of methodology, reports new data from an international survey of electoral management bodies (EMBs) (N = 78) with data from 72 countries which were asked four research questions. The survey demonstrates large differences between countries in the number and kinds of technology they use in the election process.

In particular, the article explains the independence of the EMBs, highlighting that there is no universal definition on what the term entails. It describes three models - an independent model, where elections are managed by an EMB which is institutionally independent and autonomous from the executive power; a governmental model, where elections are managed by the executive branch of a government through a ministry, or through local structures; and a mixed model, where elections are managed by the executive branch through a ministry with some level of oversight provided by the independent top tier component of the EMB. Independence can also be structural (formal) or normative (actual). In the second case, the EMB does not allow external actors to influence its decisions. This actual independence might change when ICT is introduced in elections, due to the technical knowledge that is required when using ICT. In addition, the article outlines the reason for using ICT in elections – e.g. to fight against declining turnout, to improve the integrity of the voting process, to speed up delivery of results, to prevent voter fraud and increase security in voter registration etc. The article points out a number of challenges for EMBs related to the use of ICT, such as lack of IT skills, capacity and resources to develop and monitor the ICT tools, which leads to outsourcing to private ICT service providers. The author presents the New Public Management (NPM) theory the benefits of such outsourcing which argues that government provision can be economically inefficient, so the private market should be used to supply public goods. However, he also acknowledges the concerns about the use of the private sector in the electoral context, namely that outsourcing can lead to an uneven relationship between big IT companies and less knowledgeable government agencies. A failure of an e-voting system in elections may have stronger consequences on the voters' confidence than a failure of an IT system in another sector. Last challenge is related to ownership of source codes. If the e-voting system provider is reluctant to transfer ownership of the source code, this may pose transparency issues.

The article then presents the results of a survey among 72 countries which replied to four research questions: What role do EMBs play in the decision-making process concerning the use of ICT in the electoral process? Who owns the technology that is used? Who provides the technological support on Election Day? How does the institutional design affect the use and ownership of technology?

It points out that 11 out of 72 countries do not use any technology, where most of them use technology for tabulation of results and registration of voters and candidates. Some countries use technology for biometric voter identification, incident reporting and counting of results. Only 14% of the countries state that they use voting machines and 7% use Internet voting. The results show differences in usage by region – e.g. biometric voter identification is used only in Africa, whereas voting machines are not used in Africa at all. The article presents the responses of the four questions.

In conclusion, it finds that there are differences between countries regarding the use of technology. It is not necessarily the richer, older democracies that use ICT in the electoral process. Also, countries that receive support from international donors are more likely to use technology for voter registration (e.g. in

Africa). Wide variations between countries are also observed as regards the question of ownership and support on the election day. In terms of the difference between independent and governmental EMBs, independent EMBs seem to be more ''in control'' of the technology.

As next steps, the article recommends more research and in-depth case studies to find why counties decide to introduce different ICT in the electoral process. Also, it suggests conducting similar surveys on a regular basis.

4.5.9. 1289th meeting - Democracy and Political Questions (Ref. no. 159)

Reference title: Council of Europe. 2017. 1289th meeting - Democracy and Political Questions

Key words: *e-Voting*

The recommendation aims to harmonise the implementation of the principles of democratic elections and referendums when using e-voting, thus building the trust and confidence of voters in their respective voting process and e-voting schemes.

The document discusses that the Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting remains the only source of reference on the subject. It is used in national jurisprudence even in non-member States, as well as by other relevant international actors.

Since its adoption, the Recommendation has been subject to biennial review meetings. Discussions in the Council of Europe's competent Rapporteur Group (GR-DEM) as well as a recent expert meeting on the Recommendation have also shown a growing consensus as to the need to update the present Recommendation, given newer technological and societal developments over time.

It is in this context that the Committee of Ministers decided to set up the Ad hoc Committee of Experts on legal, operational and technical standards for e-voting (CAHVE).

In 2014, when it became clear that after ten years there was a need for updating Rec(2004)11, the Ad Hoc Committee of Experts on Legal, Operational And Technical Standards for E-Voting (CAHVE), consisting of government appointed representatives from Members states and organisations with direct experience or specialised knowledge on e-voting, was created and given the mandate to revise the standards and prepare a new recommendation in the light of the new developments in the field of new technologies and elections.

The new recommendation, which consists of the actual Recommendation CM/Rec(2017)5 with core aspects of e-voting, the guidelines on the implementation of the provisions of Recommendation with specific requirements and the Explanatory Memorandum, was drafted as an enhancement of Rec(2004)11 and

deals with the most critical part of election technology, namely e-voting, which means the use of electronic means to cast and count the vote. This category includes systems such as Direct Recording Electronic (DRE) voting machines, ballot scanners, digital pens and internet voting systems.

It aims to harmonise the implementation of the principles of democratic elections and referendums when using e-voting, thus building the trust and confidence of voters in their respective voting process and e-voting schemes.

4.5.10. A review of E-voting the past, present and future (Ref. no. 194)

Reference title: Gibson et al. 2016. *A review of E-voting the past, present and future*

Key words: *Remote electronic voting, internet, review, state-of-the-art, e-voting*

The report reviews the past, present and future of on-line voting, from postal voting up to cloud voting. It reports on the role of technology transfer, from research to practice, and the range of divergent views concerning the adoption of on-line voting for critical elections.

The study aims to give a view of the evolution on electronic voting, including its benefits and challenges, to come to some recommendation for its usage in the future.

As a methodology, this report was built by 4 experts on the field of electronic voting based on their knowledge and expertise, with a contribution of 5 specifically selected papers which made a significant contribution to the debate on electronic voting.

The report discusses the evolution of remote voting, where postal voting already exists for centuries, and is still today in use as a trusted way of voting in many countries. The interest in internet voting began in the mid 1990ties where the initial technological steps were taken to realise internet voting. Why up till now the internet voting has not really been taking up, was because of the many political, social and legal matters that arose when deploying Internet voting.

E-voting has been facing lots of issues. The fact that it could be supervised by an authority drew some criticism. This could be countered by executing risk-limiting audits and manual recounts of election turnouts. Because there is so much electronic computers and devices between the voter and the vote-registration for Remote Electronic Voting (REV) that there is a bit of distrust by the people, and no generally accepted solution for this exists. On the other hand, the remote electronic banking is a widely accepted as being safe and secure. This is only an impression as it has bene proven that banking apps also suffer fraud. And there is an extra requirement for voting: there is a unique combination of anonymity, privacy and auditability. The observation of the elections is harder to organise, if even possible.

Another issue is that it is harder to control who actually was the person behind the vote via internet voting. Some people could be forced to vote on a certain candidate, or there is no guarantee of correct voter authentication. Therefor it should be ensured that voters have an opportunity to verify that their vote is cast as they intended and correctly recorded (individual verifiability), and anyone can verify that all recorded votes were properly included in the tally (universal verifiability).

On the other hand, there are some benefits connected to internet voting. It is expected to be less costly, and the ere is a higher voting turnout expected.

Around the world many countries have showed interest, of have started small- or large-scale trials of an online voting system. With the exception of Estonia, the most evolved countries are still in a level of deciding whether or not to adopt internet voting, even after some successful trials. Some other countries have categorically rejected the possibility of using internet voting.

In conclusion, depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Also changing the way in which people vote has many social and political implications.

As a way forward, the authors suggest some recommendation for future use of internet voting. It must be both trustworthy for, and trusted by, its users. The debate on adopting internet voting should be done in collaboration with academic, practitioners and policy makers, so that decisions can be made on the basis of the best evidence and reason available. And finally: secure Internet voting is not an objective in itself—the real objectives are to understand and improve the quality of elections, including their integrity, accessibility, and levels of participation.

4.5.11. Constitutional Constraints for the Use of Information and Communication Technologies in Elections (Ref. no. 203)

Reference title: Krimmer. 2016. Constitutional Constraints for the Use of Information and Communication Technologies in Elections

Key words: *Electoral principles, electronic elections, e-voting, new voting technologies, internet voting*

The article discusses the basic regulations that can be derived from constitutional rules, electoral principles and special case law on the matter.

The document aims to, based on the findings, to propose principal considerations for developing a legal basis for the introduction of electronic elections.

The article describes that to date, most e-voting studies discuss approaches for developing more sophisticated algorithms to solve the problems of unequivocally identifying voters, secretly casting votes, and counting them honestly and accurately. Few authors have addressed how the technology

influences the legal basis or provided actual guidance on how to use such a system. However, following recent high-profile courts decisions on this issue, collaborations between technical and legal sciences are emerging, leading to more sustainable electronic election projects.

While there is no definite solution to the problem of whether technology depends on law or law depends on technology, it is clear that single-disciplinary approaches are insufficient, and that integrated, collaborative efforts are required to deliver legislation for electronic elections, as well as the procurement of such systems.

Security is the ultimate concern when discussing the use of electronic election. Due to their complexity, important principles are sometimes questioned. However, it should be made clear that any electronic system always will have to live up to the exact same standards applied to traditional paper-based systems. While some of the principles need interpretation and/or translation into digital realities, this does not necessarily mean that they should be altered.

4.5.12. *Internet Voting in Austria: History, Development, and Building Blocks for the Future (Ref. no. 204)*

Reference title: Krimmer. 2016. Internet Voting in Austria: History, Development, and Building Blocks for the Future.

Key words: *Internet voting, Austria, trust*

This dissertation aims to investigate the origins of Internet voting, analyse several deployments of Internet voting technology in Austria and identify – based on these accumulated experiences – building blocks that can be useful in decision-making on and planning of future uses of Internet voting technology within Austria and throughout the world.

In terms of methodology, the Professor Krimmer's work addresses a number of research questions, namely, about the origin of Internet voting, the implementation experiences of Internet voting in Austria and the building blocks that can be identified for developing future Internet voting both inside and outside Austria. To conduct the review of the progress of remote electronic voting, the research used research articles, system documentation, whitepapers, technical reports, and press releases to conduct the review.

In particular, the dissertation points out that while early efforts were driven by the belief that elections could make easy use of the Internet, it was shown that while the principles have to be interpreted and consequently applied in a different way, the same principles can still be derived for Internet voting, like integrity, secrecy, transparency, accountability and public confidence. The first countries which raced to run elections using electronic voting systems were Estonia, Costa Rica, Bosnia Herzegovina, Germany, and the United States, however only Estonia was victorious in 2005. To date, Estonia is the only country that has introduced this form of voting without any preconditions or other limitations.

In Austria, the intentions to use information and communication technologies (ICT) in elections concentrated on parliamentary affairs. Austria sought to conduct Internet voting in 2000 in student elections. The Federation of Students' elections in 2009 were a remarkable event that demonstrated highly contentious political debate around the topic. This debate continued after the elections, which were held in May 2009 and suffered from the intense debate and protests and consequential organizational shortcomings. The experiences also showed that accurate legal regulations are needed to show interaction with the constitutional legal texts and to ensure accountability to a remote electronic voting channel through legal means. International standards were a first step, but regulations based on actual experience were needed to show how remote electronic voting channels could be realized and how to avoid problems identified in pilot implementations. This practical knowledge also shows that sophisticated algorithms are not always the key to success. Rather, several key implementations make use of very basic technical means to realize the tasks given by law. In addition, the voters should be able to understand the processes behind the voting systems in order to build trust.

The work establishes a number of criteria for assessment of E-voting. The basic problem of electronic voting requires solving the unequivocal identification of a voter and, at same time, being able to guarantee anonymity with a secret ballot casting. There are four technologies used for identification in E-voting – username and password; transaction number (TAN), biometrics and smart cards. Regarding anonymity, the dissertation points out that it is established at certain moments in time depending on the stage in the electoral cycle – e.g. in the pre-election period, by the organising body, most commonly with a system using TAN, or during the vote casting procedure in the second stage of the elections. In the post-electoral period, anonymity is established after the end of the election day; the votes can still be identified, but the count can only be conducted together, meaning the content of a single vote is never released. Another criterion for assessment is the size of the votes cast, where national and regional elections are the biggest in size.

On the basis of the aforementioned experiences, twelve building blocks were compiled discovered. These include design decisions, such as the following: the form of electronic voting, adaptations of the legal base, the technical means for identification and secrecy, observation, control functions for the electoral commission, evaluation processes, transparency functions, ballot sheet designs, controlling the organizational context as well as providing options for planning and implementation. This framework therefore facilitates and eases the generation of feasibility studies and other analyses and decision making ahead of using Internet voting in an election. With little adaption it can also be used for the use of other voting technologies.

In conclusion, the findings also show that implementing remote an electronic voting system is a complex topic. It requires trust in the election administration; otherwise, suspicion will arise when more technology is introduced and implemented in an election process. Remote electronic voting is one of the most challenging information technology (IT) projects.

4.5.13. *Handbook for the Observation of New Voting Technologies (Ref. no. 208)*

Reference title: Organisation for Security and Co-operation in Europe. 2013. Handbook for the Observation of New Voting Technologies

Key words: *new voting technologies, observation, types of new voting technologies, key observing principles, secrecy, integrity, transparency, equality, universality, public confidence, accountability*

This handbook provides basic guidance on how to observe the use of new voting technologies (NVT)[95] in electoral processes. Several OSCE participating States have implemented or tested NVT during their elections, making use of electronic voting machines, ballot scanners, Internet voting or other electronic means.

The handbook aims to assist election observers in identifying and assessing the various elements of NVT that may impact the conduct of democratic elections.

In terms of methodology, the handbook first provides background to observing NVT, in particular by introducing their advantages and challenges, and by explaining the key principles in observing their use in the elections (secrecy, equality and universality of the vote, integrity of the results, transparency, accountability and public confidence). It also explains the role of election observation mission (EOM) analysts in observing and analysing NVT, as well as the work of NVT analysts in assessing NVT.

In particular, the handbook acknowledges the increased use of NVT in recent years by a number of OSCE States, in processes such as voter registration and tabulation of results, but also, in voting and counting of votes in some countries which has raised questions about the extent to which such applications are in line with OSCE commitments and other international good practices for democratic elections.

In terms of advantages, NVT may increase voter turnout, facilitate involvement of citizens living abroad, lower election administration costs, facilitate the conduct of simultaneous elections, reduce human error (including invalid ballots), improve the accuracy of counting, and increase the speed of tabulation and publication of results. It may also increase access for voters with disabilities and speaking minority languages to elections. However, NVT-related challenges include the need to preserve the secrecy of the vote, while at the same time ensuring the integrity of the results. Internet voting has proven difficult to respect both these fundamental principles simultaneously. Another challenge is that NVT triggers the need to amend legislation, to ensure planning and to provide voter education and training. If not fully addressed, these challenges may weaken public trust in elections.

Furthermore, the handbook gives an overview of different types of NVT – ballot scanning technology, direct recording electronic (DRE) voting systems, Internet voting, hybrid forms of NVT (controlled environment of polling station with centralised recording and counting of Internet voting).

The handbook goes on to explore the role of the EOM. Their key tasks are to understand how NVT are regulated and whether the electoral legislation clearly defines at least the principles for secrecy, equality, universality, transparency, accountability and the integrity of the results. For instance, in terms of security, what provisions in the criminal laws are envisaged in case of cyberattacks, in terms of accountability – if the law regulates the liability of the private NVT vendors, etc. The handbook also defines the role of the NVT analyst, in assessing the public procurement procedures of NVT, and the role of the election administration in the use of NVT. Finally, EOM should report and make recommendations after every election and follow-up.

[95] The handbook defines NVT as the use of information and communications technologies (ICT) applied to the casting and counting of votes. This understanding includes the use of electronic voting systems, ballot scanners and Internet voting.

In conclusion, the findings also show that implementing remote an electronic voting system is a complex topic. It requires trust in the election administration; otherwise, suspicion will arise when more technology is introduced and implemented in an election process. Remote electronic voting is one of the most challenging information technology (IT) projects.

4.6. Hate speech and extreme negative rhetoric

4.6.1. Media Regulatory Authorities and hate speech (Ref. no. 33)

Reference title: Council of Europe. 2017. Media Regulatory Authorities and hate speech

Key words: *media regulation, freedom of expression, fundamental rights, hate speech, elections, new technologies*

The Reginal publication is a result from JUFREX project (Reinforcing Judicial Expertise on Freedom of Expression and the Media in southeast Europe) and describes various cases of hate speech in online media and media outlets, some occurred during elections period and the activities of the National Regulatory Authorities in the field of electronic media (NRA).

The publication aims to contribute to a wider understanding of what hate speech concept encompasses, while providing recommendations and identifying mechanisms to prevent and tackle this problem.

In terms of methodology the publication first explores the concept of hate speech and then analyses cases of hate speech in seven (7) Europe southeast region countries (Albania, Bosnia and Herzegovina, Croatia, Macedonia, Montenegro, Kosovo and Serbia). These cases occurred in media outlet and online media. This publication also compiles in final annexes “legal framework overviews of participating countries” and “Relevant case-law of the European Court of Human Rights (ECHR)”.

The publication discusses firstly on the lack of consensus on universal “hate speech” definition. Though, the publication mention several definitions proposed in different institutional documents such in the General Policy Recommendation No.15 from European Commission against Racism and Intolerance or from the Code of Conduct on illegal online hate speech where it is defined as “all conduct publicly inciting to violence or hatred directed against a group of persons of a member of such group defined by reference to race, colour, religion, descent or national or ethnic origin”.

While freedom of expression is an important fundamental right recognised both in international conventions and in national constitutions, there are certain speech that are discourage and fall under the term “hate speech” as it is not protected by Art. 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms which safeguard freedom of expression. Still on the debate of limitation to freedom of expression, the criteria used by the

ECHR to decide whether such speech is compliant with Art. 10 and Art. 17 of the European Convention of Human Rights includes: purpose of speech, content of speech and context.

Besides conceptualising hate speech and before entering into the analysis of specific cases, it debates on how hate speech is disseminated and what is the role of media on this phenomenon. The example of the ECHR decision on the case Delfi AS vs. Estonia in 2009 is reference case of a legal decision on this matter: though anonymous defamatory comments were not produced by that platform, it did not exclude that the platform had control over those comments, thus allowing them to be disseminated. This was an important step towards democratic expression online, and in 2016 countries like Germany, France and United Kingdom took a more ambitious initiative and "encouraged websites and social media to remove hate speech from Internet". However, even with a definition, hate speech could be perceived differently by different people, and here the role of the national regulator authorities is crucial.

The publication then presents several cases of hate speech on media outlets, in the 7 countries in analysis. For each example, it is mentioned the channel where hate speech was spread (radio, TV, web portal, etc.), briefly describes and quote the content that was disseminated and then it shares the evaluation and decisions from respective NRAs which could go from sanctions, warnings to the providers of such publication amongst others.

As final conclusion and Recommendations the publication indicates potential initiatives of the regional NRA besides their work and activities. In order to increase transparency, it suggests the publication of the annual report's decision from NRA in order to promote public engagement: people will analyse that when proper complains are made regarding inappropriate content, actions are taken.

For the purpose of inclusiveness, NRA should always provide the complainant with the outcome of its complaint. This would show that the case was diligently processed, whatever the result might be (sanction, warning, other)

Finally, suggests that rules and regulations adopted should be based and include but not limited to, principles of protection of the right to freedom of expression and "encouragement of introduction of new technologies".

4.7. Use of new forms of fundraising for political campaigns

4.7.1. Open Primary Elections - Political Party Innovation (Ref. no. 42)

Reference title: International Institute for Democracy and Electoral Assistance. 2019. Open Primary Elections

Key words: *open primary elections; infiltration voting, methods for detection of illicit funding, risks and benefits from open primary elections*

This paper discusses the innovative methods of political parties to include non-members, who may be close to the party in its structures by means of open primaries. Open primaries are elections within the party in which it is not only the formal membership that has the right to vote, but non-members also form part of the electorate.

In terms of methodology, the article aims to reply to some questions about what a party should consider when thinking of going for open primary elections. These are questions about the objectives of the primary elections; the design options available for such elections; the effects an open primary election might have; how an open primary election may help a political party connect to potential voters.

In particular, the article explains that open primaries have become a more common occurrence in Europe, giving supporters and sympathizers a say in the development and management of the party. The use of open primaries has also led to increased attention from the media, other political parties and society more generally. On the one hand, open primaries could be an opportunity for political parties to connect with disengaged citizens, and on the other hand to allow these citizens to influence the party's decisions (which are normally reserved for full members). On the other hand, they may give rise to illicit funding techniques, as they are sometimes not subject to the parties' financial oversight system, and they are also prone to infiltration voting.

The paper clarifies that the regulation of campaign expenditures on open primary elections is important for two reasons. First, open primaries are smaller elections than national ones, which gives money a potentially bigger role. Supporting a candidate might cost less in an open primary than in a general election, and sometimes the winner of a primary is almost guaranteed victory in the later election for leader of a party. Second, it is sometimes the case that open primaries are not subject to the party's financial oversight systems. This opens a window of opportunity for illicit funding and for candidates willing to bypass financial rules. The article thus suggests some measures that might help to avoid any undue influence of money in open primary elections. The measures include putting a cap on campaign expenditures set up in a legal framework and on individual campaign donations, set by the political party, to avoid 'buying' a candidate; setting up transparency and expenditure disclosure rules and elaborating regulations on digital campaigning , crowdfunding, donations and the use of electronic currencies; envisaging party funding for candidates.

It is likely that a large proportion of candidates' the primary election campaign expenditures will be generated by their activities online, a channel which presents significant difficulties for political parties in terms of monitoring and regulation. One option is to liaise directly with the most common providers, such as Facebook and Twitter, to obtain their support for monitoring online activities such as microtargeting or political advertisements. In addition, parties might ask candidates to disclose all payments made to online campaigns and cross- check that information with the providers.

The political party should be aware of the different campaign fundraising techniques of the candidates and ensure that all these techniques are well regulated and can be effectively monitored. For instance, if a candidate is expecting to carry out a crowdfunding campaign, the political party should establish clear rules to determine what is allowed, how campaign money must be collected and what levels of disclosure are required. The same is true for a candidate who chooses to use cryptocurrencies. The political party should clearly delineate what is acceptable and what is not when it comes to the use of cryptocurrencies to finance a campaign.

The problem of 'infiltration voting' that may occur during open primaries is also tackled in the article. It suggests a number of methods for political parties to fight it, such as, imposing restrictions on voting age and nationality (as long as these restrictions respect national legislation and are not of a discriminatory

nature); payment of a nominal fee to be entitled to vote; introduction of 'freeze periods' or using (complex forms of) data analysis to monitor voter registration trends and assess the numbers of party members and non- members who have registered, to detect anomalous behaviour or suspicious registration patterns (e.g. several registrations from a single IP address, or at standard intervals could be an indicator that the rival parties have infiltrated).

In conclusion and as a way forward, the article suggests that political parties should carefully consider the risks and the benefits from open primaries before implementing them. The first open primaries process should not serve as a yardstick for calculating future voter turnout rates, as these might change drastically in subsequent open primaries. Open primaries can help collect valuable voter data that could then be used to support policy formulation and get to know the electorate.

4.7.2. Institutions and foreign interferences (Ref. no. 125)

Reference title: European Parliament, AFCO. 2020. Institutions and foreign interferences

Key words: *election campaign, foreign interference*

The report analyses the impact of foreign interference on different aspects in the European political field, during the 2019 European parliament elections, and the COVID-19 pandemic.

The study aims to provide background information, map the institutional and policy responses, and assess the performance of the actions and tools set up to tackle the challenge of foreign interferences in the EU.

As a methodology, the article based its analysis on existing studies and findings and groups them by topic such as: definitions, Europe's response, the impact on the 2019 elections, the impact on political parties and the interference on the COVID-19 situation.

The report discusses foreign interferences as they are defined on the basis of two elements, malicious intent and lack of transparency. They cover a variety of hybrid methods that foreign actors employ to penetrate domestic politics. Democracies are the main targets of foreign interferences, which are generally carried out by autocratic actors, often making use of advanced technologies. Different techniques and technologies are used for this purpose: DDoS attacks, paralysation of journalism by means of confusion, disorientation and disinformation campaigns on social media.

As a response the EU has developed a multidimensional approach to tackle hybrid threats, and additionally, there is a large cooperation among the national authorities, and NATO. The EU has proposed the Code of Practice on Disorientation, and a Rapid Alert System has been set up to allow immediate response on disinformation.

During the 2019 European Parliament elections, the Code of Practice has shown to be only partly effective. The nature of information operations in the EP elections seemed to rely more on polarisation and less on the fabrication of false or misleading factual statements, making fact-checking alone insufficient to tackle the threat and reinforcing the need for platform regulation and media literacy projects and development.

National political parties are among the main targets of foreign interferences in Member States. As a response most MS have introduced a ban on foreign donations to political parties. Additionally, the EU has introduced penalties for European political parties deliberately attempting to gain benefits from breaches of personal data protection rules.

During the COVID-19 crisis disinformation has been rapidly spreading from Russia, China, and to a lesser extent Iran and Syria. Disinformation entails false health advices, conspiracy theories and narratives about the EU and US failures in the handling of the crisis. It is aimed at sowing confusion and misperceptions within the public and undermining the effectiveness and credibility of Western institutions.

In conclusion, foreign interferences are a major challenge for democracy. Election interferences, cyber-attacks, funding of political parties and disinformation campaigns endanger the functioning of democracy. Institutional and policy responses have been varied and multi-faceted. Both the EU and NATO have invested significant resources in strategic communication, setting up dedicated task forces to debunk, monitor and raise awareness of disinformation.

As a way forward, the article makes 11 specific recommendations to further strengthen the action of the EU and counter the threat of foreign interferences more effectively; going from 'Be quick', to 'set up communication structures' and 'Revise the Code or Practice'.

4.8. Transparency of the elections

4.8.1. Artificial Intelligence, data protection and elections (Ref. no. 38)

Reference title: European Parliament Research Centre. 2019. Artificial Intelligence, data protection and elections

Key words: *Artificial Intelligence, elections, data protection, personal data, political advertising, social media, disinformation, data surveillance*

The publication briefly elaborates on the importance of the set of European Union (EU) initiatives to strengthen free and fair elections, following Facebook/Cambridge Analytics (CA) case in 2018.

The publication aims to reinforce the importance of data protection rules in EU – especially in pre-EU elections year - while explains CA misuse of Facebook users' data to manipulate and influence their vote on United Kingdom (UK) and United Sates of America (US) polls.

In terms of methodology the publication contextualises the CA case and lists EU measure packages in reaction to that case from 2018 towards.

The publication discusses on the process of elaboration of EU initiatives debated and taken aiming to prevent similar social media influence of UK and US election in the 2019 EU elections.

Amongst other actions, the publication mentions the creation of the Social Media Working Group responsible for a long-term strategy on investigations on the collection and use of personal data by social media. It also mentions the opinion emitted by the European Data Protection Supervisor (EDPS), which contains a call for a more aggressive EU position on the topic, having some expert suggesting real enforcement of data protection rules and imposing its compliance such on limitations to automated profiling.

During 2018, EU institutions were particularly active in investigations on CA case and Facebook CEO was invited to meet several Members of the European Parliament (EP), however the result of this appointments were unsatisfactory due the answers provided. In the same year, the EP approved a resolution[96] which called for Member States collaboration with online platforms to "increase awareness and transparency regarding elections".

Although Data Protection rules are an important instrument to ensure digital technologies are compliant with democratic values, the publication reflects on the fact that alone, this instrument could be not enough. Thus, suggests that privacy and competition law should be intertwined based on a published article from EDPS[97].

The EU efforts culminated into a package of several measures such European Commission Communication on "Tackling online disinformation"; the establishment of a European network of fact-checkers or the "Code of Practice on Disinformation". Another important package was implemented in September 2018, in order to prevent the impact of disinformation based in misuse of voters' data on the electoral process such financial sanctions[98] to European political parties; a Recommendation to Member States for an election cooperation network[99] and a Guidance[100] "on the EU data protection law in the electoral context".

[96] European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection – available at https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_EN.html?redirect

[97] https://edps.europa.eu/sites/edp/files/publication/19-03-11_cpi_buttarelli_en.pdf

[98] 2018/0336(COD) Protection of personal data in the context of elections to the European Parliament

[99] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

[100] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

In conclusion and as a way forward, the publication underlines the importance of privacy and data protection to fundamental rights and freedom, thus suggesting that the use of automated and algorithm based decision-making practices requires further transparency, shared accountability from various actors and ethical considerations.

4.8.2. The impact of the information disorder (disinformation) on elections Ref. no. 81)

Reference title: European Commission for Democracy through law (Venice Commission). 2018. The impact of the information disorder (disinformation) on elections

Key words: *elections, disinformation, information disorder, online media, freedom of expression, free elections, political parties*, *electoral campaigns*, *digital advertising*

The brief consists in a support document to a prior "Study on the role of social media and the internet in democratic development"[101] prepared by José Luis Vargas Valdez (Valdez-Study).

The brief aims is twofold, first to provide input on relevant standards and other instruments related to elections and internet from the Council of Europe (CoE) and secondly to suggest additional contributions to the Valdez-Study on critical elements regarding securing the right of free elections within changed communicative spheres.

In terms of methodology, first elaborates on the (potential) impact of information disorder on elections, it then addresses the right to free elections within the instruments of CoE and finally, presents CoE instruments and standards related to elections and media.

The brief starts by identifying how during 2016 US presidential elections and UK Brexit referendums' the i) lack of rules and regulations on paid adverting and ii) the collecting and processing of voters' personal data used for election purposes without their knowledge, together represented a kind of the starting point of a more visible impact of digital environment on electoral process. The brief continues with pointing out the challenge that new forms of digital advertising (less transparent) pose on prior established legislative limits on campaign finance. This shift from advertising on traditional media channels to internet also brought a new and diverse way of transmitting political messages to voters leading to the stage of *information disorder (*disinformation*)* on different platforms. Moreover, the operators of such platforms or *internet intermediaries* by giving access, hosting, facilitating the creation and sharing of content, become owners of the flow of information availability and accessibility, in other words, the gatekeepers of information. To that extend, the brief

[101] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-LA(2018)001-e

continues mentioning how individuals depend enormously on these social media platforms' criteria on content management and moderation, while these platforms cannot guarantee the previous role of traditional media regarding "editorial filter accuracy, fact-checking and separation of fact and opinion".

The brief than proceeds to conceptualising disinformation based on the CoE Information Disorder Report 2017[102] which provides the conceptual framework to comprehend this multifaceted phenomenon wrongly described as "fake-news" and defined as following: misinformation: stands for sharing false information, but without the intent of causing harm; disinformation: stands for knowingly sharing false information with the intent to harm; mal-information: describes genuine information shared with the intent to cause harm, often by disclosing information from the private sphere into the public sphere.

Disinformation tactics and digitalisation of electoral communication in general are a threat to democratic elections. To that extend, the brief addresses the Recommendations from the CoE Election Study 2017[103] such setting up responsibilities of internet intermediaries and regarding political campaigning on their platforms and transparency on the use of personal data during electoral campaigns.

Furthermore, the brief presents two interesting academic findings. The first academic research focus on the possible reason behind the acceleration of disinformation: if caused by algorithm or human behaviour, which revealed to be the latest, against conventional assumption. The second, shows that there are false information spread with specific intention to influence election results, where the manipulation of search results by search engine providers can generate a "search engine manipulation effect" which can shift the voting preferences of indecisive voters by 20%".

The brief explores the instruments and standards of CoE regarding elections and media. Concerning standards, these were set in two main areas. First in the funding of political campaigns, where following existing Recommendations[104], the standards to be applied, amongst others, include severe rules (banning or limiting) on private donations such from foreign donors; limits to political parties' spending on election campaign and provisions on transparency regarding political parties' expenses.

Second areas is related to media coverage on electoral campaigns. Standards on this area attempt to "enable a communication context", where Member States should guarantee to citizens the access to accurate and correct information on political parties and to support their democratic choice.

In conclusion, it is recognised the importance of social media intermediaries as a positive facilitator of public and democratic debate. On the other side, it also held these intermediaries accountable for safeguarding the respect for fundamental rights such the right to free elections on their platforms.

Finally, the brief recommends a revision of rules and regulations on political advertising namely in the access to media and related to spending; Internet intermediaries should be held accountable for transparency and access, comprising access to paid political advertising in order to discourage illegal foreign

[102] https://rm.coe.int/information-disorder-report-november-2017/1680764666
[103] Council of Europes' Study on the use of internet in electoral campaigns. 2017. https://rm.coe.int/use-of-internet-in-electoral-campaigns-/16807c0e24
[104] PACE Recommendation 1516 (2001) on the financing of political parties; Recommendation Rec (2003)/4 of the committee of Ministers to member states on common rules against corruption in the funding of political parties and electoral campaigns

and national interference on elections; support to quality journalism and, finally, empowerment of voters on a critical evaluation of electoral communication avoiding exposure to disinformation of other type of harmful information

4.8.3. Joint Report on Digital Technologies and Elections (CDL-AD(2019) (Ref. no. 87)

Reference title: European Commission for Democracy Through Law (Venice Commission). 2019. Joint Report on Digital Technologies and Elections (CDL-AD(2019)

Key words: *elections, social media, disinformation*

The report analyses the use of digital technologies during electoral processes

The report discusses that digital (or "new") technologies and social media have revolutionised the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting - fundamental rights. People who engage in social media may use the internet to organise and demand better services, more transparency and meaningful participation in the political arena. Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism. This digital transformation is recasting the relation between states and citizens.

Currently we are witnessing the parallel proliferation of information and its pollution at a global scale. The internet-based services have enriched and diversified news sources, facilitating individuals' access to information and their decisions on the most crucial matters in democracy, notably on the choice of their legislature. However, at the same time, a new era of information disorder distorted the communication ecosystem to the point where voters may be seriously encumbered in their decisions by misleading, manipulative and false information designed to influence their votes. This environment potentially undermines the exercise of the right to free elections and creates considerable risks to the functioning of a democratic system.

Digital technologies have reshaped the ways in which societies translate the will of the people into votes and representation, and they have to a large extent changed political campaigning. Even though the internet fosters some aspects of the democratic contest, it also hampers them. The worldwide pervasiveness of digital technologies has moved the arena of democratic debate to the virtual world, raising many questions about their influence on voter turnout and the need to survey and regulate online social behaviour. Moreover, adequate protection against cyber warfare needs to be ensured.

As a conclusion, the holding of democratic elections, hence the very existence of democracy, is impossible without respect for human rights, particularly the freedom of expression and of the press and the freedom of assembly and association for political purposes, including the creation of political parties. Respect of these freedoms is vital particularly during election campaigns. Restrictions on these fundamental rights must comply with the European Convention on

Human Rights and, more generally, with the requirement that they have a basis in law, are in the general interest and respect the principle of proportionality. Clear criteria for balancing the competing rights should be set out in the legislation and effectively implemented through electoral and ordinary justice mechanisms.

As a way forward, the borderless nature of the internet and the private ownership of the information highways render the current challenges to democracy and electoral processes particularly complex. International cooperation and involvement of the relevant private actors are therefore indispensable to face these challenges and to ensure the right to free elections and the functioning of democracy in the future.

4.8.4. Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final (Ref. no. 101)

Reference title: European Commission. 2018. Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final

Key words: *transparency, recommendations, political advertising, cyberattacks, awareness raising, disinformation, personal data protection*

This Recommendation outlines the main possible concerns ahead of the European Parliament elections in 2019 to which Member States should be cautious.

In particular, the Recommendation puts forward a number of risks such as online targeting citizens with political advertisements and communications, often in a non-transparent way, unlawful processing of personal data, disinformation campaigns, cyber incidents and attacks targeting electoral processes, campaigns, political party infrastructure, candidates or public authorities' systems. To fight these, the Commission recommends further enhancing transparency of paid online political advertisements and communications vis-à-vis citizens of the Union ahead of the elections to the European Parliament. The Recommendation also refers to the Code of Practice on Disinformation which, at the time of its adoption, was not yet finalised. However, the we find the main points the Code now aims to address, already in the Commissions' recommendations. For instance, that Member States should promote active disclosure of the source of funding of a paid online political advertisement and communication during electoral campaigns, while fully respecting freedom of expressions. Also, political parties, foundations and campaign organisations should also undertake further transparency commitments.

Additional recommendations include (1) monitoring by Member State authorities with competences in electoral matters of unlawful online activities, (2) cooperation with other authorities likes data protection authorities and authorities in charge of cybersecurity, (3) enforcement of existing rules and imposition of sanctions, if necessary; (4) supporting national election cooperation networks to provide alerts on potential threats, to exchange information and best practices and to liaise on the application of electoral rules in the online world and on enforcement actions. The Commission also recommends enabling of

sanctions imposition on political parties or political foundations that take advantage of infringements of data protection rules to influence the outcome of elections. Member States should also engage in awareness raising activities with third parties, including media, online platforms and information technology providers to increase transparency of elections.

4.8.5. Protecting Electoral Integrity in the Digital Age (Ref. No 105)

Reference title: Kofi Annan Commission on Elections and Democracy in the Digital Age. 2020. Protecting Electoral Integrity in the Digital Age

Key words: *electoral integrity, disinformation, social media platforms, capacity-building, actions by platforms, actions by public authorities, building norms*

This Kofi Annan Commission prepared this report considering the fundamental elements of digital technology which will have a uniquely detrimental, or positive, impact on democracy and electoral processes. The report examines how the use of technology in elections can be made transparent and accountable and what opportunities and incentives digital technology can offer voters, especially young people, to engage in democratic processes. Finally, it assesses the role and impact of political finance in the deployment and use of digitally based electoral strategies and instruments.

The first objective of the report is to identify and frame the challenges to electoral integrity arising from the global spread of digital technologies and social media platforms. It also aims to develop policy measures that address these challenges but also to highlight the opportunities that technological innovation offers for strengthening electoral integrity and political participation. Finally, the report aims to define and articulate a programme of advocacy to ensure that the key messages emerging from the Commission are widely diffused and debated around the world.

In terms of methodology, in its report the Commission puts forward a series of recommendations to strengthen the capacities of electoral integrity authorities, to build norms encompassing shared understandings on the acceptable use of digital technologies in elections, and to encourage action by public authorities and technological companies to enhance electoral integrity. These recommendations originate from one of the main conclusions of the report: all relevant stakeholders – tech and digital platforms, governments, electoral authorities, traditional media and citizens – have a critical role to play in strengthening electoral integrity.

In particular, the report starts with acknowledging the positive effects of ICT technologies on democracy and electoral integrity, based on research in Africa and Latin America. Specifically, technologies effect positively political engagement by increasing voting, joining social movements, and coordinating political action. They are also an important medium for political conversation, information sharing, and democratic deliberation. However, the report focuses on the challenges that these technologies pose on democracy, specifically - polarisation, hate speech, disinformation, new forms of political advertising, and foreign interference - and addresses each one of them with specific recommendations for a way forward.

In conclusion and as a way forward the report puts forward the idea that in order to protect electoral integrity in the digital age, we will need to strengthen the capacities of the defenders of electoral integrity and build shared norms around the acceptable use of digital technologies in elections. Technology platforms and public authorities must act to bolster electoral integrity. In terms of building capacities, the specific recommendations include collaboration, information sharing and investment (by public authorities, international organisations, philanthropic foundations, and civil society) in tech talent and digital capacity, media efforts, and election management bodies that protect and promote electoral integrity. In addition, international technical assistance to help (election management bodies EMBs) to defend their election against international interference, hacking and other technical threats, should also be envisaged. In terms of building shared norms, the report endorses the call by the Transnational Commission on Election Integrity for political candidates, parties, and groups to sign pledges to reject deceptive digital campaign practices (such as use of stolen data or materials, use of manipulated imagery such as shallow fakes, deep fakes, and deep nudes, the production, use, or spread of falsified or fabricated materials, and collusion with foreign governments and their agents who seek to manipulate the election). Other recommendation in this regard include: 1) the conclusion of an international convention to distinguish legitimate cross – border assistance (by foreign governments) from illicit or unlawful interventions; 2) creation of a critical electronic electoral technologies (EET) infrastructure by democratic governments; 3) commitment by vendors of election equipment and services to a code of conduct to guarantee their products are secure, and their business practices protect the rights, privacy and data of citizens in their client countries, and adhere to honest, transparent practices in procurement and 4) creation of norms and standards for transnational political campaign consultants, including public relations and strategic communication firms, and digital marketers.

Last but not least, recommendations include the necessity of actions to be taken by public authorities and digital platforms. For instance, the former should ensure an increased legislative intervention regarding political advertising and organise digital media literacy campaigns. On the other hand, platforms should ensure more transparency and give researchers access to more platform-controlled data to allow studying the effects of polarisation and the pathology of the social platform ecosystem. They should also develop early warning systems for election-related disinformation, foreign interference, hate crimes, threats to women, violence, and voter suppression.

4.8.6. Protection of personal data in the context of EP elections (Ref. no. 110)

Reference title: Yannakoudakis. EESC. 2018. Protection of personal data in the context of EP elections

Key words: *personal data, EP elections*

The opinion focuses on the verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament.

Background information on the opinion: events have shown the risks for citizens of being targeted by mass online disinformation campaigns with the aim of discrediting and delegitimising elections. Peoples' personal data are also believed to have been illegally misused to affect the democratic debate and free elections. Ahead of the 2019 elections to the European Parliament, the European Commission has proposed a number of focused changes to Regulation No 1141/2014 on the statute and funding of European political parties and European political foundations. The proposed changes would allow sanctioning of European political parties or foundations that influence or attempt to influence the elections via an infringement of data protection rules. The proposal also sets out a procedure to verify whether a data protection breach identified by a national data protection supervisory authority has been used to influence the outcome of EP elections.

The EESC is of the opinion that the Authority for European political parties and European political foundations (APPF) is currently understaffed. The EESC therefore supports the proposal to staff the APPF in a permanent way and to confer the powers of an appointing authority on the director of the Authority, as it is essential that it has enough manpower to monitor the elections properly. The director of the Authority is appointed via the procedure as stated in Article 6(3) of the Regulation. He/she is independent and not accountable to the EU institutions. He/she does have to submit an annual report to the European Commission and the European Parliament, and it might be prudent to give the EP the power to question this report and to vote on it. This would ensure that the Authority has some accountability and that the process is more transparent.

Data use and social media have fundamentally changed the way political parties' campaign in elections, allowing them to target potential voters. This development has resulted in a greater push in social media as a form of influencing people's voting intentions. The EESC would expect the Authority to look at areas where data infringement might take place and suggest ways to stop this and put checks and balances in place to secure data protection and use of data is within well-defined parameters. The EESC suggests that greater clarification is needed to constitute what is an attempt to influence the elections via an infringement of data protection rules. The setting up of a working group consisting of Member State DPAs and the Authority should be examined, with an aim of establishing best working practice between both the Authority and the DPAs as data protection has no borders within the EU.

4.8.7. Challenging Data Exploitation in Political Campaigning (Ref. no. 112)

Reference title: Privacy International. 2020. Challenging Data Exploitation in Political Campaigning

Key words: *data exploitation, data protection, political parties, political campaigning*

The document is about data exploitation in political campaigning.

The document aims to identify actions for governments, regulators, legislators, political parties and companies to help prevent data exploitation in political campaigning.

The document discusses in the first section that around the world, laws and regulatory mechanisms are proving insufficient to provide safeguards for the way that digital campaigning has developed. Where frameworks are in place, they suffer from a vast enforcement gap. Legislators and governments must develop, strengthen and enact updated legal frameworks. Those must then be enforced by those empowered to do so, courts, oversight bodies and regulators.

The second section seeks to complement the above, with specific recommendations (some of which may already be legal requirements) to political parties and campaign groups as to how to avoid data exploitation.

The third section aims to complement the requirements of strong legislation, namely data protection and electoral law, by providing specific recommendations (some of which may already be legal requirements) for the range of companies that play a role in the digital campaigning ecosystem.

In conclusion, Privacy International considers that there are certain baseline safeguards that should be in place. The first one is that more transparency is needed from all actors involved in digital political campaigns, in order to shed much needed light on data gathering practices, how such data is used, in particular for profiling, and then how such profiles are used to target messaging. Secondly, transparency is needed for voters, for regulators and for researchers. All online and offline advertisements should be publicly available, easily searchable and machine-readable, with detailed information including who received what, why and under which circumstances. Thirdly, comprehensive data protection laws must be implemented and enforced. Any loopholes that can be exploited by political campaigns must be closed. Fourthly, electoral laws need to be updated for the digital age. They must reflect that digital political campaigning takes place outside the strict electoral period and require detailed and timely reporting on campaign advertising and financing. Fifthly, these legal frameworks must provide effective redress (both individual and collective) and meaningful sanctions if they are violated. Lastly, regulators, judicial and other supervisory/oversight authorities, in particular those responsible for data protection and electoral law, must have sufficient independence and adequate resources (both technical, human and financial) to enforce the law.

4.8.8. Guide for civil society on monitoring social media during elections (Ref. no. 131)

Reference title: Democracy Reporting International. 2019. Guide for Civil Society on Monitoring Social Media during elections

Key words: *monitoring social media, elections, disinformation, civil society*

This guide analyses how different stakeholders such as tech experts, tech journalists, academics or civil society, among others have started experimentally monitoring social media**.** Thus, this guide is a publicly available resource for any organisation that aim to observe social media in elections.

In terms of methodology, the guide is divided in four main chapter addressing challenges of social media to observers of elections and its impact on elections itself.

The guide defines social media as websites and computer programs that allow people to communicate and share information online (using a computer or a mobile phone). Social media monitoring in elections can be seen as an extension of traditional election monitoring. However, traditional media usually encompasses a limited set of actors (TV and radio stations, and newspapers).

The advent of social media allowed an ongoing exchange of amounts of information incomparably larger than before. Information is also passing around the globe in a much faster way and is potentially reaching massive audiences. Furthermore, information production is larger than before, but users frequently consume it focusing on headlines, pictures or videos. Therefore, Social media brings a new challenge to election observers, in the sense that in order to monitor social media, election observers have to analyse a much higher amount of data and be prepared for unexpected and swift developments.
The second chapter elaborates on social media's impact on the electoral process. Such impact could be related to how content shared on social media might influence political behaviour in different levels and periods (short, middle and long term). It brings threats to democratic debate, which the guide divides in three sources, the three M's: the *message* which refers to the content of the message and could bring issues of what is permitted speech; *messenger* which concerns to the sender/origin of the message and brings issues on the authenticity and legitimacy and *messaging* which refers to the form of distribution of the message and also link to problems of authenticity. Moreover, the guide notes that social media phenomena such as disinformation, advertising or hate speech have particular characteristics and influence election differently.

The third chapter develops on how to monitor social media and presents a methodological approach. The monitoring preparation effort should start between4-5 months before the elections and the coverage should include the campaign period and the pre-electoral and post-electoral period.
A final chapter advises on how and when to publish the reports from social media monitoring. The data collated to produce such finding should be distinguish between public and private data, where the private data should be managed ethically, moreover, made anonymous and untraceable.

In conclusion, the guide offers a comprehensive list of activities, steps, periods and aspect to be considered when different organisations and stakeholders, especially civil society organisations, proceed with the monitoring of social media during elections.

4.8.9. The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age (Ref. no. 199)

Reference title: Kofi Annan Foundation. 2020. The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age

Key words: *social media, electoral integrity, online disinformation, microtargeting, campaigning,*

The document aims to identify and frame the challenges to electoral integrity arising from the global spread of digital technologies and social media platforms. Develop policy measures that address these challenges, and which also highlight the opportunities that technological innovation offers for strengthening electoral integrity and political participation. Define and articulate a programme of advocacy to ensure that the key messages emerging from the Commission are widely diffused and debated around the world

The document discusses that new information and communication technologies (ICTs) pose difficult challenges for electoral integrity. In recent years foreign governments have used social media and the Internet to interfere in elections around the globe. Disinformation has been weaponized to discredit democratic institutions, sow societal distrust, and attack political candidates. Social media has proved a useful tool for extremist groups to send messages of hate and to incite violence. Democratic governments strain to respond to a revolution in political advertising brought about by ICTs. Electoral integrity has been at risk from attacks on the electoral process, and on the quality of democratic deliberation. The relationship between the Internet, social media, elections, and democracy is complex, systemic, and unfolding. Our ability to assess some of the most important claims about social media is constrained by the unwillingness of the major platforms to share data with researchers

4.8.10. How to take a "gold standard" approach to political advertising transparency and policy (Ref. no. 184)

Reference title: Who Targets Me. 2020. How to take a "gold standard" approach to political transparency and policy

Key words: *political advertising, campaigns, transparency, Facebook ad library, social platforms*

This article develops on six proposed "gold standard" for the improvement of the transparency of the online political advertising.

In terms of methodology, the article briefly introduces some issues related to political advertising, followed by explanation of the six elements to be considered in the increasing of transparency on political advertising.

The article discusses at first on how Facebook created an ad library which even though is still an imperfect tool it is an important starting point and useful tool. The article than points out how the absence of government regulations allowed private companies to set up their own rules.

Following the idea that more transparency is needed in political advertising, the article set six "goal standards" to reach such transparency.

First important standard is related to increasing ad library data quality for accountability and research. In order to increase data quality, amongst other aspects, should be published all political ads in their entirely and its spending; publish targeting information so the methods being used by campaigns are transparent. This element includes the process of labelling ads as to whether they are using specific language targeting, amongst other information.

Secondly, there should be improvements on auditing tools and processes. This encompasses social platforms to provide detailed descriptions of ad approval processes and allow annual independent audits/verification; require annual re-verification of political advertisers; to provide users with a summary of the political ads they have seen in the last six months; allow them to download/share these lists in a privacy compliant way.

The third aspect noted in the article for increasing transparency within political advertising is related to elections management. This includes activities and actions such as participate in regular meetings with academia, journalists, regulators and civil society to discuss emerging and outstanding issues and standardise and publish the list of advice provided to political campaigners on use of platforms, support arrangements, processes, advice, consultancy and so on.

The fourth "gold standard" is directly related to the Ad Library standards. On this matter, the suggestions for improvements are, amongst others, to work with other stakeholders to develop a universal ad library, fed by API data from many advertisers and platforms and allow trusted advertising companies to submit data to ad libraries, based on a common standard.

The fifth standard for the improvement of transparency in political advertising is linked to further engagement with alternative regulatory proposals, especially on topics such as Reducing the number of ads available to advertisers, removing social features from political ads and How to handle anonymity for campaigners in repressive/dangerous environment.

Lastly, the article suggests that should be an active monitoring of the new practices.

In conclusion, the article proposed concrete suggestions wrapped in six main "gold standards" for increasing transparency on the political advertising. As the interests of civil society, private companies, political parties and other stakeholders are considerable different, the proposed six "gold standards" acceptance will depend on the discussion and balance of the trade-offs between those stakeholders.

5. Annex: List of all References

No.	Author. Year. Title	Summary	Relevance	Reasoning	Category[105]
1.	Dobber, Fathaigh, Zuiderveen Borgesius. 2019. The regulation of online political micro-targeting in Europe	This paper focuses on the following questions: What is online political micro-targeting, and what are its promises and threats? It combines insights from both a legal and social science perspective. The authors focus mostly on European countries and the US. Section 2 Introduces the practice of online political micro-targeting. Section 3 discusses the promises of online political micro-targeting, and Section 4 the threats. Section 5 discusses why the threats, while serious, should not be overstated. Section 6 explores how policymakers in European countries could intervene and sketches some problems they would encounter if they wanted to intervene. Section 7 concludes that more research and debate about online political micro-targeting is necessary.[106]	High	Discusses use of new technologies and techniques (in particular, online micro-targeting) in political campaigning, which is an activity of the first stage of the electoral process, therefore directly falling within the scope of this study.	Preparation
2.	Centre for Public Impact. 2016. The Public Impact Fundamentals Helping governments progress from idea to impact	The paper discusses a framework of concepts, drivers and tools that any government has at its disposal to improve policy outcome.[107]	Low	Cf. summary	Horizontal
3.	European Commission. 2018. Securing free and	The paper sets the situation on free and fair European elections of 2019, exposing the challenges and threats. It	High	Discusses policy priorities and measures to defend free and fair elections.	Horizontal

[105] Indicates if a document elaborates on the use of technologies in a general context, or it analyses use of technologies at a horizontal level for all stakes of the electoral process, and /or to the specific stages of electoral process, i.e. preparatory, voting and post-elections

[106] Summary prepared by the contractor

[107] Summary prepared by the contractor

	fair European elections A Contribution from the European Commission to the Leaders' meeting	then discusses policy priorities and measures for the defence of free and fair European elections.[108]			
4.	European Regulators Group for Audiovisual Media Services. 2019. Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation	The report contains the outcome of a follow-up analysis of the major social media companies - Google, Facebook, Twitter - with regards to its compliance with the commitment on the Code of Practice on disinformation, on different aspects of political and issue-based advertising during the European elections of May 2019, and. Finally, it draws conclusions of the monitoring and challenges encountered.[109]	High	Monitors compliance of online platforms to the commitment of Code of Practice on disinformation	Preparation
5.	European Parliamentary Research Service. 2019. Regulating disinformation with artificial intelligence	This study examines the consequences of the increasingly prevalent use of artificial intelligence (AI) disinformation initiatives upon freedom of expression, pluralism and the functioning of a democratic polity. The study examines the trade-offs in using automated technology to limit the spread of disinformation online. It presents options (from self-regulatory to legislative) to regulate automated content recognition (ACR) technologies in this context. Special attention is paid to the opportunities for the European	High	The use of new technologies (AI) in the fight against disinformation.	Preparation

[108] Summary prepared by the contractor
[109] Summary prepared by the contractor

		Union as a whole to take the lead in setting the framework for designing these technologies in a way that enhances accountability and transparency and respects free speech.[110]			
6.	Committee of experts on media pluralism and transparency of media ownership. 2018. Internet and electoral campaigns - Study on the use of internet in electoral campaigns	This study was conducted on request of the Committee of Ministers to 'carry out a study on a possible standard-setting instrument on media coverage of elections with particular regard to the use of internet in electoral campaigns. The study analyses the key concepts of fair, clean and clear elections and explains the context and evolution of internet advertising for political objectives. The study concludes with a list of recommendations to existing policies of Member States on the organisation and regulation of elections.[111]	High	Cf. Summary	Preparation
7.	European Regulators Group for Audiovisual Media Services. 2018. Internal Media Plurality in Audiovisual Media Services in the EU Rules & Practices	The report discusses Media Plurality in general, and its relation to elections in a broader sense. The changing media landscape and cross-border dimensions are also analysed. "The report is based on data gathered from 31 national regulatory authorities (28 ERGA members + 3 observers) through a comprehensive questionnaire. It makes no recommendations but strives to ensure that policymakers contemplating possible interventions are as fully informed as possible."	Medium	Cf. summary	Preparation

[110] Summary prepared by the contractor

[111] Summary prepared by the contractor

8.	High Level Expert Group on Artificial Intelligence. 2019. Policy and Investment Recommendations for Trustworthy AI	The study focuses on recommendations for private and public spending in AI projects and research, based on ethical and societal considerations made in a previous study.[112]	Medium	Discusses Trustworthy AI	Preparation
9.	European Commission. 2018. Flash Eurobarometer 464. Fake news and disinformation online?	This paper discusses the levels of trust in news and information, the people's perception of fake news, the public confidence in identifying in misleading news, the people's views on the extent of the problem and views on which institutions and media actors should act to stop the spread of fake news.[113]	High	Discusses the peoples' perception on fake news and the role of the media in it.	Preparation
10.	Avaaz. 2019. Far right networks of deception - Avaaz investigation uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections	The report explores disinformation networks tactics and content in six (6) EU countries (Germany, UK, France, Italy, Poland and Spain) especially on Facebook. It than proposes the adoption of "Correct the record", which consists in a 5-step process that makes corrections verified by independent fact-checkers.[114]	High	Discusses the way new tactics are used in spreading disinformation via social media sources	Preparation

[112] Summary prepared by the contractor
[113] Summary prepared by the contractor
[114] Summary prepared by the contractor

11.	Facebook. 2019. Facebook Baseline Report on Implementation of the Code of Practice on Disinformation	The report provides an overview of Facebook's approach to implementing the EU Code of Practice on Disinformation, including details of Facebook's policies, products, services and actions they take to address the harms caused by disinformation online.[115]	Medium	The report applies to uses of new technologies and techniques (disinformation/fake news) in a broader context, which could be horizontally applied including in the electoral context	Preparation ; Voting; Post-election
12.	European Commission. 2018. EU Code of Practice on Disinformation	This Code of Practice was signed by the major internet companies that disperse information and news amongst citizens of the European Union. For example, Facebook, Instagram etc. are concerned.[116]	High	Cf. summary	Preparation
13.	International Institute for Democracy and Electoral Assistance. 2018. Digital Microtargeting	The paper explains the techniques of digital microtargeting in a political advertising context. It then exposes the legal, financial and ethical considerations before listing the risks.[117]	High	Discusses how Microtargeting is used by parties in election campaigns	Preparation
14.	European Commission. 2018. Tackling online disinformation: a European Approach	The Communication elaborates on the key challenges of online disinformation, its impacts on European democratic values and it aims at setting a framework of principals and objectives to be consider as guide to actions on raising public awareness on disinformation phenomena.[118]	High	Elaborates on main challenges of online disinformation and defines key areas of intervention to mitigate the phenomena impact on the European elections of 2019.	Preparation

[115] Summary prepared by the contractor
[116] Summary prepared by the contractor
[117] Summary prepared by the contractor
[118] Summary prepared by the contractor

15.	European Commission. 2018. Commission guidance on the application of Union data protection law in the electoral context	The paper discusses the problem of data protection in the context of political microtargeting. The objective of the guidance paper is to highlight the data protection obligations, of relevance for elections, by the different actors in the electoral process.[119]	High	Discusses the possibilities and points of attention when microtargeting is used.	Preparation
16.	Alaphilippe et al. 2019. Automated tackling of disinformation Major challenges ahead	This study discusses the phenomenon of mis-, mal- and disinformation. It discusses how social platforms, search engines, online advertising, and computer algorithms enable and facilitate the creation and spread of online misinformation. It also presents current understanding in why people believe false narratives, what motivates their sharing, and how they impact offline behaviour (e.g. voting). This is complemented by a brief overview of self-regulation, co-regulation, and classic regulatory responses, as currently adopted by social platforms and EU countries. The study includes a roadmap of initiatives from key stakeholders in Europe and three case studies on the utility of automated technology in detecting, analysing, and containing online disinformation. The study concludes with the provision of policy options.[120]	High	Discusses uses and impact of new technologies and techniques in the context of the elections process and its stages.	General
17.	High Level Group on Fake News and Online Disinformation.	'The High-Level Group of experts was convened to advice on policy initiatives to counter fake news and disinformation spread online. The final report contains interesting ideas on the definition of disinformation. It analyses the impact of	High	Discusses the concept of 'disinformation' and 'fake news'	Preparation

[119] Summary prepared by the contractor

[120] Summary prepared by the contractor

	2018. A multi-dimensional approach to disinformation	disinformation before elaborating on policy recommendation. It advocates the use of multi-dimensional solutions involving different actors.'			
18.	European Political Strategy Centre. 2018. A Collection of Think Pieces from 35 leading practitioners and experts	The publication assembles the notes of keynote speakers at the 'High-Level Conference on Election interference in the Digital Age: Building Resilience to Cyber-Enabled Threats' on 15-16 October 2018.[121]	Medium	Discusses different views of practitioners and experts on election interference	Preparation
19.	Goldsmith, Ruthrauff. 2013. Case Study Report on Electronic Voting in the Netherlands	Interesting analysis on the 2006 civil society campaign "we do not trust voting computers" in Netherlands and its impact on reversing the use of e-voting system.[122]	Medium	Discuss the impact of distrust in voting machines. The paper dates from 2013, on an issue from 2006. It is not specifically related to the new technologies.	Voting
20.	Russel, Zamfir. 2018. Digital technology in elections - Efficiency versus credibility?	Reference to several examples of innovative technologies introduced in different countries' electoral process discussing their benefits and problems.[123]	High	Discusses the benefits and problems of implemented new technologies for elections	Voting; Post-election
21.	Loeber. 2016. E-voting in the Netherlands past, current, future	'This paper is a case study of a country in which e-voting used to be the general norm until 2006; the Netherlands. Since the abandonment of e-voting, several attempts have been made to reintroduces some form of e-voting. This	Low	Discusses issues related to the electoral process in general, without engaging topics related to uses or impact of new	Voting

[121] Summary prepared by the contractor
[122] Summary prepared by the contractor
[123] Summary prepared by the contractor

		paper describes these attempts and tries to give an insight in the possible future developments of e-voting in the Netherlands. It also analyses which issues play a major role in debates on the use of e-voting.'		technologies and techniques. In addition, the paper dates from 2014, i.e. not entirely up-to-date	
22.	Democracy Reporting International MediaLab ISCTE-IUL. 2019. Disinformation Risks in Portugal's Election - More Brazil Than Europe	'ISCTE-IUL is monitoring social media debate on public Facebook pages and in public WhatsApp groups during these elections, with support from Democracy Reporting International. The risk of online disinformation in Portugal's campaign for parliamentary elections on 6 October is relatively low, even though instances of false information are noted on some Facebook pages. Facebook is by far the most important social media platform in Portugal, as well as YouTube. Messaging services owned by Facebook (Facebook messenger, WhatsApp) have also become highly popular. A number of factors reduce disinformation risks in Portugal: The Portuguese public has a relatively high trust in traditional media (68%) and much less trust in information found on social media (26%). The country is not in the geo-political spotlight, reducing the risk of external disinformation campaigns.'	Medium	Factsheet on disinformation in Portuguese elections.	Preparation
23.	Relatórios OberCom Outubro. 2019. Fake News em ano eleitoral Portugal em linha com a UE	The report makes an overview of European Union (EU) and Portugal positions and approaches against fake news. It also addresses the impact and different tactics of disinformation in electoral campaigning online (more focused on a Portuguese case) and elaborates on three initiatives to mitigate such phenomena such fact-checking, media literacy and collaborative journalism.[124]	High	Discusses on the impact of fake news especially during preparation of elections and presents initiatives to prevent and mitigate based on use of innovative technologies such Artificial Intelligence.	Preparation
24.	European Political Strategy Centre.	This document consists of a newsletter from the in-house think thank from European Commission (EC) European	Medium	Document share information and conferences on Democracy and	Preparation

[124] Summary prepared by the contractor

	2018. EPSC Newsletter Democracy and Governance in the Digital Age	Political Strategy Centre (EPSC) dedicated to Democracy and Governance issues. It advertises on upcoming conferences and authors insights on the matter and share briefly other contributions and activities debating on elections and democratic systems' new challenges such cyber interference.[125]		governance issues. It addresses elections and disinformation impact, though not developing further, as it is not the documents' purpose.	
25.	Štětka et al. 2018. Facebook as an Instrument of Election Campaigning and Voters' Engagement: Comparing Czechia and Poland	'This article examines and compares the character and determinants of Internet users' engagement with political party communication in 2013 and 2015 Parliamentary election campaigns in Czechia and Poland, via the social media. The results suggest that the level of support for a party status is largely independent of the content of the message in both countries. The type of content has, however, an effect on the intensity of criticism by the users, with policy-related subjects generating more negativity than mobilization- or campaign-oriented statuses. Finally, the study points to both gender gaps and gender as a strong predictor of user negativity, as female users – while constituting a minority of participants in both countries – tend to be significantly less negative in their comments towards the home party.'	Medium	Discuss the impact of the use of Facebook for campaigns. It is not specifically related to the new technologies.	Preparation
26.	Schaake et al. 2018. Software Vulnerability Disclosure in Europe - Technology,	'This report puts forward the analysis, policy implications and main recommendations for the design and implementation of a forward-looking policy on software vulnerability disclosure (SVD) in Europe. It is the result of a collective effort led by CEPS, which in September 2017 formed a Task Force on Software Vulnerability Disclosure in Europe, composed of industry experts, representatives of	Medium	Discusses technical aspects and policy implications, and provides recommendations in relation to cybersecurity of information systems which could indirectly be applicable to the electoral process where cybersecurity is an	General

[125] Summary prepared by the contractor

	Policies and Legal Challenges	EU and international institutions, academics, civil society organisations and practitioners (see a list of participants in Annex 1). Meeting on four separate occasions in the period between September 2017 and February 2018, the group explored ways to formulate practical guidelines for governments and businesses to harmonise the process of handling SVD throughout Europe. These discussions led to policy recommendations addressed to member states and the EU institutions for the development of an effective policy framework for introducing coordinated vulnerability disclosure (CVD) and government disclosure decision processes (GDDP) in Europe. Based on its examination of current best practices throughout Europe, the US and Japan, the Task Force recommends implementation of various policies related to SVD. Part of this report concentrates on CVD and Part II focuses on GDDP.'		important aspect to be taken into account for preserving the secrecy and the integrity of the vote as well as for the overall use of information technologies used in the electoral process.	
27.	Martin, Shapiro. 2019. Trends in Online Foreign Influence Effort	'Foreign governments have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation. We analyse 53 distinct foreign influence efforts (FIEs) targeting 24 different countries from 2013 through 2018. FIEs are defined as (i) coordinated campaigns by one state to impact one or more specific aspects of politics in another state (ii) through media channels, including social media, (iii) by producing content designed to appear indigenous to the target state. The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization. We draw on more than 460 media	High	The Report gives an overview of foreign influence efforts that influence social media and news in other countries.	Preparation

		reports to identify FIEs, track their progress, and classify their features.'			
28.	Trechsel, Kucherenko, Silva. 2016. Potential and Challenges of E-Voting in the European Union Study	'This study was commissioned and supervised by the European Parliament's Department for Citizens' Rights and Constitutional Affairs at the request of the AFCO Committee. It addresses the potentials and challenges of the implementation of Internet voting in European Parliament elections. It considers the social, political, legal, and technological implications of its introduction as an alternative to on-paper ballot and builds on the recent experience of previous trials and successful e-enabled elections to issue technical recommendations regarding Internet voting in the European Union.'	High	Discusses potentials and challenges of the implementation of Internet voting in European Parliament elections.	Voting
29.	Chatham House. 2019. Online Disinformation and Political Discourse - Applying a Human Rights Framework	Chapter 2 of this paper clarifies core terms and concepts such as digital platforms, disinformation, personal data, elections and political discourse. Chapter 3 provides an overview of cyber activities that may influence voters with specific examples from different countries. These cyber activities include creation, distribution and maximisation of the influence of disinformation and divisive content. Chapter 4 summarises a range of responses to the issue in different countries (the UK, the US, Germany, France, Singapore), the EU and initiatives of the digital platforms like Facebook, Twitter and Verizon Media in the form of rules and standards. Chapter 5 discusses relevant human rights law, with specific reference to: the right to freedom of thought, and the right to hold opinions without interference; the right to privacy; the right to freedom of expression; and the right to participate in public affairs and vote. Chapter 6 offers some conclusions and sets out	High	Discusses use of new technologies and techniques in political campaigning, which is an activity of the first stage of the electoral process, therefore directly falling within the scope of this study.	Preparation

		recommendations on how human rights ought to guide state and corporate responses.[126]			
30.	Ferreira, Fantin, Pupillo. 2020. CEPS Task Force Evaluation of the HLEG Trustworthy AI Assessment List (Pilot Version)	'As part of the Task Force's in discussions on the evolution of the application of AI in cybersecurity, this report aims at assessing the High-Level Expert Group (HLEG) on AI Ethics Guidelines for Trustworthy AI, presented on April 8, 2019. In particular, this report analyses and makes suggestions on the Trustworthy AI Assessment List (Pilot version), a non-exhaustive list aimed at helping the public and the private sector in operationalising Trustworthy AI. The list is composed of 131 items that are supposed to guide AI designers and developers throughout the process of design, development, and deployment of AI, although not intended as guidance to ensure compliance with the applicable laws. The list is in its piloting phase and is currently undergoing a revision that will be finalised in early 2020. This report would like to contribute to this revision by addressing in particular the interplay between AI and cybersecurity. This evaluation has been made according to specific criteria: whether and how the items of the Assessment List refer to existing legislation (e.g. GDPR, EU Charter of Fundamental Rights); whether they refer to moral principles (but not laws); whether they consider that AI attacks are fundamentally different from traditional cyberattacks; whether they are compatible with different risk levels; whether they are flexible enough in terms of clear/easy measurement, implementation by AI developers and SMEs; and overall, whether they are likely to create obstacles for the industry.'	Medium	Discusses technical aspects in the area of cybersecurity without specific mentions and references to the elections process and its stages. However, the paper is of horizontal nature, as its findings are applicable to all fields of application of the AI technology, including in the electoral context.	General

[126] Summary prepared by the contractor

31.	Appelman et al. 2019. The spreading of disinformation through internet services and the regulation of political advertisements	'The research is based on seven research questions submitted by the Ministry of Interior. The questions vary from very general to very specific, but all relate to the broader problems surrounding disinformation, the existing legal framework and the possibility of further regulation. These seven questions are therefore all answered in the context of the broad analysis in the report of the relevant legal framework for the dissemination of disinformation through internet services and possible regulatory options.'	High	Discusses how the dissemination of disinformation affects society. It looks into the existing legal framework and how this can be regulated in the future.	Preparation ; Voting; Post-election
32.	Richter. 2019. Disinformation in the media under Russian law	'This article by Andrei Richter provides an overview of the legislation and case law concerning disinformation in the Russian Federation. It builds upon the chapter "Russian Federation" in an earlier publication by the European Audiovisual Observatory, "Media reporting: facts, nothing but facts?" It covers five specific cases where disinformation is deemed illegal. These are: 1) a required reliability of information "essential for the public" on popular news aggregators; 2) a most recent general ban on unreliable "socially significant" online information; 3) a ban on false information about the activity of the USSR during the Second World War; 4) a ban on knowingly false accusations of officials of having committed extremist actions; and 5) prohibition of untrue advertising. The article also makes reference to the recent practice of the national self-regulation body on disinformation in the media.'	Medium	Discusses disinformation under Russian law, which does not directly relate to the scope of the study, however, can be used for comparative purposes.	General
33.	Council of Europe. 2017. Media Regulatory Authorities and hate speech	This Reginal publication resulting from JUFREX project (Reinforcing Judicial Expertise on Freedom of Expression and the Media in south-east Europe), aims to contribute to a wider understanding of the concept of hate speech while providing recommendations and identifying mechanisms to prevent and tackle this problem. The publication first explores the concept of hate speech and then analyses	High	The publication does not extensively elaborate on the use of new technologies; however, it offers interesting analysis on countries that experienced cases of hate speech techniques throughout some stages of the	Preparation

		cases of hate speech in seven (7) Europe southeast region countries (Albania, Bosnia and Herzegovina, Croatia, Macedonia, Montenegro, Kosovo and Serbia). These cases occurred in media outlet and online media. This publication also compiles in final annexes "legal framework overviews of participating countries" and "Relevant case-law of the European Court of Human Rights (ECHR)". Finally, it represents a useful tool to further activities for various relevant stakeholders such as media regulatory bodies. [127]		electoral process, throughout different channels and shares the evaluation and decisions from each countries' NRAs	
34.	European Parliament, Council of the European Union. 2014. Regulation (EU, EURATOM) No 11412014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations	The Regulation aims to create a specific legal, financial and regulatory system for European political parties and European political foundations. It increases their visibility, recognition and effectiveness by giving them a European legal personality and greater funding flexibility. The Regulation creates the independent Authority for European Political Parties that registers, verifies and may impose penalties on European political parties and foundations. It also sets the conditions for registration and de-registration and the obligation for transparent spending of EU funded campaigns.[128]	High	Horizonal reference, EU legislation on funding of political parties.	EU legal and policy framework

[127] Summary prepared by the contractor

[128] Summary prepared by the contractor

35.	Fletcher et al. 2018. Measuring the reach of fake news and online disinformation in Europe	The purpose of this RISJ factsheet is to provide top level usage statistics for the most popular 300 sites that independent fact-checkers and other observers have identified as publishers of false news and online disinformation in two European countries: France and Italy. The factsheet focuses on measuring these sites' reach, attention, and number of interactions on Facebook. It compares these figures with equivalent data for a small selection of the most widely used French and Italian news brands.[129]	Medium	Does not discuss electoral process and new technologies used therein, however in could be used as good source of information for preparation of stakeholder consultations.	General
36.	European Commission. 2019. Report on the implementation of the Action Plan Against Disinformation	'The report by the Commission and the High Representative provides a first assessment of the progress achieved so far and sets out the main lessons for the future. It explains in more detail how the Action Plan and the Elections Package helped to fight disinformation in the context of the European elections. It is also the contribution of the Commission and the High Representative to the European Council meeting on 20-21 June 2019.'	High	Report on disinformation in the European Elections of 2019.	Preparation
37.	Boucher. 2016. What if blockchain technology revolutionised voting How blockchain technology could be used for e-voting	This article provides a brief explanation on how blockchain technology could be used in electronic voting and what its potential impacts and further developments are.[130]	High	Discusses use of new technologies and techniques (in particular, blockchain) in electronic voting, which is an activity of the second stage of the electoral process, therefore directly falling within the scope of this study.	Voting

[129] Summary prepared by the contractor

[130] Summary prepared by the contractor

38.	European Parliamentary Research Service. 2019. Artificial intelligence, data protection and elections	The paper briefly elaborates on the importance of the set of European Union (EU) initiatives to strengthen free and fair election, following Facebook/Cambridge Analytics (CA) case in 2018. In conclusion and as a way forward, the paper underlines the importance of privacy and data protection to fundamental rights and freedom, thus suggests that the use of automated and algorithm based decision-making practices requires further transparency, shared accountability from various actors and ethical considerations.[131]	High	It discusses on EU initiatives taken following Cambridge Analytics case on UK and US polls, in order to prevent similar influence on 2019 EU election.	Preparation ; Voting; Post-election
39.	European Citizens' Rights Involvement and Trust. 2013. Guidelines for European Citizens' Rights, Involvement and Trust	The European Union launched a Year of Citizens in 2013 to celebrate the 20th anniversary of the inclusion of European citizenship in the Maastricht Treaty. As a result of the case law of the European Court of Justice, a comprehensive legal framework is in place governing free movement. This is the first right of the European citizen. European citizenship has now become an established fact in Europe, "destined to become the fundamental status of nationals of Member States" in the words of the European Court of Justice. But what of its future in a period of doubt about the European project? What is the relationship between a wider European citizenship and EU citizenship? Is this new form of citizenship post-national and self-standing, and if not, how does it relate to national citizenship? What else but a transnational citizenship holds Europe together and if that is becoming more evident as a result of the economic crisis, how can a more full-scale European citizenship emerge? The	Medium	Discusses rights of EU citizens in general	General

[131] Summary prepared by the contractor

		aim of ECIT's Guidelines is to stimulate debate on such questions.			
40.	International Institute for Democracy and Electoral Assistance. 2018. Online Political Crowdfunding, Political Party Innovation Primer 2	Small donations to parties from individuals in the form of membership fees and physical donation tins, recently called 'crowdfunding', are both community-building and money-making exercises. This Primer introduces the concept of online political crowdfunding and the different forms that are currently used by political parties. The online crowdfunding can be seen as a more transparent way for parties to give an insight on their funding's and it gives possibilities to the empowerment of excluded and less influential groups.[132]	Medium	Discuss the impact of the use of online crowdfunding from smaller donations. It is not specifically related to the new technologies.	Preparation
41.	International Institute for Democracy and Electoral Assistance. 2018. Collaboration between Citizen Movements and Political Parties	'This Primer describes how successful collaboration can emerge between parties and movements, and thereby increase citizens' involvement in politics. It is based on interviews and workshop discussions that took place in The Hague, the Netherlands, in November and December 2017, and draws mostly from the latest developments in political parties from Europe.'	Low	It discusses how movements collaborate with political parties. And increase citizens involvement in politics.	General
42.	International Institute for Democracy and Electoral Assistance. 2019. Open Primary Elections	This paper discusses the innovative methods of political parties to include non-members, who may be close to the party in its structures by means of open primaries. On the one hand, open primaries could be an opportunity for political parties to connect with disengaged citizens, and on the other hand to allow these citizens to influence the	High	Discusses use of new techniques (in particular, infiltration voting, online fundraising and other campaign fundraising techniques etc.) in the context of open primaries, which is an activity of the first stage of the electoral	Preparation

[132] Summary prepared by the contractor

		party's decisions. On the other hand, they may give rise to illicit funding techniques.[133]		process, therefore directly falling within the scope of this study.	
43.	High Level Expert Group on Artificial Intelligence. 2019. A Definition of AI Main Capabilities and Disciplines	The HLEG paper expands the definition of Artificial Intelligence (AI), as proposed within the European Commission's Communication on AI to clarify certain aspects of AI as a scientific discipline and as a technology, with the aim to avoid misunderstandings, to achieve a shared common knowledge of AI that can be fruitfully used also by non-AI experts, and to provide useful details that can be used in the discussion on both the AI ethics guidelines and the AI policies recommendations.[134]	Medium	Provides comprehensive information on the technology AI and its main capabilities, without specifically referring to its use in an electoral context	General
44.	Ferrara. 2017. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election	This paper aims to analyse forms of social media manipulation, especially disinformation and social bot operations in the run up to the 2017 French presidential elections, focusing on the MacronLeaks disinformation campaign. "Nearly 17 million posts occurred between April 27 and May 7, 2017 (Election Day)" were collected from Twitter dataset. In conclusion, the paper confirms results from previous academic contributions sustaining the existence of a "black market of reusable political disinformation bots", but the study goes further this argument and add the new discovery of identifying bots already present during 2016 US presidential election campaign and supporting alt-right positions, however inactive since then. Secondly, the paper also concludes that regarding audience of MacronLeaks campaign, it was mainly composed by "English-speaking American alt-right community, rather than French users", potential voters,	High	It examines disinformation campaigns in the run up to presidential elections. Analyses bots' users in social platforms (Twitter) by mean of new technologies (Machine leaning, algorithm, etc,)	Preparation

[133] Summary prepared by the contractor

[134] Summary prepared by the contractor

		which also explains the limited success of this disinformation campaign.[135]			
45.	Papakyriakopoulos et al. 2018. Social media and microtargeting: Political data processing and the consequences for Germany	Political campaigns employ microtargeting, a specific technique used to address the individual voter. The article elaborates on how the use of microtargeting can be more challenging depending on the laws of the country (USA, Germany, France). The article further discusses on how the data can be collected, put into different clusters and analysed.[136]	Medium	Discuss the technique of microtargeting, and the related risk on biases in the collected data. It is not specifically related to the new technologies in a way of a threat to elections or democracy.	Preparation
46.	Bulut et al. 2019. Blockchain-Based Electronic Voting System for Elections in Turkey	'Traditional elections satisfy neither citizens nor political authorities in recent years. They are not fully secure since it is easy to attack votes. It threatens also privacy and transparency of voters. Additionally, it takes too much time to count the votes. This paper proposes a solution using Blockchain to eliminate all disadvantages of conventional elections. Security and data integrity of votes is absolutely provided theoretically. Voter privacy is another requirement that is ensured in the system. Lastly, waiting time for results decreased significantly in proposed Blockchain voting system.'	High	It discusses how blockchain technology is used in the voting systems in the elections in Turkey.	Voting
47.	Jefferson et al. 2019. What We Don't Know About the Voatz "Blockchain" Internet Voting System	This article aims to urge the disclosure of more information on the features and functionalities of the "Voatz" blockchain internet voting system. In terms of methodology, the article explains that Voatz is a recent start-up company that is operating an Internet voting system intended for public elections, used in West Virginia, US in the recent years. The authors consider that the functioning mechanisms of the	High	Discusses use of new technologies and techniques (in particular, blockchain) in electronic voting, which is an activity of the second stage of the electoral process, therefore directly falling within the scope of this study.	Voting

[135] Summary prepared by the contractor

[136] Summary prepared by the contractor

		Voatz system should be more transparent and clearer to the public, and therefore urges Voatz to reveal some technical details on their system by asking a number of important questions. [137]			
48.	Network and Information Security Cooperation Group. 2018. Compendium on Cyber Security of Election Technology	'In line with the focus of the NIS directive, this compendium specifically focuses on events that are cyber-enabled or relate to the security of network and information systems in the context of elections. Social media, information operations, and disinformation are outside of the scope of this initiative, while internet/remote voting solutions are not at its heart, but can inform the practices discussed.'	Medium	Discusses on events that are cyber-enabled in the context of elections. Social media, political advertising or disinformation campaigns are not addressed.	Preparation
49.	Cherubini, Graves. 2016. The rise of fact-checking sites in Europe	An increasing number of fact-checking outlets exist, and across different countries, different organisational forms, and different self-identified orientations, they share a common commitment. The two most important organisational forms fact-checking takes in Europe are the newsroom model associated with existing news media, and the NGO model that operates independently. The fact-checkers identify in different and sometimes multiple ways: reporters, activists or experts. Whatever their organisational form, research practices, and funding model, all fact-checking outlets still rely in a large part on existing news media to publicise their work.[138]	Medium	The paper focusses more on how the fact checker websites identify themselves, rather than on the fight against fake news.	Preparation
50.	European Data Protection Supervisor. 2019.	The content of this short document reflects on the vision for privacy in the digital age. It was a vision of an EU with world-class data protection standards, leading by example. It saw	Low	Gives an overview of work carried out by EDPS between 2015 and 2019	General

[137] Summary prepared by the contractor

[138] Summary prepared by the contractor

	Leading by Example 2015 - 2019	the EDPS, in the role as a supervisory authority and policy advisor, as a centre of excellence for data protection.[139]			
51.	European Data Protection Supervisor. 2019. Europe Votes 2019 - how to unmask and fight online manipulation (Opening speech)	Opening speech by Giovanni Buttarelli on how to unmask and fight online manipulation. [140]	Medium	Opening speech for "Europe Votes 2019: how to unmask and fight online manipulation"	Preparation ; Voting; Post-election
52.	European Data Protection Supervisor. 2019. Annual Report 2019 - Executive Summary	'The Annual Report provides an insight into all EDPS activities in 2019, which was the last year of a five-year EDPS mandate. EDPS activities therefore focused on consolidating the achievements of previous years, assessing the progress made and starting to define priorities for the future. Of particular note were EDPS efforts to ensure that new EU rules on data protection are put into practice.'	Medium	Gives an overview of activities by EDPS in 2019	General
53.	Academic Network on European Citizenship Rights. 2016. Type A Report – Political Participation of Underrepresented Groups in the EU (Executive Summary)	'This report presents the findings and recommendations of the Pilot Studies that are part of the overall Report on the political participation of underrepresented groups in the EU.'	Medium	Discusses challenges of underrepresented groups to political representation. There is not specific mentions and references of new technologies or techniques influence in the electoral process.	Preparation

[139] Summary prepared by the contractor

[140] Summary prepared by the contractor

54.	EU-CITZEN: Academic Network on European Citizenship Rights. 2018. Type B report - Political Participation of Mobile EU Citizens – Insights from pilot studies on Austria, Belgium, Bulgaria, Germany, Greece, Hungary, Ireland, and Poland (Draft version)	This is a draft version and not to cite or circulate. 'The report provides an overview of the electoral participation of mobile EU citizens in all 28 Member States and a presentation of eight case studies on the following Member States: Austria, Belgium, Bulgaria, Germany, Greece, Hungary, Ireland, and Poland.'	Medium	This is a draft version and not to cite or circulate. Examines voter registration rules, remote voting modalities offered to mobile EU citizens, which is an activity of the first and second stage of the electoral process. E-voting option is mentioned, but not further developed and there is no reference to use of new technologies and techniques on electoral process.	Preparation
55.	EU-CITZEN: Academic Network on European Citizenship Rights. 2018. Annex: Consolidation of Member States fiches (Draft version)	This is a Draft version. This Annex is the consolidation of EU Member States fiches regarding Legal framework, registration and voting conditions, measures facilitating voting rights and statistics (i.e. universe of voters and election turnout).[141]	Medium	It develops on e-voting scenarios, but document focus on conditions and topics from preparation Stage for the elections, not making reference to the use of new technologies or techniques	Preparation

[141] Summary prepared by the contractor

56.	Grajewski. 2020. Artificial Intelligence	This note offers links to recent commentaries, studies and reports from international think tanks on AI and related issues.[142]	Medium	List of Think Thanks studies, reports and comments on AI	General
57.	Sgueo. 2020. Digital Democracy Is the Future of Civic Engagement Online	'This briefing examines three key global trends that are driving the on-going digitalisation of democratic decision-making. First are demographic patterns. Second, a more urbanised global population will make cities ideal settings for innovative approaches to democratic decision-making. Third, technological advancements will cut the costs of civic mobilisation and pose new challenges for democratic systems.'	Low	Discusses what technology means for government systems in general.	General
58.	Bentzen. 2018. Foreign influence operations in the EU	This briefing looks into how foreign powers influence political decision-making beyond one's own political sphere. Two approaches of projecting power are looked at: the soft and the sharp approach. It gives also examples of active measures then and now: the case of the Kremlin; and European responses to disinformation campaigns. At the end it focuses on evolving tools and actors.[143]	High	Discusses how foreign powers influence try to influence elections with disinformation.	Preparation
59.	Davies. 2014. Social media and election campaigning	This briefing is about how social media is used and what the effect is in election campaigns across Europe.[144]	High	Discusses how social media is used in election campaign and what the effect is.	Preparation
60.	Boucher. 2019. Technology and social polarisation	Briefing about two STOA studies which explores the mechanisms by which technologies and techniques may foster polarisation in Europe. One study approaches the question with reference to trends in the production and consumption of news media, while the other focuses on	High	Discusses how technologies such as social media and techniques such as psychological profiling can be combined in election campaigns with worrying effects.	Preparation

[142] Summary prepared by the contractor
[143] Summary prepared by the contractor
[144] Summary prepared by the contractor

		trends in political campaigning and communication strategies.[145]			
61.	Neudert, Marchal. 2019. Polarisation and the use of technology in political campaigns and communication	'This report offers a comprehensive overview of the relationship between technology, democracy and the polarisation of public discourse. It provides an in-depth analysis of the technological affordances that enhance and undermine political decision-making, both now and in the future. As conclusion, two principles and policy options for fostering a better relationship between digital technology and public life were formulated.'	High	Discusses how technology can exacerbate social and political polarisation	Preparation
62.	Martens et al. 2018. The digital transformation of news media and the rise of disinformation and fake news: An economic perspective	'This report contains an overview of the relevant economic research literature on the digital transformation of news markets and the impact on the quality of news. It compares various definitions of fake news, including false news and other types of disinformation and finds that there is no consensus on this. It presents some survey data on consumer trust and quality perceptions of various sources of online news that indicate relatively high trust in legacy printed and broadcasted news publishers and lower trust in algorithm-driven news distribution channels such as aggregators and social media.'	High	Discusses the impact of fake news in general but also how it can influence elections	Preparation
63.	Mair et al. 2019. Understanding our political nature How to put knowledge and reason at the heart of political decision-making	'The behavioural sciences, social sciences and humanities can bring new insights into political behaviour, such as how and why emotions, values, identity and reason affect how we think, talk and take decisions on political issues.'	Low	Discusses how behavioural sciences gives us insight in political behaviour.	Horizontal

[145] Summary prepared by the contractor

64.	Nikoltchev et al. 2016. Mapping of media literacy practices and actions in EU-28	'This report is focused on projects relating to media services delivered on electronic communication networks, both linear and non-linear, and on information services where pertinent, whereas press, radio and off-line media are excluded from the report's scope. Considering the existence of specific studies on actions related to school curricula, the European Commission has asked to include only media literacy actions that have taken place outside schools.'	Low	Discusses how citizens interact and understand media	Horizontal
65.	Devaux et al. 2019. Study on media literacy and online empowerment issues raised by algorithm-driven media services	'The objective of this study was to understand how the provision and consumption of news online works (in particular in social media platforms), which problems it raises with regard to the functioning of democracies, what is currently in place to counter these issues and their implications, and what (other) options should be explored. This study proposes three concrete behavioural experiments to be conducted that would test whether social media platforms could counter cognitive biases and trigger a more analytical type of thinking by online users.'	Low	Discusses how algorithms are used in online media services	Horizontal
66.	European Commission. 2019. Communicating ahead of the 2019 European Elections	'The analysis looks ahead of the Commission's communication and mobilisation efforts ahead of the EU elections and cooperation with the EP. It assesses what worked well and the challenges the Commission faced in communication the three stands: 1) what the EU does; 2) why and how to vote; 3) how to engage.'	Medium	Discusses how the Commission communicated and ahead of the 2019 EU Elections	Preparation
67.	Merkel. 2019. Past, Present and Future of Democracy - Policy Review	'The Policy Review takes stock of the results, findings and recommendations, and assesses the needs, gaps and pertinent foci for future European research on democracy. These should enrich future steps in the design and implementation of Horizon Europe. Finding ways of bolstering and improving our democratic institutions is a matter of paramount significance.'	Low	Discusses the fragility and deficits of today's established democracies	Horizontal

68.	Bayer et al. 2019. Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States	'This study assesses the impact of disinformation and strategic political propaganda disseminated through online social media sites. It examines effects on the functioning of the rule of law, democracy and fundamental rights in the EU and its Member States. It also formulates recommendations on how to tackle this threat to human rights, democracy and the rule of law. It specifically addresses the role of social media platform providers in this regard.'	High	Discusses how technology changed the democratic process and how it interfered with it	Preparation
69.	Expert Group on Liability and New Technologies. 2019. Liability for Artificial Intelligence and other emerging digital technologies	'This report focuses on artificial intelligence and other emerging digital technologies, such as the Internet of Things or distributed ledger technologies, have the potential to transform our societies and economies for the better. However, their rollout must come with sufficient safeguards, to minimise the risk of harm these technologies may cause, such as bodily injury or other harm.'	Medium	Discusses how liability regimes should be designed – and, where necessary, changed – in order to rise to the challenges emerging digital technologies bring with them.	Horizontal
70.	Theben et al. 2018. Study on the impact of the internet and social media on youth participation and youth work - Executive Summary	'This study explores how the internet and social media influence young people's active citizenship and participation in the public spheres of democratic societies and how those working with them, particularly youth workers as well as public authorities, can use these tools to engage with all young people, including disadvantaged groups, in an effective and meaningful way.'	Medium	Discusses the role of internet and social media in young people's life and how it influences their citizenship.	Horizontal
71.	European Union Agency for Fundamental Rights. 2018. BigData Discrimination in	'This focus paper specifically deals with discrimination, a fundamental rights area particularly affected by technological developments. When algorithms are used for decision making, there is potential for discrimination against individuals. The principle of non-discrimination, as enshrined in Article 21 of the Charter of Fundamental Rights of the European Union (EU), needs to be taken into account	Medium	Discusses how algorithms are used in decision making and how it can cause discrimination against individuals.	Horizontal

	data-supported decision making	when applying algorithms to everyday life. This paper explains how such discrimination can occur, suggesting possible solutions. The overall aim is to contribute to our understanding of the challenges encountered in this increasingly important field.'			
72.	European Commission. 2019. European Elections 2019 – Political Report	Report on the results of the 2019 European Elections.[146]	High	Analyses the result of the 2019 EU Elections.	Post-election
73.	CERT-EU. 2019. Election Hacking Bulletin	'CERT-EU has identified four main categories of attacks (which sometimes are combined) to hack an election: 1) Obtaining sensitive information related to a candidate, a political party or an institution; 2) Influencing public opinion (including via disinformation) in favour of or against specific candidates or votes; 3) Attacking voting systems, electoral processes & institutions or instilling distrust in them; 4) Disrupting or undermining the campaign of particular candidates'	Medium	Discusses how hacking is used to influence public opinion and how to make citizens distrust the electoral process and institution	Preparation
74.	United Nations Educational Scientific and Cultural Organization. 2019. Elections and media in digital times	'This report is about the increasing digitalization of societies across the world has led to unprecedented opportunities to seek, receive and impart political information and ideas, which are the lifeblood of elections. The Internet, and in particular social media and social messaging have changed the way politicians, political parties and the electorate communicate with each other, with the chance of being more direct and quicker than at any point in history. But there are also growing concerns about the disruptive effects on public debate arising from the misuse of digital	High	Discusses how the digitalisation of the societies caused unprecedented opportunities to seek, receive and impart political information. It also looks into how micro-targeting is used for the spreading of misinformation.	Preparation

[146] Summary prepared by the contractor

		technologies. Political micro-targeting of individual voters is driven by aggregated personal data, which is not always obtained in lawful ways. Moreover, micro-targeting practices are sometimes manipulative. The report is a follow-up to UNESCO's 36 C/Resolution 53, wherein the Organization's Member States requested UNESCO to monitor the status of press freedom and safety of journalists and to report on the developments in these fields to the Organization's General Conference.'			
75.	Zalc, Becuwe, Buruian. 2019. The 2019 Post-Electoral Survey Have European Elections Entered a New Dimension	This report looks in detail at who went to vote in the 2019 European elections, analysing the variations between EU countries, socio-demographic and socio-professional groups.[147]	High	Discusses the results of the 2019 election	Post-election
76.	European Parliament. 2019. A pro-European - and young - electorate with clear expectations	Statistical overview of the results of EP elections.[148]	Medium	Discusses the results of the 2019 election	Post-election
77.	European Commission. 2019. Flash Eurobarometer 478 How do we build a stronger,	'This report provides a deeper exploration of the attitudes and opinions of young people aged 15-30. It covers the proportion of respondents who have been abroad for learning experiences, and the reasons why respondents have not participated in learning experiences in other countries; young respondents' participation in social, civic	Low	Discusses the attitude and opinions of young people	Horizontal

[147] Summary prepared by the contractor

[148] Summary prepared by the contractor

	more united Europe? The views of young people	and political activities, including organised voluntary activities, as well as reasons for not participating in these activities; Opinions about the most important things schools should offer young people, and the topic areas that are not taught sufficiently in schools; Young respondents' views about the priorities for the EU in years to come; The most useful actions for young people the EU could support'			
78.	European Commission. 2019. Special Eurobarometer 486 Europeans in 2019	'This report consists of four parts. In the first section, "Life in the European Union", respondents discuss the main concerns at both national and European levels. The second part, "The European Union in 2019", addresses views on the EU's present circumstances, including opinions about the EU's main assets, challenges and most positive results. In the third part, "The European Union and its citizens", respondents discuss what the EU means to them personally, as well as their subjective and objective knowledge of the European Union. The report ends with a chapter on "Europe today and tomorrow", where we discuss whether respondents support more decision-making at EU level, the areas in which technology will have the biggest impact in Europe, and the policies that would be most helpful to Europe's future. Finally, other topics include Europeans' confidence in the future, optimism about the future of the European Union, and the prospects for young people.'	Low	Discusses how citizens feel in the EU and how they would like to see it in the future.	Horizontal
79.	European Commission. 2019. Special Eurobarometer 489 Rule of law	The Commission started a process of reflection on how to strengthen the rule of law in the EU. The Commission outlined three pillars that could contribute to the more effective enforcement of the rule of law: 1) better promotion; 2) early prevention; 3) tailored response.[149]	Low	It assesses the importance to citizens of a number of aspects of the rule of law as whether these aspects need improving in their country.	Horizontal

[149] Summary prepared by the contractor

80.	European Commission. 2018. Standard Eurobarometer 90 Media use in the European Union	This Eurobarometer survey analyses media habits of European citizens, a topic which has been approached through the following domains: 1) Media habits and trust in the media; 2) The level of information about European matters; 3) Information sources for political matters and the European Union; 4) Opinion about pluralism and the independence of national media; 5) Europeans and fake news; 6) Social networks.[150]	Medium	Discusses the media habits of EU citizens	Horizontal
81.	European Commission for Democracy through law (Venice Commission). 2018. The impact of the information disorder (disinformation) on elections	'This brief (hereinafter: the Brief) is to support the 'Study on the role of social media and the Internet in democratic development' prepared by José Luis Vargas Valdez* for the Venice Commission of the Council of Europe (hereinafter: the Valdez-Study). The aim of the Brief is to (a.) provide input on relevant Council of Europe (hereinafter: CoE) standards and other instruments and materials relating to elections and the internet; and (b.) suggest additions to the Valdez-Study for a better presentation of the critical aspects regarding the enjoyment of the right to free elections within the transformed communicative spheres.' In conclusion, it is recognised the importance of social media intermediaries as a positive facilitator of public and democratic debate. On the other side, it also held these intermediaries accountable for safeguarding the respect for fundamental rights such the right to free elections on their platforms.	High	Raising awareness on the CoE standards in elections and the internet. Talks about the impact of disinformation in elections	Preparation
82.	European Commission for Democracy Through Law	'The explanatory report explains the principles, from the Code of good practice in electoral matters, set forth in the guidelines, defining and clarifying them and, where necessary, including recommendations on points of detail.	High	Guideline can provide a way to identify malicious approaches in elections	Horizontal

[150] Summary prepared by the contractor

	(Venice Commission). 2018. Code of good practice in electoral matters, Guidelines and explanatory report (Adopted by the Venice Commission AT its 52nd session – 2002)	The report was adopted by the Council for Democratic Elections at its 3rd meeting (16 October 2002), and subsequently by the Venice Commission at its 52nd Session (18-19 October 2002).'			
83.	Rapid Response Mechanism Canada. 2019. Open data analysis - European Parliamentary Elections: Comprehensive Report	'The main objectives of this report are to: shine light on any effort to artificially amplify unsubstantiated or false information challenging the legitimacy and fairness of the UK, Irish or EU democratic and electoral systems; identify key issues that were highly divisive and exploited within the context of the EU elections in the UK, Ireland and Italy in order to identify narratives that may transcend borders and be used in other contexts; and identify notable tactics used by malign, foreign actors. (…) In relation to the EU Parliamentary Elections, a key insight from RRM Canada is that while no significant evidence of state-based foreign interference was observed, the digital ecosystem is ripe and ideal for exploitation by foreign malign actors.'	High	It is a quantitative report that has findings regarding legitimacy and fairness in elections	Preparation
84.	Organization for Security and Co-operation in Europe. 2017. Political advertising and media campaign during	'The present Comparative Study provides for findings within the project "Political advertising and media campaign during the pre-election period". The final objective of the project is to improve the quality of the media legal framework regulating political advertising.'	High	Has information on the freedom and regulation of political advertising.	Preparation

	the pre-election period: A Comparative Study				
85.	Ministry of the Interior and Kingdom relations Democracy and Governance. 2019. Aan de Voorzitter van de Tweede Kamer der Staten-Generaal: Policy means for protecting democracy against disinformation	This letter is discussing the policy means for the protection of Dutch society against disinformation. It covers topics such as: which actions are ongoing and which are necessary, in the fight against disinformation, and an analysis of the threats.[151]	High	It is about Dutch actions against disinformation	Preparation
86.	Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation. 2019. Progress Report - November 2019	'This 2nd report of the Interdepartmental Group (IDG) on Security of the Electoral Process and Disinformation presents a first assessment of the progress achieved on the recommendations of the 1st IDG Report, since its publication in July 2018. (…)The main finding was that risks to the electoral process in Ireland are relatively low but that the spread of disinformation online and the risk of cyber-attacks on the electoral system pose more substantial risks. This aligned with EU findings and recent international experience. The Report outlined 7 recommendations, which were developed to form the basis for a multi-faceted, whole of government approach to safeguarding of the electoral process from disinformation and security risks.'	High	Cf. summary	Preparation ; Voting; Post-election

[151]Summary prepared by the contractor

87.	European Commission for Democracy Through Law (Venice Commission). 2019. Joint Report on Digital Technologies and Elections (CDL-AD(2019)	'The report analyses the use of digital technologies during electoral processes. The report discusses that digital (or "new") technologies and social media have revolutionised the way people interact and exercise their freedom of expression and information, as well as other related - and sometimes conflicting - fundamental rights. People who engage in social media may use the internet to organise and demand better services, more transparency and meaningful participation in the political arena. Individuals all over the globe are now able to shape global perceptions, position topics in their national agendas and foster political activism. This digital transformation is recasting the relation between states and citizens.'	High	Touches on matters such online social media and democracy of electoral process. Discusses about free elections	Preparation ; Voting; Post-election
88.	Dutch Ministry of Interior and Kingdom Relations. 2019. Letter to the House of Representatives on policy means for protecting democracy against disinformation	The actions by the Cabinet will be implemented according to three spearheads: prevention, reinforcing the information position and (if necessary), response. Preventive actions are aimed at preventing the impact and spreading of disinformation. Reinforcing the information position and information sharing provide a timely insight into and interpretation of the (potential) threats. Reactive actions are responses in the event that disinformation occurs. Given the nature of the threat in our country and the principles operated by the Cabinet, the current emphasis is on preventive actions.[152]	High	Touches upon disinformation, media literacy, transparency by examining regulation etc.	Preparation
89.	Council of Europe. 2017. Online media and journalism - challenges and accountability	The resolution acknowledges the positive aspects of media outlets and online social media such creation of media pluralism, awareness of human rights violation in different countries and or even its role as "watchdog". On the other hand, the Assembly raises concerns on other aspects such	Medium	No direct reference to elections nor to new technologies. Shows the approaches taken and the recommendations which could be already actioned.	Horizontal

[152] Summary prepared by the contractor

	(Resolution 2143 (2017)	the possibility of political groups to launch concerted action or the swift in resources from media outlets to internet and social media which as impact for examples in weakening professional media. Moreover, the Recommendations of the Assembly pertaining to tackling topics such as disinformation, regulation, media literacy and others. [153]			
90.	Committee of Ministers of the Council of Europe. 2007. Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns	The document discusses the necessary revision of Recommendation No. R (99) 15 of the Committee of Ministers on measures concerning media coverage of election campaigns. This related to the significant differences which still exist between the print and the broadcast media.[154]	Low	Has a number of recommendations that could be interesting to see how they are addressed by regulation and media, but rather dated as it is from 2007.	Preparation
91.	Committee of Ministers of the Council of Europe. 2016. Recommendations and Declarations of the Committee of Ministers of the Council of Europe	'The principles of fairness, balance and impartiality in the coverage of election campaigns by the media should apply to all types of political elections taking place in member States, that is, presidential, legislative, regional and, where practicable, local elections and political referenda.'	Medium	For identifying similarities with later recommendations and potentially spotting implementations of the recommendation.	Horizontal

[153] Summary prepared by the contractor
[154] Summary prepared by the contractor

	in the field of media and information society				
92.	Electoral Administration Team of the UK Cabinet Office. 2018. Protecting the Debate: Intimidation, Influence and Information	This consultation document reviews the following recommendations and issues: governmental consultation on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners; A consolidation and clarification of the electoral offence of undue influence; an extension on the electoral law requirements for an imprint on campaigning materials to electronic communications.[155]	High	Talks about intimation of public life, undue influence and other important issue that affect public life and the election process.	Preparation
93.	a) Lupiáñez-Villanueva et al. 2018. Study on the Benefits and Drawbacks of Remote Voting + Technical Appendices Faulí et al. 2018. Study on the benefits and drawbacks of remote voting solutions - Presentation of Main findings	The study examines the barriers to voting encountered by different groups of citizens and maps the different types of remote voting solutions available in the EU Member States, outlining their benefits and drawbacks. In conclusion, the study points out that options for remote voting and how they operate vary greatly from one country to another, depending for example, on the electoral system, the method by which voters are registered, the design of the solution, demographic factors, and the aspects of the voting process (such as ballot secrecy) most valued by the population. This implies that in European elections, citizens vote under different systems. While proposing a common approach to the availability of remote voting for European Parliament elections would reduce the complexity of the	High	c.f. summary	Voting

[155] Summary prepared by the contractor

		current status quo, it would also affect the prerogatives of Member States.[156]			
94.	European Committee of the Regions. 2019. Draft Opinion - Action Plan against Disinformation	'The recommendations include principles and ideas intended to protect personal liberties, to avoid over-reaction, and to build public support. The opinion warns that "without sufficient transparency, there is a great risk that measures to counter disinformation themselves fall victim to hostile information attacks" and therefore argues for "the public having access to comprehensive information and being kept abreast of, for instance, data protection, personal data processing and financing aspects". It says, "the possible spread of disinformation must be systematically and continuously monitored" – "but not all the time", suggesting that such high-intensity monitoring should be restricted to the run-up to elections and times of crisis and abrupt social change.'	Medium	Action plan against disinformation in general	Horizontal
95.	Finck. 2019. Artificial Intelligence and Online Hate Speech	'This Issue Paper provides an overview of related opportunities and challenges. It first documents the problem of online hate speech and the shortcomings of current forms of human-based content moderation processes before introducing the potential of machine- and deep-learning, highlighting that AI may trigger important efficiency gains in this area. At the same time, however, there are also considerable weaknesses associated with current forms of AI, most importantly its over inclusiveness which causes considerable problems from the freedom of expression perspective. The paper will consider if and how future developments in artificial intelligence may address	Medium	Discusses opportunities and challenges regarding AI and online hate speech.	Horizontal

[156] Summary prepared by the contractor

		some of these issues and the paper closes with suggestions of themes for future discussion.'			
96.	European Commission. 2019. First Annual Self-Assessment Reports on the Code of Practice of Disinformation	The document provides information on the annual reports submitted by the signatories of the Code of Practice on Disinformation such as Facebook, Twitter, Google and Microsoft, on the various measures they have implemented in compliance with their obligations to fight online disinformation.[157]	High	The document contains an overview of measures specifically relating to activities from the stages of the electoral process, such as online political advertising, which directly falls within the scope of this study.	General
97.	European Union Agency for Fundamental Rights. 2019. Data Quality and artificial Intelligence – mitigating bias and error to protect fundamental rights	The paper discusses the notion of bias in the training data among other aspects. It describes the way data are being collected by businesses for data analysis aiming at business growth. It emphasizes the discrepancies in the data depending on the medium they are collected. For example, the data gathering from the internet is not a very efficient way to do so since there are specific groups that don't have access to it. The same goes for social media as many people choose not to use them and as such, the data inevitably have a bias. This is particularly noticeable for households with low income that either don't have internet access. Furthermore, the paper uses examples of biased results when low quality data are used in the training process of the AI systems. Low quality could affect the access to a fair trial.[158]	Medium	The paper is part of the project work of the European Fundamental Rights Agency on Artificial Intelligence and big data. It debates on specific problematic use of AI by giving examples of biased results when low quality data are used in the training process of the AI systems. Low quality could affect the access to a fair trial. However, it does not reflect or cover use of new technologies such AI in elections' context.	Horizontal
98.	European Union Agency for Fundamental Rights. 2019. Facial	'Facial recognition technology (FRT) makes it possible to compare digital facial images to determine whether they are of the same person. Comparing footage obtained from video cameras (CCTV) with images in databases is referred	Medium	Cf. summary	Horizontal

[157] Summary prepared by the contractor

[158] Summary prepared by the contractor

	recognition technology: fundamental rights considerations in the context of law enforcement	to as 'live facial recognition technology'. Examples of national law enforcement authorities in the EU using such technology are sparse-but several are testing its potential. This paper therefore looks at the fundamental rights implications of relying on live FRT, focusing on its use for law enforcement and border-management purposes. EU law recognises as 'sensitive data' people's facial images, which are a form of biometric data. But such images are also quite easy to capture in public places. Although the accuracy of matches is improving, the risk of errors remains real-particularly for certain minority groups. Moreover, people whose images are captured and processed might not know this is happening-and so cannot challenge possible misuses. The paper outlines and analyses these and other fundamental rights challenges that are triggered when public authorities deploy live FRT for law enforcement purposes. It also briefly presents steps to take to help avoid rights violations.'			
99.	European Union Agency for Fundamental Rights. 2019. Artificial Intelligence, Big Data and Fundamental Rights (project report not published)	This project assesses the pros and cons for fundamental rights of using artificial intelligence (AI) and big data for public administration and business purposes in selected EU Member States.[159]	Medium	(Project with status ongoing. Final project report not available)	Horizontal

[159] Summary prepared by the contractor

100.	European Union Agency for Fundamental Rights. 2020. E-media Toolkit on Migration	'In today's media landscape the way in which journalists and editors receive, process and publish news is constantly changing. Journalists face immense time pressure, as news frequently breaks online. (…) To facilitate training on the coverage of migration news, this Trainer's Manual is a tool to be used together with the e-Media Toolkit. This manual includes factual reporting examples that illustrate work dilemmas in the newsrooms of television channels, newspapers, radio stations and online outlets. It covers only Migration domain.'	Low	This pilot toolkit has been devised by journalists and media trainers to help reporters and editors working on international migration. It will be the starting point of a broader project on how to cover news while maintaining respect for diversity and human rights.	Horizontal
101.	European Commission. 2019. Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final	The Recommendation points out that ahead of the elections for the EU Parliament the Member States should form Election cooperation networks, ensure transparency in political advertising, impose appropriate sanctions for infringements of rules on the protection of personal data and perform awareness raising activities.[160]	High	Cf. summary	General

[160] Summary prepared by the contractor

102.	European Commission. 2020. Tackling COVID-19 disinformation - Getting the facts right (JOIN (2020) 8 final)	The Joint Communication focuses on the immediate response to disinformation around the coronavirus pandemic, looking at the steps already taken and concrete actions to follow, which can be quickly set in motion based on existing resources. It also highlights areas where the crisis has pointed to more fundamental challenges, to be further assessed as the crisis evolves and to form part of the wider approach to strengthen democracy, which will be set out in the European Democracy Action Plan, as announced in President von der Leyen's Political Guidelines. Its aim will be to further strengthen the EU's work to counter disinformation and to adapt to evolving threats and manipulations, as well as to support free and independent media. The upcoming Digital Services Act, regulating digital services, is part of this comprehensive approach.[161]	High	Discusses how to tackle COVID-19 disinformation.	EU legal and policy framework
103.	a) European Commission. 2020. Report on the 2019 elections to the European Parliament (COM (2020) 252 final) b) European Commission. 2020. Report on the 2019 elections to the European	The report shows that young and first-time voters drove turnout figures to the record high. The 2019 election campaign was the most digital to-date – almost half of EU citizens now rely on online news as their main source for information about national and European politics. Yet the Member States have differing rules when it comes to digital campaigning, including on paid-for political content online. A dynamic European debate emerged on a number of topics, showing progress in developing a European political dimension; however, national-specific issues remain key for candidates and voters alike. European citizens expressed increased satisfaction with free and fair elections in the EU, but further work is necessary to protect democracy from	High	Cf. summary	Preparation ; Voting

[161] Summary prepared by the contractor

	Parliament (SWD (2020) 113 final)	foreign interference and manipulation and promote free and fair elections in Europe.[162]			
104.	International Republican Institute. 2019. Democracies under pressure - a global survey	'The idea of democracy is based on a political order whose main feature is making the exercise of power subject to the consent of the governed. During the 20th century the idea of democracy triumphed over modern tyrannies. This study elaborates on the public opinion on the transparency of the political process, the trust in the democracy in their country, trust in the institutions, and their interest in politics. It also handles some topics related to threats to democracy such as: leadership by a strongman, authoritarianism, and the connection between the government and armed forces. The public opinion is also asked about the use of issue topics such as migration and religion. The results of this international study, carried out in forty-two democracies, are presented here under the title Democracies under pressure.'	Medium	This survey tries to get a picture of the citizens on the level of transparency and on how well the democracy in their country is perceived. It does not go deeper on any technology itself.	Horizontal
105.	Kofi Annan Commission on Elections and Democracy in the Digital Age. 2020. Protecting Electoral Integrity in the Digital Age	The Annan commission was convened before Kofi Annan's death in 2018 in defence of electoral integrity against the misuse and abuse of social media. The Report prepared by the commission puts forward 13 recommendations grouped in 4 main categories – building capacity, building norms, actions by public authorities and actions by platforms.[163]	High	Cf. summary	General
106.	Lim. 2020. Disinformation as a Global Problem –	'This research project discusses disinformation in the European Union (EU) and Southeast Asia (SEA). The report examines the characterisation and context of	High	Study on disinformation in the European Union.	Preparation ; Voting;

[162] Summary prepared by the contractor

[163] Summary prepared by the contractor

	Regional Perspectives	disinformation, provides an overview of its creators and its circulation, where creation refers to production and its underlying motivations and circulation refers to the different ways it is disseminated, amplified and sustained, and rounds up with a discussion on foreseeable trends. It finds that disinformation is ultimately a national security problem, and any assessment of, and response to, disinformation must be formulated with developments in other domains.'			Post-election
107.	Hegelich, Serrano. 2019. Microtargeting in Germany for the 2019 European Elections	This article aims to analyse how microtargeting techniques were used and if and how they had impact on 2019 European Parliament elections in Germany. In terms of methodology, as many other articles, this article also starts by analysing the tools made available by the platform operators (Google, Facebook or Twitter) - such reporting tools and the application programming interfaces (APIs) such Facebook Ad Library API or the Google Cloud BigQuery API. In conclusion, the article argues that though there is a clear evidence that in the last 2019 European Parliament election in Germany, the political parties' online advertising strategy had an important relevance on their campaigning strategy, it was not exploited to its maximum, for example by increasing the budget allocated for microtargeting technique. Secondly, and as other articles raised before, the data made available by the platforms operators is not fully complete and reliable, as they provide and work with different definitions of what are political ads for example.[164]	High	The article analyses the use of microtargeting 2019 European Parliament elections in Germany.	Preparation

[164] Summary prepared by the contractor

108.	Davis, Livingston, Hindman. 2019. Suspicious Election Campaign Activity on Facebook	This article elaborates on the techniques used to create artificial promotion of political campaigns on Facebook, done by the German political far right party Alternative für Deutschland (AfD).[165]	High	Elaborates on the techniques of artificial promotion to make use of social media, by the use	Preparation
109.	European Regulators Group for Audiovisual Media Services. 2019. Assessment of the Implementation of the EU Code of Practice on Disinformation	The overarching study objective is to support the European Commission's evaluation of the Code of Practice's effectiveness. The assessment focuses on the 13 current Signatories of the Code of Practice on Disinformation (online platforms and business associations). The study's overall conclusion is that the Code of Practice has produced positive results. Firstly, it has established a common framework under which to agree on and implement activities to tackle disinformation, Secondly, it has established a platform for negotiation that has produced concrete results in the form of regular monitoring of Signatory activities and continuous action to combat disinformation activities, The main criticism of the Code relates to its self-regulatory nature, lack of uniformity of implementation, monitoring, and lack of clarity around its scope and some of the key concepts.[166]	High	The assessment relates directly to the electoral process as online disinformation and the way it is addressed by online platforms is a main threat to free and fair elections.	General
110.	Yannakoudakis. EESC. 2018. Protection of personal data in the context of EP elections	'Opinion of the EESC: The EESC supports the objectives of the Commission proposal and agrees that democracy is one of the fundamental values on which the EU is founded. The EESC recognises that the procedures for the elections of the EP are Member State governed within the EU framework. Enabling the Authority for European political parties and European political foundations (the 'Authority') to impose	High	Opinion on protection of personal data in EP elections	General

[165] Summary prepared by the contractor

[166] Summary prepared by the contractor

		sanctions is one way of ensuring personal data is protected and not misused for political gain. The EESC supports the additional staffing of the Authority with a view that this staff will be better positioned to work with the national DPAs to ensure that data protection infringements are properly investigated and where found sanctions applied.'			
111.	EESC. 2017. Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion)	This document consists in the opinion of the EESC on Artificial Intelligence on different domains. It elaborates on its opportunities and threats, its benefits for the humanity. Finally, the document delivers some recommendation on the use of AI. No special reference is made to the electoral process nor to new technologies and techniques.[167]	low	This reference does not discuss issues related to the electoral process and its stages in general. It briefly mentions concerns on impact of AI in various domains, being elections one of them. It does not make references to disinformation, microtargeting or other techniques.	Horizontal
112.	Privacy International. 2020. Challenging Data Exploitation in Political Campaigning	'Around the world, political campaigns are becoming increasingly reliant on the exploitation of people's data for political gain. Privacy International considers that there are certain baseline safeguards that should be in place: More transparency is needed from all actors involved; Comprehensive data protection laws must be implemented; Electoral laws need to be updated for the digital age; supervisors of data protection must have sufficient independence.'	High	Discusses political campaigning.	Preparation

[167] Summary prepared by the contractor

113.	Privacy International. 2020. Public opinion about data-driven election campaigning in the UK	Result of a poll after the 2019 elections in the UK, asking people about 'data-driven political campaigning'. It is found that most people oppose the use of targeted ads during elections and oppose election spending when the source of funding is unknown.[168]	Medium	It only describes what people think of the practice of 'Data driven political campaigning'. It doesn't go into detail on the functionalities of the technology itself.	Preparation
114.	Geller. Politico. 2020. Some states have embraced online voting. It's a huge risk.	People's phones, tablets and computers are vulnerable to hackers. Securing the internet could take a decade or more. But some states are implementing online voting anyway. The article puts forward some main security issues that make online voting more vulnerable than other online operations.[169]	High	The article refers to online voting, which is Stage II of the electoral process, therefore directly falling within the scope of this study.	Voting
115.	Esposito, Tse, Entsminger, Jean. MIT Insights. 2020. AI in the election industry demands transparency	'Whatever shapes voting, shapes democracies. Increasingly, AI is becoming such a go-to tool for shaping voting. As the race for the US presidency picks up speed, another area we should expect is the expanding use of AI in election prediction.'	High	AI in the election industry	Preparation ; Voting
116.	European Economic and Social Committee. 2020. The effects of campaigns on participation in	This document is an exploratory opinion requested by the Croatian presidency to the EESC. It presents a set of recommendation such as the improvement of self-regulation in the field of online disinformation or the improvement of EU action against domestic to foster 'timely monitoring, enhances professional journalism and fosters media literacy.'[170]	High	Cf. Summary	Horizontal

[168] Summary prepared by the contractor
[169] Summary prepared by the contractor
[170] Summary prepared by the contractor

	political decision-making				
117.	Madiega. 2020. Reform of the EU liability regime for online intermediaries	'The E-commerce Directive, adopted in 2000, aims at harmonising minimum standards of liability for internet (online) intermediaries across the European Union (EU). Under the current EU legal framework, digital or online platforms are not legally responsible for hosting illegal content but are required to remove such material once it is flagged.'	Medium	Handles the EU liability regime for online intermediaries, from an e-commerce perspective, not focussing on the elections process perspective.	Preparation
118.	Joint Research Centre. 2020. Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives	This report analyses how disinformation campaigns have evolved into more complex hostile narratives, taking Italy, France, and Spain as case studies to prove what has been observed and determined from analytical and numerical research. This report highlights how hostile narratives target citizens' vulnerabilities using algorithmic content curation. The case studies describe how different disinformation campaigns have been used in Italy, France and Spain. It also provides examples on how hostile disinformation narratives were employed in France and Italy.[171]	High	The report contains an analysis of disinformation campaigns in three EU Member States through algorithms, which directly falls within the scope of this study. It is also prepared by JRC which brings forward its horizontal nature	General
119.	Joint Research Centre. 2019. Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda	'Disinformation strategies have evolved from "hack and dump" cyber-attacks, and randomly sharing conspiracy or made-up stories, into a more complex ecosystem where narratives are used to feed people with emotionally charged true and false information, ready to be "weaponised" when necessary. Manipulated information, using a mix of emotionality and rationality, has recently become so pervasive and powerful to the extent of rewriting reality, where the narration of facts (true, partial or false) counts more than the facts themselves. Every day, an incredible	High	Study on disinformation strategies.	General

[171] Summary prepared by the contractor

		amount of information is constantly produced on the web. Its diffusion is driven by algorithms, originally conceived for the commercial market, and then maliciously exploited for manipulative purposes and to build consensus. Citizens' vulnerability to disinformation operations is not only the result of the threats posed by hostile actors or psychometric profiling - which can be seen as both exploiters and facilitators - but essentially due to the effect of three different factors: Information overload; Distorted public perceptions produced by online platforms algorithms built for viral advertising and user engagement; The complex iteration of fast technology development, globalisation, and post-colonialism, which have rapidly changed the rules-based international order. In rapidly and dynamically evolving environments, increasing citizens' resilience against malicious attacks is, ultimately, of paramount importance to protect our open democratic societies, social values and individual rights and freedoms.'			
120.	European Committee of the Regions. 2019. Artificial Intelligence for Europe	The document elaborates on AI in various domains, its benefits and reasons to be supported. It does not refer to elections nor to the use or other new technologies.[172]	Low	Reference to AI and its benefits in general. Electoral process or elections related topics are not addressed.	General
121.	European Committee of the Regions. 2019. Digital Europe for All: delivering	The opinion specifies recommendation for making new technologies (such as AI), available in the Digital Single Market, so it can serve for all citizens in Europe. It can help	Medium	The article elaborates on new technologies in Europe, but does not specify on the field of elections	Horizontal

[172] Summary prepared by the contractor

	smart and inclusive solutions on the ground	in the creation of jobs, a better cohesion, and improve the interoperability.[173]			
122.	European Committee of the Regions. 2019. Tackling online disinformation: a European Approach	In its Opinion, the European Committee of the Regions provides policy recommendations on the Communication of the Commission: Tackling online disinformation: a European approach. It emphasises the role of Charter of Fundamental Rights of the EU for the main guarantees of the rights of all EU residents, the efforts of the main social media players to combat disinformation by 'self-regulation' and their partnerships with fact-checkers. However, this turns out to be insufficient. The Opinion highlights the role of local and regional authorities in the fight against disinformation, the importance of civic education and support of local media and non-governmental organisations engaged in combating the phenomenon.[174]	Medium	It refers to disinformation in general, without making specific reference to political campaigning or other part of the electoral process which can be impacted by online disinformation.	Horizontal
123.	European Committee of the Regions. 2019. Action Plan against Disinformation	EESC Opinion on the Action Plan against Disinformation.[175]	Medium	Cf. Summary	Horizontal
124.	European Parliament. 2019. Activity Report of the Committee on Constitutional Affairs - 8th	'This document provides an overview of the committee's work over the European Parliament's 8th parliamentary term, namely from July 2014 to June 2019. It deals with each of the committee's areas of competence, focusing on the highlights and identifying the priorities that the committee sought to promote during that period.'	Medium	This document address to elections concerns such citizens participation, however it does not make reference to any type of disinformation techniques impact or similar.	Horizontal

[173] Summary prepared by the contractor
[174] Summary prepared by the contractor
[175] Summary prepared by the contractor

	Parliamentary Term (July 2014 - June 2019)				
125.	European Parliament and AFCO. 2020. Institutions and foreign interferences	"This study, commissioned by the European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs at the request of the AFCO Committee, assesses the EU responses to counter foreign interferences. It examines in particular the effectiveness of the EU action against foreign interferences in the 2019 European Parliament elections, the COVID-19 crisis and the issue of foreign donations to European political parties. The study concludes with specific policy recommendations to enhance the EU's responses."	High	Cf. Summary	Preparation
126.	European Parliament. 2019. Opinion on the Conference on the Future of Europe 10.12.2019	The document is an opinion of the Committee on Constitutional Affairs (AFCO) on a Conference on the Future of Europe, which had for main objective to identify what the EU did well and what needs to be improved to make the EU more democratic. The Opinion points out that the Conference should take stock of the initiatives used in the run-up to the 2019 elections in preparation of the 2024 elections.[176]	Low	Does not contain specific references to the stages of the electoral process and the use of new technologies therein.	General
127.	European Commission. 2020. First baseline reports – Fighting COVID-19 disinformation Monitoring Programme	'The Commission publishes the first set of reports provided by the online platform signatories of the Code of Practice as part of the COVID-19 monitoring and reporting programme set out in the Communication: Tackling COVID-19 disinformation - Getting the facts right'	Medium	Does not contain specific references to the stages of the electoral process and the use of new technologies therein.	General

[176] Summary prepared by the contractor

128.	European Commission. 2020. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement	The document sets out the key findings of the EC services' assessment of the implementation and effectiveness of the Code of Practice on Disinformation during its initial 12-months period of operation and provides an overview and an assessment of the implementation and effectiveness of the commitments subscribed to by the signatories of the Code.[177]	High	Assessment of the Code of Practice on Disinformation	EU legal and policy framework
129.	European Commission. 2020. Disinformation: EU assesses the Code of Practice and publishes platform reports on coronavirus related disinformation	The assessment shows that the Code has proven a very valuable instrument and has provided a framework to ensure greater transparency of platforms' policies against disinformation within the EU. At the same time, certain shortcomings have bene highlighted mainly due to the Code's self-regulatory nature, examples given are: absence of relevant key performance indicators (KPI's), lack of clearer procedures, missing structured cooperation between platforms, etc. In the fight against Coronavirus-related disinformation platforms have shown that they can further improve their performance. The crisis has also upgraded the collaborations with fact-checkers and researchers and the demoting or removing of content confirmed as false or misleading. Additional to the Code, new initiatives have been launched by the platforms such as: give visibility to authoritative content, improve user's awareness, detect and hamper manipulative behaviour, and limit advertising.[178]	Medium	The first part of this paper refers to another assessment already analysed (Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement), while the second part gives the key findings of how the platforms tackle the corona crisis, which is not related to the elections process.	Preparation
130.	European Data Protection Board.	The Guidelines focus on the use of social media as a significant development in the online environment over the	High	Cf. Summary	General

[177] Summary prepared by the contractor

[178] Summary prepared by the contractor

	2020. Guidelines 8/2020 on the targeting of social media users	past decade. They aim to clarify the role of social media providers and targeters as joint controllers of personal data, and their responsibilities under the General Data Protection Regulations (GDPR).[179]			
131.	Democracy Reporting International. 2019. Guide for civil society on monitoring social media during elections	This document provides important support regarding methodology , definitions and approaches to be used by civil society organisations on monitoring social media during election.[180]	High	Cf. Summary	General
132.	European Commission, Joint Research Centre. 2020. Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis	'In terms of methodology, four groups of actors fall within the scope of the Guidelines: social media providers, their users, targeters and other actors which may be involved in the targeting process (data brokers, data management providers, marketing service providers, ad networks and exchanges, data analytics companies etc.). The Guidelines clarify each of these groups and their role in targeting. Regard taken of the joint responsibility that may be inherent to targeters and social media provider towards social media users, the document offers guidance concerning the targeting of these users as regards the said responsibilities.'	Medium	Cf. Summary	Preparation ; Voting; Post-election
133.	Garnett, James. 2020. Cyber Elections in the Digital Age: Threats and Opportunities	'Elections are essential for delivering democratic rule, in which ultimate power should reside in the citizens of a state. This introduction argues that the management and contestation of elections have now entered a qualitative new historical period because of the combined	High	Integration of technology into the elections.	Preparation ; Voting

[179] Summary prepared by the contractor

[180] Summary prepared by the contractor

	of Technology for Electoral Integrity	development of new technology and broader sociological developments. The era of cyber-elections is marked by: (a) the new ontological existence of the digital, (b) new flows of data and communication, (c) the rapid acceleration of pace in communications, (d) the commodification of electoral data, and (e) an expansion of actors involved in elections. These provide opportunities for state actors to incorporate technology into the electoral process to make democratic goals more realizable. But it also poses major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals such as political equality and popular control of government. The article argues that this new era therefore requires proactive interventions into electoral law and the rewriting of international standards to keep pace with societal and technological change.'			
134.	Loeber. 2020. Use of Technology in the Election Process: Who Governs?	'There have been major concerns about the role of technology in elections, as highlighted by debates in different countries such as the U.S., the Netherlands, and Norway. One area of concern is that a lot of the equipment is not owned by the public sector—but there has been barely any research on election technology ownership in a comparative perspective. This article reports new data from an international survey of electoral management bodies (EMBs) (N = 78) with data from 72 countries. There are large differences between countries in the number and kinds of technology they use in the election process. An important finding is that even though most countries use some form of election technology, the use of election technology for actual voting (voting computers or Internet voting) is relatively rare. In terms of the difference between independent and governmental model EMBs, independent	High	The article discusses use of ICT technologies and electoral process. Although it does not specifically mention innovative technologies, it talks about e-voting among other activities that are supported by technologies in the electoral process.	General

		EMBs seem to be more ''in control'' of the technology used. This means that they are more likely to have a decisive role in the decision-making process and to have ownership of the technology and provide the technological support for it. These findings signal that the introduction of technology does not seem to have a negative impact on the independent position of EMBs. This means that EMBs that have a formal independent position are also in most cases independent from other actors in the election process, such as other governmental agencies and vendors, when it comes to the use of technology.'			
135.	Pal. 2020. Social Media and Democracy: Challenges for Election Law and Administration in Canada	'This article considers the challenges posed by social media for election law and administration in the Canadian context, particularly in relation to political advertising. (…) The existing legal rules that regulate electoral activity off-line appear to be largely inadequate for a world in which social media is an important part of political communication and advertising. Either they do not apply to online politics or, if they do, the law has been underenforced or exposed as out of date. The author proposes changes to the Canadian legal regime. (…) These proposals include enhanced disclosure rules for political advertising on social media, a separate social media spending limit for political parties and interest groups, and enhanced regulation of social media platforms, including by treating them as ''broadcasters'' for specific purposes under the Elections Act.'	Medium	Does not contain specific references to the use of new technologies.	General
136.	Huckle, White. 2017. Fake News: A Technological Approach to Proving the Origins	'In this article, we introduce a prototype of an innovative technology for proving the origins of captured digital media. In an era of fake news, when someone shows us a video or picture of some event, how can we trust its authenticity? It seems that the public no longer believe that traditional	High	Discusses a prototype of an innovative technology for proving the origins of captured digital media. In an era of fake news, when someone	Preparation

	of Content, Using Blockchains	media is a reliable reference of fact, perhaps due, in part, to the onset of many diverse sources of conflicting information, via social media. Indeed, the issue of "fake" reached a crescendo during the 2016 U.S. Presidential Election, when the winner, Donald Trump, claimed that The New York Times was trying to discredit him by pushing disinformation. Current research into overcoming the problem of fake news does not focus on establishing the ownership of media resources used in such stories—the blockchain-based application introduced in this article is technology that is capable of indicating the authenticity of digital media. Put simply, using the trust mechanisms of blockchain technology, the tool can show, beyond doubt, the provenance of any source of digital media, including images used out of context in attempts to mislead. Although the application is an early prototype and its capability to find fake resources is somewhat limited, we outline future improvements that would overcome such limitations. Furthermore, we believe that our application (and its use of blockchain technology and standardized metadata) introduces a novel approach to overcoming falsities in news reporting and the provenance of media resources used therein. However, while our application has the potential to be able to verify the originality of media resources, we believe that technology is only capable of providing a partial solution to fake news. That is because it is incapable of proving the authenticity of a news story as a whole. We believe that takes human skills.'		
137.	Sathiaraj, Cassidy, Rohli. 2017. Improving	'The problem of accurately predicting vote counts in elections is considered in this article. Typically, small-sample polls are used to estimate or predict election outcomes. In this study, a machine-learning hybrid approach is proposed.	Medium	Technical explanation on how AI works for predicting elections. General

	Predictive Accuracy in Elections	This approach utilizes multiple sets of static data sources, such as voter registration data, and dynamic data sources, such as polls and donor data, to develop individualized voter scores for each member of the population. These voter scores are used to estimate expected vote counts under different turnout scenarios. The proposed technique has been tested with data collected during U.S. Senate and Louisiana gubernatorial elections. The predicted results (expected vote counts, predicted several days before the actual election) were accurate within 1%.'			
138.	Kruikemeier, Sezgin, Boerman. 2016. Political Microtargeting Relationship between Personalised Advertising on Facebook and Voters' Responses	'This study examines the relationship between exposure to political personalized ads on Facebook and voters' responses toward those ads and studies the mediating role of the use of persuasion knowledge in this relationship. Results from an online experiment (N = 122) demonstrate that exposure to a personalized ad from a political party activates persuasion knowledge, which in turn leads to lower intentions to engage in electronic word of mouth, but only for those participants who recall seeing the Sponsored label. We found no effects on source trustworthiness. Adding a text explaining the practice of personalized advertising did not lead to higher levels of persuasion knowledge and did not change the responses toward the message.'	High	The article discusses political advertising in social media which is directly within the scope of this study.	Preparation
139.	European Commission, Joint Research Centre. 2018. Artificial Intelligence - A European perspective	'This report presents a European view of Artificial Intelligence (AI) based on independent research and analysis by the European Commission Joint Research Centre to inform the debate at the European level.'	Medium	This report presents a European view of Artificial Intelligence (AI) based on independent research and analysis by the European Commission Joint Research Centre to inform the debate at the European level. However, the	General

				report does not address election process related issues or impact.	
140.	European Commission, Joint Research Centre. 2019. The Future of Government 2030+: A Citizen Centric Perspective on New Government Models	'The future of government 2030+ : a citizen centric perspective on new government models' project brings citizens to the centre of the scene. The objective is to explore the emerging societal challenges, analyse trends in a rapidly changing digital world and launch an EU-wide debate on the possible future government models. To address this, the project adopts a novel approach that combines citizen engagement, foresight and design, while being rooted in recent literature from the field of digital politics and media. Our future-oriented perspective looks at possible societal, technological and economic changes to identify enablers for new forms of government from 2030+ onwards. The project intentionally does not look at path-dependencies of today's governmental institutions. On the contrary, it opens up the imagination by exploring new future forms of government that are driven by the needs of diverse stakeholders. This leads to the main question of the project: 'How will citizens, together with other actors, shape governments, policies and democracy in 2030 and beyond?'	Medium	Cf. Summary	General
141.	European Commission, Joint Research Centre. 2019. The Future of Government 2030+: Policy implications and recommendations	'The recommendations include a series of policy options and actions that could be implemented at different levels of governance systems. As these recommendations have shown, collaboration is needed across different policy fields and they should be acted upon as integrated package. Although the majority of recommendations is intended for the EU policymakers, their implementation could be more effective if done through lower levels of governance, e.g. local, regional or even national.'	Medium	Cf. Summary	Preparation ; Voting; Post-election

142.	European Union. 2012. Consolidated Version of the Treaty on European Union	Art. 2 (TEU) 'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.'	High	The Treaty is part of the EU legal framework, setting main principles of the European Union and legal basis for all other EU acts.	EU legal and policy framework
143.	European Parliament, Council of the European Union. 2002. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	'The Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)'	Medium	The rules regarding protection of personal data has been described in a more recent and up to date regulation: GDPR (2018).	Horizontal
144.	European Parliament, Council of the European Union. 2000. Directive 2000/31/EC on certain legal aspects of	The Directive establishes harmonised rules on issues such as transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. It also enhances administrative cooperation between the Member States and the role of self-regulation.	High	The Directive is part of the EU legal framework relating to provision of digital services by intermediaries, who are stakeholders in this study.	EU legal and policy framework

	information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)	The Directive exempts intermediaries from liability for the content they manage if they fulfil certain conditions.[181]		
145.	European Parliament, Council of the European Union. 2018. Directive (EU) 2018/ 1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio visual media services in view of changing market realities	'This document is an amendment to the previous Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.'	Medium	Does not contain specific references to the use of new technologies. Horizontal

[181] Summary prepared by the contractor

146.	European Commission. 2018. Recommendation on measures to effectively tackle illegal content online (C(2018) 1177 final)	Recommendations on measures to effectively tackle illegal content online such as disseminating certain information relating to terrorism, child sexual abuse, illegal hate speech or infringements of consumer protection laws.[182]	Medium	These recommendations handle all types of online crimes, including, but not focussing on, crimes related to elections. There is no mentioning of new technologies.	Horizontal
147.	European Commission. 2020. White Paper on Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65 final)	'The White Paper on Artificial Intelligence and the European data strategy are the first pillars of the new digital strategy of the Commission. They are fully aligned with the need to put people first in developing technology, as well as with the need to defend and promote European values and rights in how we design, make and deploy technology in the real economy and how we improve the services of the public sector towards the citizens.'	High	Cf. Summary	Horizontal
148.	European Commission. 2019. Building Trust in Human-Centric Artificial Intelligence (COM(2019) 168 final)	'With the focus on a more human-centric AI in Europe, new challenges have emerged for AI technologies. The learning capabilities of these digital machines enables them to take and implement decisions without human intervention. To avoid unintended harm, AI technology should be developed in a way that puts people at its centre and is thus worthy of the public's trust – compliant with law and with the ethical principles. The document refers to the Ethics Guidelines on AI of the AI HLEG, which elaborates on seven principles of a trustworthy AI.'	High	Cf. Summary	Horizontal

[182] Summary prepared by the contractor

149.	European Commission. 2018. Artificial Intelligence for Europe (COM(2018) 237 final)	'The Strategy on AI for Europe places people at the centre of the development of AI (human-centric AI). It is a three-pronged approach: to boost the EU's research and industrial capacity and AI uptake across the economy, to prepare for socio-economic changes, and to ensure an appropriate ethical and legal framework. The Strategy identifies the necessity of coordinated actions and common efforts in order for the EU to stay at the forefront of the AI uptake and to ensure that EU values are respected. These actions should include, among others, increased investments in AI, research and innovation, increased data availability, increased trainings and digital awareness. '	High	Cf. Summary	Horizontal
150.	European Commission. 2018. Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)	'Delivering on the Strategy on AI for Europe, adopted in April 2018, the Commission presented a coordinated plan for joint actions between the Commission and the Member States. The Coordinated plan sets as its main objectives: the promotion of the common efforts of the Member States (e.g. in adopting national strategies); the fostering of public-private partnerships; and the financing of start-ups and innovation enterprises. It also focuses on security-related aspects of the AI applications and infrastructure.'	High	Cf. Summary	Horizontal
151.	European Commission. 2018. Towards a common European data space (COM(2018) 232 final)	'The article presents a package of measures proposed by the Commission, in view of establishing a common data space in the EU. These measures include: the re-use of public sector information; update of the Recommendation on access to and preservation of scientific information; and guidance on sharing private sector data.'	High	Cf. Summary	Horizontal
152.	European Data Protection Supervisor. 2018. Opinion 3/2018 on	'The ensuing debate has revolved around the misleading, false or scurrilous information ('content') served to people with the intention of influencing political discourse and elections, a phenomenon come to be labelled 'fake news' or	High	The Opinion discusses issues and threats related to the use of social media by political advertisers using databases and artificial	General

	online manipulation and personal data	'online disinformation'. Solutions have focused on transparency measures, exposing the source of information while neglecting the accountability of players in the ecosystem who profit from harmful behaviour. Meanwhile market concentration and the rise of platform dominance present a new threat to media pluralism. For the EDPS, this crisis of confidence in the digital ecosystem illustrates the mutual dependency of privacy and freedom of expression. The diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy. This Opinion is therefore concerned with the way personal information is used in order to micro-target individuals and groups with specific content, the fundamental rights and values at stake, and relevant laws for mitigating the threats.'		intelligence to micro-target individuals online, which is can be applied horizontally to the electoral process.	
153.	European Commission. 2016. Code of Conduct on Countering Illegal Hate Speech Online	In 2016, The European Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online". This agreement aimed to prevent and counter the spread of illegal hate speech online.[183]	Medium	Reference discusses the uses and impact of new techniques - hate speech - in a broader context, which could be horizontally applicable to the electoral process and its stages.	General
154.	European Union. 2000. The Charter of Fundamental Rights of the European Union	Enshrines through a range of personal, civil, political, economic and social rights in the EU, such as right of personal data protection (Art.8), freedom of expression and information (Art. 11), right to vote and to stand as a	High	Only some articles in the Charter relate to the rights of EU citizens in relation to the use of technology in elections	EU legal and policy framework

[183] Summary prepared by the contractor

	(CFR) [2012], OJ C 326/391 (Art. 8, 11, 39, 40 and others) (2000/C 364/01)	candidate at elections to the European Parliament (Art. 39), and municipal elections (Art. 40).[184]			
155.	Terzis et al. 2020. Disinformation and Digital Media as a Challenge for Democracy	'The book discusses diverse academic and professional comments from all over the world, touching upon topics that range from the theoretical approaches to and the conceptualisation of disinformation, to the experiences of dealing with disinformation, to the solutions for dealing with disinformation and their critique.'	High	This book is motivated, to a large extent, by some recent troubling developments in public discourse, namely the developments in information, misinformation and disinformation practices. From the beginning of history, various and diverse means or channels of communication have been used to inform, misinform (unintentionally) and disinform (deliberately). However, in recent decades, the emergence and development of new information and communications technologies (ICT), combined with the ever-increasing digitalisation and globalisation of almost every aspect of modern life, among others, have opened up new and uncharted avenues to that end. This book therefore focuses on disinformation practices occurring with the help of digital media as these practices bring to the fore	General

[184] Summary prepared by the contractor

				profound negative ramifications for the functioning of a democratic polity	
156.	Broadband Commission for Sustainable Development. 2020. Balancing Act Countering Digital Disinformation While Respecting Freedom of Expression	'Targeted analyses and recommendations address the life cycle of online disinformation: from production to transmission, reception and reproduction. The chapters could be of special interest to legislators and policy makers (counter disinformation campaigns, electoral-specific responses, the Freedom of Expression Assessment Framework); Internet companies, producers and distributors (content curation, technical and algorithmic, advertisement policy, demonetisation responses); journalists, investigative researchers and fact checkers; universities and applied and empirical researchers; target audiences (educational, ethical and normative, empowerment and credibility labelling responses). The findings are organised into a typology of 11 different categories of responses to disinformation – ranging from identification and investigatory responses, through to policy and legislative measures, technological steps, and educational approaches. For each category of response, the reader will find a description of work being done around the world, by which actors, how it is funded and who or what is targeted. The report further analyses the underlying assumptions and theories of change behind these responses, while weighing up the challenges and opportunities. Each category of response is also assessed in terms of its intersections with the universal human right of freedom of expression, with a particular focus on press freedom and access to information. Finally, case studies of responses to COVID-19 disinformation are presented within each category. At the heart of this knowledge product is the	High	Discusses the impact of disinformation in different social life areas, including on elections.	General

		need to balance responses to disinformation with respect for freedom of expression. The research shows us that this can be done.'			
157.	Civitates. 2019. 2019 Annual Report	This is the organisation's 2019 annual report reflecting Civitates' journey throughout 2019: how within Civates line of work aimed at a strong and resilient civil society, granting 'that partners have been consolidating the work of their cross-sectoral coalitions'. Moreover, it touches upon Civates new line of work, to 'support the field of independent, public interest journalism in Europe.'[185]	Medium	Does not contain specific references to the stages of the electoral process and the use of new technologies therein.	General
158.	Council of Europe. 2001. Convention on Cybercrime	This convention serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.[186]	Medium	This document tackles cyber-crimes of the early ages of internet. No reference of new technologies, or specifically to elections.	General
159.	Council of Europe. 2017. 1289th meeting - Democracy and Political Questions	'The present guidelines are the updated version of the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections. The original two guidelines were approved in 2011 with the aim of providing guidance on how to implement the provisions on certification and transparency of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting of 30 September 2004.'	High	Discusses e-Voting	EU legal and policy framework; Voting
160.	DebunkEU. 2020. 70 % of the	'NATO's Defender Europe 2020 exercise, scheduled for May in Eastern Europe, was set to become the Alliance's largest	Medium	This is a blogpost and therefore not part of an EU policy or legal	General

[185] Summary prepared by the contractor

[186] Summary prepared by the contractor

	information about the NATO exercise Defender 2020 was misleading	exercise on the continent since the Cold War, with the United States and other NATO partners planning to deploy about 37,000 soldiers. Since September last year, Debunk EU has recorded a great stir in Russian-speaking portals by disinforming the public – more than 400 publications about these exercises appeared, most of which (70%), were misleading.'		framework, scientific article or analytical piece of literature. It does not refer to elections, however its views related on disinformation and foreign interference can be horizontally applied to elections.	
161.	DebunkEU. 2020. 70 % of the information about the NATO exercise Defender 2020 was misleading	This document contains the findings of the NATO's Defender Europe 2020 exercise analysis. 'Debunk EU has recorded a great stir in Russian-speaking portals by disinforming the public — more than 400 publications about these exercises appeared, most of which (70%), were misleading.'	Medium	Does not contain specific references to the stages of the electoral process and the use of new technologies therein.	General
162.	DebunkEU. 2020. COVID-19 related disinformation becomes a tool to promote anti-Baltic narratives	'As global health organisations keep voicing their concerns about alarming rates of COVID-19 cases, specialists are also warning about the infodemic which was inflicted by the coronavirus. Debunk EU analysis has shown that false and misleading information about COVID-19 did not only affect public perception of the virus in the Baltic countries but was also used to validate Kremlin-promoted clichés.'	Medium	This article shows the political use of disinformation in general, not specifically in an electoral environment.	General
163.	DebunkEU. 2020. Disinformers take an advantage of COVID-19 crisis	'As global health organizations keep voicing their concerns about alarming rates of COVID-19 cases, specialists are also warning about the infodemic which was inflicted by the coronavirus. Debunk EU analysis has shown that false and misleading information about COVID-19 did not only affect public perception of the virus in the Baltic countries but was also used to validate Kremlin-promoted clichés.'	Medium	Discusses COVID-19 disinformation in the Baltics	General
164.	DebunkEU. 2020. Election fraud in Belarus brought a surge of pro-	'The events in Belarus, where people are protesting after the implicit falsification of the results of presidential election, were topical in the media agenda-setting in August. Therefore, it is not surprising that the pro-Kremlin propaganda actively used this topic too. In its own	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature. It does not refer to elections,	General

	Kremlin propaganda	narratives about Belarus, it reserved special places for the Baltic states (especially for Lithuania). The Baltic states, together with other regional countries, were presented as the provokers of the protests.'		however its views related on disinformation and foreign interference can be horizontally applied to elections.	
165.	DebunkEU. 2020. Irrelevant and insignificant depiction of the Baltics in pro-Kremlin media	'With the focus slowly moving away from the political upheaval in Belarus, the ever-present narrative of Russophobia is regaining its popularity in the Kremlin-related media. This rhetoric goes in line with depicting Lithuania, Latvia, and Estonia as irrelevant, irrational, and incompetent players in the international arena, as well as in their domestic affairs. Throughout the 1st - 31st of October, Debunk EU analysts found 666 articles with false and misleading content from 53 pro-Kremlin media outlets in the Baltic states in English, Estonian, Latvian, Lithuanian, and Russian languages. The articles had a potential reach of 216.8 million contacts.'	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature.	General
166.	DebunkEU. 2020. Irrelevant and insignificant depiction of the Baltics in pro-Kremlin media	Analysis of number of false articles and misleading content from 53 pro-Kremlin media outlets in the Baltic states in English, Estonian, Latvian, Lithuanian, and Russian languages.[187]	Medium	Statistical representation of detected misinformation related to the Baltic countries. No in-dept analysis of the risks to free and fair democracy.	General
167.	DebunkEU. 2020. NATO drills, COVID-19 rules , alleged interference in Belarus used to	'While the second wave of COVID-19 is raging, the pandemic still is at the core of false/misleading information targeting Lithuania, Latvia, Estonia, and Poland. Accusations of not being able to handle the crisis, spread by the Kremlin related media, doubled down on the ever-present narratives of Baltic countries and Poland serving the West by interfering	Medium	Discusses COVID-19 disinformation in the Baltics and Poland	General

[187] Summary prepared by the contractor

	target the Baltics and Poland	in Belarus and allowing NATO military exercises on their territory.'			
168.	DebunkEU. 2020. Negative communication creates an impression of no real political choice in Lithuanian elections	'While a notorious contest for voter 's attention was raging in the public space, there were repeated attempts in digital media to discredit Lithuanian Seimas elections and discourage citizens from voting. Debunk EU research has shown that during the election campaign negative communication in digital news outlets was directed towards three main targets: voting process itself, elections management body, and participants of the elections (candidates and political parties). It was noticed that negative publications were attempting to create an impression, that there is no political force in Lithuania which is capable to represent their constituents.'	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature.	Preparation
169.	DebunkEU. 2020. Negative posts on Facebook sought to discredit democratic processes in Lithuania	'With the new government starting their term, Lithuanian parliamentary election of 2020 is still in the spotlight. Political campaigns often become subjects of attempts to discredit, spread divisive narratives, and confuse voters by spreading false/misleading information. The main targets of negative communication on Facebook concerning the election were electoral process, electoral management body, and participants in the election themselves. According to Debunk EU, those messages potentially sought to discourage people from voting because of COVID-19 pandemic, discredit the Central Electoral Commission, and enhance the negative attitude towards the political system in Lithuania.'	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature.	General
170.	DebunkEU. 2020. Political unrest in Belarus keeps fuelling disinformation	'Belarusian political turmoil still influences coverage about neighbouring Estonia, Latvia, and Lithuania in pro-Kremlin media. Throughout the month of September, Debunk EU experts analysed 1,567 articles with false and misleading content from 74 pro-Kremlin media outlets. Those pieces	Medium	Statistical representation of detected misinformation related to the Baltic countries. No in-dept analysis of the risks to free and fair democracy.	General

	against Baltic states	included various accusations — from imputing Baltic countries for stirring up the crisis in Belarus, to accusing them of growing support towards neo-Nazism'			
171.	DebunkEU. 2020. Russian media Belarusian opposition is anti-Russian and is selling itself to the West	'After Alexander Lukashenka has secretly inaugurated himself for one more term in September, the protests in Belarus have erupted with a new force. Even though right after the election Russian media was quite critical towards Belarusian regime, after Lukashenka called and met with Vladimir Putin several times, the tone has become way calmer. According to Debunk EU, compared to August, throughout September and October Russian media was eager to attack the West for interfering in Belarusian affairs and influencing the opposition leader Sviatlana Tsikhanouskaya.'	Medium	Discusses Russia media attacking the West for interfering in Belarusian affairs and influencing the opposition leader Sviatlana Tsikhanouskaya.	General
172.	DebunkEU. 2020. Softening criticism towards Lukashenko in pro-Kremlin media - fading power of the Belarusian regime	'The results of Belarusian presidential election have brought protests to an anticipated scale. The fight for the democratic future began not only on the streets, but also in the virtual space. Pro-Kremlin media is also heavily involved. Debunk EU analysts have noticed that the assessment of Alexander Lukashenko regime in Russian media started to change after Lukashenko called and talked to Vladimir Putin. This insight was made after analysing 1209 articles which appeared in the biggest Russian information channels throughout the month of August.'	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature.	General
173.	DebunkEU. 2020. US organisation expands its cooperation with Lithuanians in the fight against Chinese disinformation	'The Alliance for Securing Democracy, an independent organisation operating in the United States, just a few weeks earlier has launched a monitoring of misleading information in China. A new version of the "Hamilton" dashboard, which has so far been used to track Russian disinformation, has been developed for this purpose. The AI based tool "Debunk.eu", created by Lithuanians, has previously been included in "Hamilton" to monitor Russian	Medium	This is a blogpost and therefore not part of an EU policy or legal framework, scientific article or analytical piece of literature.	General

		information channels, and consequently, this cooperation has been extended to China's disinformation monitoring. According'			
174.	DebunkEU. 2020. With a dramatic surge of COVID-19 cases, Baltic states may be facing the second wave of infodemic	Debunk analysis on disinformation related to COVID-19 in the Baltic countries.[188]	Medium	Statistical representation of detected misinformation related to the Baltic countries. No in-dept analysis of the risks to free and fair democracy.	General
175.	Democracy Reporting International. 2020. Lessons Learned Social Media Monitoring during Humanitarian Crises	'Where do you start if you want to monitor social media during elections? To help get you started, DRI's Madeline Brady summarizes lessons learned from five projects that covered national elections across Europe in 2019 and 2020. We dive into each project, provide examples for teams deciding on what to monitor, how to assemble a team and other critical questions. The lessons learned from these five projects show that further steps are needed from government, social media companies and research institutions to improve the quality of monitoring work by civil society. For example, civil society groups require clear processes to access data from companies and access to additional metrics to successfully monitor social media. DRI is also working on other tools to address the challenges faced by social media monitoring teams, which will be available in July 2020.'	High	Discusses Case Studies from five EU Elections 2019-2020 Funded	Preparation ; Voting; Post-election
176.	Election Observation and Democratic	'Elections provide examples of human rights in practice. Achieving a genuine, democratic electoral process is part of establishing a system of government that can ensure	Medium	Cf. Summary	Preparation ; Voting;

[188] Summary prepared by the contractor

	Support. 2016. Compendium of International Standards for Elections	respect for human rights, the rule of law and the development of democratic institutions. The European Union has a long tradition of supporting human rights, democracy and the rule of law throughout the world, and these principles are enshrined in the basic EU treaties as fundamental values. In this context, election observation constitutes an important EU foreign policy and external assistance instrument. This Compendium provides an overview of international standards for elections, the key relevant texts, a matrix of the commitments of individual states, information on standards by area of assessment and a list of useful references for further information. This fourth edition also includes an explanation of human rights protection systems and election-related jurisprudence. It is complemented by an online database of international election-related caselaw, available at www.eods.eu. The Compendium is primarily designed for people working on EU election observation missions (EU EOMs), but may also be useful to interested stakeholders and analysts, including parliamentarians and lawmakers, election administrators, other international observer groups, citizen observers, candidates and parties, implementers of technical assistance and other interested stakeholders. International standards provide those interested in an election with a tool for assessing the process according to agreed criteria for genuine elections. It is the EU's expectation that EU EOMs will make regular use of this tool to assess the conduct of elections in line with international standards and ensure coherence among EU EOMs.'			Post-election
177.	Election-Watch.eu. 2019. Elections to the European	'Election-Watch.EU conducted this EAM with the objective of raising awareness of the importance of the European elections, promoting good practices, contributing to	Medium	Cf. Summary	Post-election

	Parliament Election Assessment Mission - Final Report	European electoral integrity and providing recommendations to further strengthen European electoral processes. Upcoming electoral reform advocacy will target newly elected MEPs, EU governments and political parties to demonstrate commitment to UN, EU, Council of Europe and OSCE standards and commitments. An underlying objective is to strengthen civic engagement in European electoral processes, with a special focus on youth participation. The EAM also aimed for the recognition of the value of non-partisan election observation not only outside the EU, but also within Europe, to further strengthen European democracies.'			
178.	Election-Watch.EU. 2020. Rapid Assessment Covid-19 & Elections in Europe	The Election-Watch.EU Rapid Assessment takes stock of the current impact of Covid-19 on elections in Europe.[189]	Medium	More related to the COVID-19 impact on elections than on the technology impact.	Preparation ; Voting; Post-election
179.	EU DisinfoLab. 2020. Covid-19 Disinformation Narratives, Trends, and Strategies in Europe	'As the virus swept across the world, they decided to zoom into the narratives defining what the WHO term as "the infodemic". Based on our monitoring of independently fact-checked disinformation from France, Italy, and Spain, we have been able to draw trends from the content, such as the strategies and platforms used to disinform. They have analysed the time period from the end of January to the last week of March and accordingly noticed an evolution in the disinformation.'	Medium	Discusses COVID-19 disinformation	General
180.	EU DisinfoLab. 2019. The Suavelos galaxy - a	'They say they're "positive and not depressive", "confident and not defeatist", and "open and non-elitist". But the Suavelos' creators claim to be mostly "white nationalists",	Medium	This is a blogpost in the disinfo.eu website and not an official article. It does not refer to elections,	General

[189] Summary prepared by the contractor

	showcase of uninhibited racism	and even – quite simply – "racist". This website, prized by some of the French far right, defends the idea that the "ethnic" issue takes precedence over others. These nationalist messages expose the movement to the moderation of platforms such as Facebook and YouTube, which have hardened their tone in 2019 since the Christchurch attack and the El Paso shooting, which was perpetrated by white supremacists. Yet the Suavelos network does not disarm in the face of what it considers to be "censorship", and multiplies their initiatives, creating secondary Facebook pages, Telegram channels, online chatrooms, an association for concealed purposes, etc. The authors put all the pieces of this puzzle together, with the cooperation of the Belgian NGO EU DisinfoLab, which specialises in disinformation research in Europe. And it appears that Suavelos does not lack the imagination to spread their racist thinking and strives to reach a wider audience than the nationalist fringe.'		however, it provides interesting views about hate speech, crowdfunding and advertising on Facebook, which may have implications on the elections as well.	
181.	European Commission. 2020. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European	'EU action plan to create a fair democracy in a digital world. Including topics such as: rules on the financing of European political parties; implement professional standards; support media pluralism; Improving EU and Member State capacity to counter disinformation; More obligations and accountability for online platforms; Empowering citizens to make informed decisions.'	High	tackles all topics related to democracy and elections.	EU legal and policy framework

	Democracy Action Plan				
182.	EU DisinfoLab. 2019. Voter suppression campaigns in Spain No contéis conmigo #Yonovoto (Don't count on me #Idon'tvote)	The article elaborates on the event before the Spanish 2019 elections, to discourage voters to go voting.[190]	Medium	Although the voter suppression happens also via fake Facebook accounts, the main focus of the article is on why it happened and who did it. No focus on technology itself.	Preparation ; Voting
183.	EU DisinfoLab. 2020. How two information portals hide their ties to the Russian news agency InfoRos	'In March 2020, EU DisinfoLab stumbled across articles from a French website called "ObservateurContinental.fr" which had spread disinformation related to COVID-19, including an article repropagating an interview with the US professor of international law Francis Boyle, who had falsely asserted without evidence that the "COVID-19 is a perfect biological weapon". Based on this, EU DisinfoLab began to look deeper into Observateur Continental and uncovered that two information portals (oneworld.press and observateurcontinental.fr) hide their ties to InfoRos – a news agency previously linked to Russian military intelligence (GRU), according to reports by the Washington Post and Stanford Internet Observatory.'	Medium	Discusses COVID-19 disinformation	General
184.	Who Targets Me. 2020. How to take a "gold standard" approach to political	The article briefly introduces some issues related to political advertising. It then proposes six "gold standards" for the improvement of the transparency of the online political advertising. As the interests of civil society, private companies, political parties and other stakeholders are	High	Cf. Summary	Preparation

[190] Summary prepared by the contractor

	transparency and policy	considerable different, the proposed six "gold standards" acceptance will depend on the discussion and balance of the trade-offs between those stakeholders.[191]			
185.	European Centre for Electoral Support European Partnership for Democracy. 2016. EURECS A European response to electoral cycle support	'EU electoral support revolves around two activities: election observation and electoral assistance. While election observation focuses on the process close to the electoral event, electoral assistance may be provided throughout the entire electoral cycle. (…) Taking into account the lessons learned by ECES and the members of EPD, particularly in the last five years, have devised and are currently implementing a joint "European response to electoral cycle support", also known as EURECS. This strategy encompasses a practical implementation approach to electoral support, informed by past experience also from EUEOMs. The strategy builds on several key objectives, which are in line with the EU Action Plan on Human Rights and Democracy (2015-2019).'	Medium	The document elaborates on two main activities regarding EU electoral support - election observation and electoral assistance - but does not contain specific references to use of new technologies or new techniques.	Preparation ; Voting; Post-election
186.	European Centre for Electoral Support. 2018. Opportunities and Challenges in the Use of Technology in Elections Experience from West and Southern Africa	Conference on then use of technology in the elections in Nigeria, sponsored by the European Centre for Election Support.[192]	Medium	This document is only an elaborate leaflet for a conference for the use of technology in elections in Nigeria.	Preparation ; Voting; Post-election

[191] Summary prepared by the contractor

[192] Summary prepared by the contractor

187.	European Centre for Electoral Support. 2020. Delivering Electoral and Democracy Support Under COVID-19 ECES Preparedness and Responses	'The spread of the coronavirus (COVID-19) pandemic has reached unprecedented levels across the globe. Together with its impact on health systems and economies, the crisis also bears lesser known long- and short-term consequences for elections, democracy, and countries' security. This paper aims to inform on the responses the European Centre for Electoral Support (ECES) has been developing and bringing to its beneficiary countries and partners amid the health crisis, while honouring its donors' values and requirements.'	Medium	Discusses the ECES response to deliver electoral and democracy support under COVID-19	General
188.	European Citizen Action Service. 2019. Digital Democracy Day 2019 Report on Harnessing the Potential of Technology in Elections	'On 7 March 2019, ECAS held its fifth annual Digital Democracy Day - Harnessing the Potential of Technology in Elections - focused on the use of Information and Communications Technology (ICT) to engage citizens in political elections, with a particular focus on the 2019 European Parliament elections. The event was organised in the framework of the YOU VOTE EU project, under the European Union's Rights, Equality and Citizenship Programme of the European Commission. As part of this project, ECAS and its partners developed "Your Vote Matters", an online participative platform that engages European citizens in the 2019 European Parliament elections by informing and connecting them with their current representatives or new candidates. More than 70 participants from 20 different countries took part in the conference, which was also livestreamed and reached over 2000 people online.'	Medium	This is report summarizing the discussions from the Digital Democracy Day and is therefore not part of the policy and legal framework, or a scientific article or an analytical piece of literature.	General
189.	European Citizen Action Service. 2019. Online Disinformation Finding the Silver	'ECAS's conference "Online Disinformation: Finding the silver bullet in the digital world", organised in partnership with the European Economic and Social Committee (EESC), focused on exploring possible solutions to countering online disinformation, from potential regulatory approaches to efficient initiatives and actions to empower citizens. The	Medium	This is a report from event held by ECAS on the topic of online disinformation. It does not explore or provide specific references regarding the use of new technologies on elections.	General

	Bullet in the Digital World	event took place on 12 November 2019 and discussed with distinguished speakers and an engaged audience if there is a silver bullet capable of building the necessary resilience in our society to ensure a prosperous, safe and democratic digital future for European citizens.'			
190.	European Economic and Social Committee. 2019. Societies outside Metropolises the role of civil society organisations in facing populism	An analysis to provide guidelines to help us better understand the rise of the phenomenon of populism across the entire EU.[193]	Medium	The focus lays on the history and evolution of populism in different countries, not so much on the use of technology in elections.	General
191.	European Free Aliance. 2016. 2019 Manifesto	This 2019 EFA manifesto lays the policy foundations for this group. It will provide a common basis throughout the 2019-2024 parliamentary term.[194]	Low	Discusses the EFA Manifesto for 2019-2024 parliamentary term	General
192.	European Partnership for Democracy. 2020. Universal Advertising Transparency by Default	'The political campaigning landscape has changed significantly with the digitalisation of our public sphere, which has created new opportunities for political participation, but also poses significant risks to the integrity of elections and political debate. Unlike broadcast political ads shown to the wider public, online ads are tailored to specific homogenous groups of people, which can segment and polarise the voter base and distort political debate. Advertisers can purchase exorbitant amounts of ads and flood people's social media feeds, thereby buying themselves space in public policy and political debates. The	Medium	Does not directly discuss use or impact of new technologies in electoral context, however the views expressed may be applied horizontally on elections.	General

[193] Summary prepared by the contractor

[194] Summary prepared by the contractor

		lack of transparency of which ads are shown to whom, why, and who has paid for them, further creates a situation where anyone - from a political party and interest group to a foreign advertising firm like Cambridge Analytica - can distort political debate and easily evade public interest scrutiny. This threatens the credibility of our electoral processes, and ultimately the legitimacy and representativeness of our democracies.'			
193.	Finnish Ministry of Justice. 2020. National Democracy Program 2025 plan of action	'This document is the National Democracy Program Action Plan for 2020. The action plan is a document based on and supplemented by the entries in the government program during the programming period on the basis of an assessment of the situation and consultations. The action plan defines measures and timetable for democracy projects during the government term. The action plan is updated annually. On the basis of the action plan, a report will be drawn up in 2022 Government decision - in - principle on the democracy program for 2025.'	Medium	Cf. Summary	General
194.	Gibson et al. 2016. A review of E-voting the past, present and future	'Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many	High	Elaborates on E-voting in elections.	Voting

		different types of election throughout the world for several decades.'			
195.	Groupe d'Experts Belge sur les fausses Informations et la Désinformation. 2018. Rapport du Groupe d'Experts Belge sur les fausses Informations et la Désinformation	'On May 2, 2018, the Minister of the Digital Agenda launched an expert consultation on fake news and the spread of disinformation on the internet. The expert group was tasked with formulating recommendations and proposals to combat these two phenomena. The experts were invited to make recommendations on the regulations and the position to be adopted by Belgium during international meetings, but also to put forward concrete proposals to set up in Belgium a "laboratory" in order to fight against false information and disinformation spread on the internet.'	Medium	Discusses fake news and disinformation	General
196.	Huotarinen et al. 2020. Election Information System life cycle assessment (Finnish Ministry of Justice)	Not available in English	Medium	The report is provided in Finnish and does not have an official EN translation. Although it describes an assessment the life-cycle of an election information system, it does not refer to use of new technologies in the electoral context	Preparation ; Voting; Post-election
197.	International Foundation for Electoral Systems. 2018. Cybersecurity in Elections, Developing a Holistic Exposure and Adaptation Testing	'Most countries now automate and digitalize at least part of their elections, from the use of e-voting to electronic voter databases. The issues around cybersecurity in elections are therefore increasingly universal and are becoming more complex.' This document elaborates on types of Cybersecurity Exposure in Elections, namely, technology, human or procedural exposure. It briefly elaborates on the	Medium	This article exposes the what are the main Cybersecurity Exposure in Elections. However, does not develop into detail on the use of new technologies in the overall electoral process	Preparation ; Voting; Post-election

		use of Electronic Voting Machines in India, Germany and Finland.[195]			
198.	Kofi Annan Foundation. 2019. The Internet's Challenge to Democracy Framing the Problem and Assessing Reforms-annotated	Analyses specific dangers of the internet and technologies on the elections, and reform options to combat these digital dangers to democracy.[196]	High	Analyses the impact of the internet and technologies on the elections.	Preparation ; Voting; Post-election
199.	Kofi Annan Foundation. 2020. The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age	'New information and communication technologies (ICTs) pose difficult challenges for electoral integrity. In recent years foreign governments have used social media and the Internet to interfere in elections around the globe. Disinformation has been weaponized to discredit democratic institutions, sow societal distrust, and attack political candidates. Social media has proved a useful tool for extremist groups to send messages of hate and to incite violence. Democratic governments strain to respond to a revolution in political advertising brought about by ICTs. Electoral integrity has been at risk from attacks on the electoral process, and on the quality of democratic deliberation. The relationship between the Internet, social media, elections, and democracy is complex, systemic, and unfolding. Our ability to assess some of the most important claims about social media is constrained by the	High	Discusses new technologies in elections	Preparation ; Voting; Post-election

[195] Summary prepared by the contractor

[196] Summary prepared by the contractor

		unwillingness of the major platforms to share data with researchers'			
200.	Krimmer, Duenas-Cid, Krivonosova. 2020. Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly?	'During a pandemic, many countries and organizations must decide whether to postpone upcoming elections or to hold them (Krimmer et al., 2020a). If the decision is made to hold the election, three main scenarios come to mind: continue using the existing system but include measures to ensure the health of participants; or look for alternatives among remote voting channels which could ensure social distancing is guaranteed either by postal voting, or internet voting.'	Medium	The article discusses alternatives; however, it does not refer to use of new technologies in the electoral context.	General
201.	Krimmer, Duenas-Cid, Krivonosova. 2020. New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?	'New ways of voting in elections are being sought by electoral administrations worldwide who want to reverse declining voter turnouts without increasing electoral budgets. This paper presents a novel approach to cost accounting for multi-channel elections based on local elections in Estonia. By doing so, it addresses an important gap in the academic literature in this field. The authors confirm that internet voting was most cost-efficient voting channel offered to Estonian voters.'	Medium	This article develops on a new approach to calculate costs for multi-channel elections but does not contain specific references to the use of new technologies.	Voting
202.	Krimmer. 2012. The evolution of e-voting why voting technology is used and how it affects democracy	Describes the evolution of e-voting, motivating factors to choose for e-voting, and how it affects democracy.[197]	Medium	Elaborates on E-voting in elections, but this article is mostly an older 'review on e-voting' , while a more recent 'review on e-voting' (even including same authors) from 2016 "Gibson et al. 2016. A review of E-voting the	Voting

[197] Summary prepared by the contractor

				past, present and future", is already included in this literature list.	
203.	Krimmer. 2016. Constitutional Constraints for the Use of Information and Communication Technologies in Elections	'Electronic elections are increasingly popular worldwide. Almost every discussion addressing the introduction of electronic processes into an election begins with the question of whether such a system would be in line with existing legislation. Here we outline the basic regulations that can be derived from constitutional rules, electoral principles and special case law on the matter. Based on our findings, we propose principal considerations for developing a legal basis for the introduction of electronic elections.'	High	Discusses electronic elections	Preparation ; Voting; Post-election
204.	Krimmer. 2016. Internet Voting in Austria History, development and building blocks for the future	This dissertation aims to investigate the origins of Internet voting, analyse several deployments of Internet voting technology in Austria and identify – based on these accumulated experiences – building blocks that can be useful in decision-making on and planning of future uses of Internet voting technology within Austria and throughout the world. In line with the goals of this thesis, it will address the following research questions: - How did Internet voting originate? - What experiences were noted in the process of implementing Internet voting in Austria? - What building blocks can be identified for developing future Internet voting both inside and outside Austria?[198]	High	Discusses use case of Internet voting in Austria	Voting
205.	Lie Detectors. 2018. European Commission's drive to tackle Fake News and Digital	This document is a press release on the 'European Commission's drive to tackle Fake News and Digital Disinformation needs fast action on education and independent funding guarantees'. Therefore, not part of an	Medium	Cf. Summary	General

[198] Summary prepared by the contractor

	Disinformation needs fast action on education and independent funding guarantees	EU policy or legal framework, scientific article or analytical piece of literature.[199]			
206.	Moravian Land Movement. 2020. Long-term program	This document is a Czech political movement long term program of actions and intentions on different political views such as education, elections, economy, etc.[200]	Low	It barely touches the topic of elections.	General
207.	Organization for Security and Co-operation in Europe. 2010. Election Observation Handbook (Sixth edition)	'This handbook sets out the ODIHR's observation methodology and serves as a reference for all ODIHR election observers. It informs the OSCE community at large, including governments of participating States, political parties, candidates, voters, media and civil society, as well as other international organizations, about the basis for the planning, deployment and implementation of and follow-up to an election observation mission (EOM). Further, it elaborates the process by which elections in OSCE participating States are assessed for their compliance with the Organization's election-related commitments, other international standards for democratic elections and national legislation.'	Medium	Discusses election observation methodology	Preparation ; Voting; Post-election
208.	Organization for Security and Co-operation in Europe. 2013. Handbook for the Observation of	This handbook is designed to provide basic guidance on how to observe the use of new voting technologies (NVT) in electoral processes. Several OSCE participating States have implemented or tested NVT during their elections, making use of electronic voting machines, ballot scanners, Internet voting or other electronic means. This handbook is designed	High	Analyses the context for new voting technologies and provides an assessment of them.	Voting

[199] Summary prepared by the contractor

[200] Summary prepared by the contractor

	New Voting Technologies	to assist election observers in identifying and assessing the various elements of NVT that may impact the conduct of democratic elections.[201]			
209.	Organization for Security and Co-operation in Europe. 2020. Alternative voting methods and arrangements	'This paper provides a review of various voting methods and arrangements that depart from the traditional paper-based voting in polling stations on election day and analyses them from the perspective of applicable international standards and good practice. It aims to provide guidance for election management bodies (EMBs) and legislators as they consider a shift towards, or an expansion in use of, such alternative methods and arrangements. To facilitate a critical and comprehensive evaluation of the available options, the paper identifies both the benefits and possible pitfalls associated with the different solutions and offers guiding questions and considerations to help design responses that take account of potential risks.'	Medium	The term New Voting Technologies as defined in this paper refers to the use of information and communication technologies for casting and counting of votes. This typically includes the use of electronic voting machines to cast votes, in-polling station ballot scanners, and Internet voting. Thus, does not develops on the use of new technologies defined in the context of this study which includes Artificial Intelligence, Blockchain or Internet of Things.	Preparation ; Voting
210.	Organization for Security and Co-operation in Europe. 2020. Human Dimension Commitments and State Responses to the Covid-19 Pandemic	'This report aims to help OSCE participating States learn lessons from the Covid-19 pandemic in order to strengthen their institutions ahead of future challenges. It begins with an overview of obligations when declaring a state of emergency and any attendant restrictions on fundamental freedoms and human rights and goes on to describe the impact of the emergency measures implemented around the OSCE region on democratic institutions and human rights.'	Medium	This repost studies the impact of COVID on democracy and human rights. In the matter of elections many other distance voting procedures were proposed (postal voting, election duration, voting in advance) instead of new technological solutions.	General
211.	Roscoe. 2020. What are we to do	This blog post is the product of a series of conversations among EU-based civil society organisations on policy	Medium	Discusses microtargeting	Preparation

[201] Summary prepared by the contractor

	about microtargeting	options related to political ads, transparency and microtargeting.[202]			
212.	The European Consumer Organisation. 2020. BEUC's comments on the EDPB's Guidelines on the Targeting of Social Media users	'Social media plays a central role in the daily lives of consumers. Thanks to sophisticated algorithms and techniques that monitor and analyse how consumers use their services social media companies can create detailed profiles of consumers. These profiles are then used to offer products and services to consumers and target them with specific information and content based on their declared, observed or inferred commercial, political, or other interests. Having such intimate knowledge of consumers' preferences endangers their privacy and data protection right as well as their autonomy and freedom of choice. This can also have serious consequences for society at large. The information collected can be used to exploit consumers' vulnerabilities and unduly influence their choices and behaviour, for example by targeting sports betting ads towards people struggling with gambling addictions. It is necessary to ensure that social media companies respect the GDPR and do not use consumers' personal data in ways beyond their knowledge and control to target them and manipulate their behaviour. BEUC welcomes and supports the guidelines of the European Data Protection Board (EDPB) and the efforts made by the Board to clarify key aspects for a respectful and legitimate use of consumers' personal data by social media platforms and targeters.'	Medium	Does not discuss electoral process and new technologies used therein, however targeting of social media users is an issue in the electoral context as well, therefore the BEUC's opinion could be used horizontally.	General
213.	The European Consumer Organisation.	'In response to the European Commission's White Paper on Artificial Intelligence, BEUC prepared recommendations to design a regulatory framework for Artificial Intelligence (AI)	Medium	This document develops on the use of new technologies, especially AI, however in a much	General

[202] Summary prepared by the contractor

	2020. BEUC's Response to the European Commission's White Paper on Artificial Intelligence	and Algorithmic-based Decision Making (ADM) which responds to consumers' needs and expectations.'		more broader sense and does not contain specific references to the stages of the electoral process.	
214.	United Nations Development Programme European, Commission, Institute for Democracy and Electoral Assistance. 2007. Joint Training on Effective Electoral Assistance	Training documentation on election and voting methods and assistance of technological tools.[203]	Medium	Slides deck on training material of voter registration tools from low to high tech. No elaboration on the possible threats to democracy.	Preparation ; Voting
215.	United Nations. 1948. Universal Declaration of Human Rights (Preamble)	'The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected.'	Low	Discusses Human Rights	General

[203] Summary prepared by the contractor

216.	Wahlbeobachtung.org. 2020. Social Media Monitoring Early Parliamentary Election- Final Report	Online campaigning on social media platforms has become an integral part of electoral politics in Austria. Two thirds of the Austrian public use Facebook and YouTube, and half of them also use these platforms to inform themselves about political news. It is therefore important to closely monitor the inner workings and dynamics of these new electoral arenas. Wahlbeobachtung.org assembled an international team consisting of election observers, political scientists, data scientists, and social media experts to conduct a social media monitoring project at the occasion of the Austrian early parliamentary elections on 29 September 2019. The goal was to monitor the electoral campaign on the social media platforms Facebook, Twitter, and YouTube.	High	Discusses monitoring of social media and online platforms in electoral campaigns context in Austria.	Preparation
217.	Zuiderveen Borgesius et al. 2018. Online Political Micro-targeting: Promises and Threats for Democracy	'Online political microtargeting involves monitoring people's online behaviour, and using the collected data, sometimes enriched with other data, to show people-targeted political advertisements. Online political microtargeting is widely used in the US; Europe may not be far behind. This paper maps microtargeting's promises and threats to democracy. For example, microtargeting promises to optimise the match between the electorate's concerns and political campaigns, and to boost campaign engagement and political participation. But online microtargeting could also threaten democracy. For instance, a political party could, misleadingly, present itself as a different one-issue party to different individuals. And data collection for microtargeting raises privacy concerns. We sketch possibilities for policymakers if they seek to regulate online political microtargeting. We discuss which measures would be possible, while complying with the right to freedom of expression under the European Convention on Human Rights.'	High	Discusses a new technique used in the elections - online political microtargeting	General

BIBLIOGRAPHY

No.	Author. Year. Title
1.	Dobber, Fathaigh, Zuiderveen Borgesius. 2019. The regulation of online political micro-targeting in Europe
2.	Centre for Public Impact. 2016. The Public Impact Fundamentals Helping governments progress from idea to impact
3.	European Commission. 2018. Securing free and fair European elections A Contribution from the European Commission to the Leaders' meeting
4.	European Regulators Group for Audiovisual Media Services. 2019. Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation
5.	European Parliamentary Research Service. 2019. Regulating disinformation with artificial intelligence
6.	Committee of experts on media pluralism and transparency of media ownership. 2018. Internet and electoral campaigns - Study on the use of internet in electoral campaigns
7.	European Regulators Group for Audiovisual Media Services. 2018. Internal Media Plurality in Audiovisual Media Services in the EU Rules & Practices
8.	High Level Expert Group on Artificial Intelligence. 2019. Policy and Investment Recommendations for Trustworthy AI
9.	European Commission. 2018. Flash Eurobarometer 464. Fake news and disinformation online?
10.	Avaaz. 2019. Far right networks of deception - Avaaz investigation uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections
11.	Facebook. 2019. Facebook Baseline Report on Implementation of the Code of Practice on Disinformation
12.	European Commission. 2018. EU Code of Practice on Disinformation
13.	International Institute for Democracy and Electoral Assistance. 2018. Digital Microtargeting
14.	European Commission. 2018. Tackling online disinformation: a European Approach
15.	European Commission. 2018. Commission guidance on the application of Union data protection law in the electoral context
16.	Alaphilippe et al. 2019. Automated tackling of disinformation Major challenges ahead
17.	High Level Group on Fake News and Online Disinformation. 2018. A multi-dimensional approach to disinformation
18.	European Political Strategy Centre. 2018. A Collection of Think Pieces from 35 leading practitioners and experts
19.	Goldsmith, Ruthrauff. 2013. Case Study Report on Electronic Voting in the Netherlands

20. Russel, Zamfir. 2018. Digital technology in elections - Efficiency versus credibility?

21. Loeber. 2016. E-voting in the Netherlands past, current, future

22. Democracy Reporting International MediaLab ISCTE-IUL. 2019. Disinformation Risks in Portugal's Election - More Brazil Than Europe

23. Relatórios OberCom Outubro. 2019. Fake News em ano eleitoral Portugal em linha com a UE

24. European Political Strategy Centre. 2018. EPSC Newsletter Democracy and Governance in the Digital Age

25. Štětka et al. 2018. Facebook as an Instrument of Election Campaigning and Voters' Engagement: Comparing Czechia and Poland

26. Schaake et al. 2018. Software Vulnerability Disclosure in Europe - Technology, Policies and Legal Challenges

27. Martin, Shapiro. 2019. Trends in Online Foreign Influence Effort

28. Trechsel, Kucherenko, Silva. 2016. Potential and Challenges of E-Voting in the European Union Study

29. Chatham House. 2019. Online Disinformation and Political Discourse - Applying a Human Rights Framework

30. Ferreira, Fantin, Pupillo. 2020. CEPS Task Force Evaluation of the HLEG Trustworthy AI Assessment List (Pilot Version)

31. Appelman et al. 2019. The spreading of disinformation through internet services and the regulation of political advertisements

32. Richter. 2019. Disinformation in the media under Russian law

33. Council of Europe. 2017. Media Regulatory Authorities and hate speech

34. European Parliament, Council of the European Union. 2014. Regulation (EU, EURATOM) No 11412014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations

35. Fletcher et al. 2018. Measuring the reach of fake news and online disinformation in Europe

36. European Commission. 2019. Report on the implementation of the Action Plan Against Disinformation

37. Boucher. 2016. What if blockchain technology revolutionised voting How blockchain technology could be used for e-voting

38. European Parliamentary Research Service. 2019. Artificial intelligence, data protection and elections

39. European Citizens' Rights Involvement and Trust. 2013. Guidelines for European Citizens' Rights, Involvement and Trust

40. International Institute for Democracy and Electoral Assistance. 2018. Online Political Crowdfunding, Political Party Innovation Primer 2

41. International Institute for Democracy and Electoral Assistance. 2018. Collaboration between Citizen Movements and Political Parties

42. International Institute for Democracy and Electoral Assistance. 2019. Open Primary Elections

43. High Level Expert Group on Artificial Intelligence. 2019. A Definition of AI Main Capabilities and Disciplines

44. Ferrara. 2017. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election

45. Papakyriakopoulos et al. 2018. Social media and microtargeting: Political data processing and the consequences for Germany

46. Bulut et al. 2019. Blockchain-Based Electronic Voting System for Elections in Turkey

47. Jefferson et al. 2019. What We Don't Know About the Voatz "Blockchain" Internet Voting System

48. Network and Information Security Cooperation Group. 2018. Compendium on Cyber Security of Election Technology

49. Cherubini, Graves. 2016. The rise of fact-checking sites in Europe

50. European Data Protection Supervisor. 2019. Leading by Example 2015 - 2019

51. European Data Protection Supervisor. 2019. Europe Votes 2019 - how to unmask and fight online manipulation (Opening speech)

52. European Data Protection Supervisor. 2019. Annual Report 2019 - Executive Summary

53. Academic Network on European Citizenship Rights. 2016. Type A Report – Political Participation of Underrepresented Groups in the EU (Executive Summary)

54. EU-CITZEN: Academic Network on European Citizenship Rights. 2018. Type B report - Political Participation of Mobile EU Citizens – Insights from pilot studies on Austria, Belgium, Bulgaria, Germany, Greece, Hungary, Ireland, and Poland (Draft version)

55. EU-CITZEN: Academic Network on European Citizenship Rights. 2018. Annex: Consolidation of Member States fiches (Draft version)

56. Grajewski. 2020. Artificial Intelligence

57. Sgueo. 2020. Digital Democracy Is the Future of Civic Engagement Online

58. Bentzen. 2018. Foreign influence operations in the EU

59. Davies. 2014. Social media and election campaigning

60. Boucher. 2019. Technology and social polarisation

61. Neudert, Marchal. 2019. Polarisation and the use of technology in political campaigns and communication

62. Martens et al. 2018. The digital transformation of news media and the rise of disinformation and fake news: An economic perspective

63. Mair et al. 2019. Understanding our political nature How to put knowledge and reason at the heart of political decision-making

64. Nikoltchev et al. 2016. Mapping of media literacy practices and actions in EU-28

65. Devaux et al. 2019. Study on media literacy and online empowerment issues raised by algorithm-driven media services

66. European Commission. 2019. Communicating ahead of the 2019 European Elections

67. Merkel. 2019. Past, Present and Future of Democracy - Policy Review

68. Bayer et al. 2019. Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States

69. Expert Group on Liability and New Technologies. 2019. Liability for Artificial Intelligence and other emerging digital technologies

70. Theben et al. 2018. Study on the impact of the internet and social media on youth participation and youth work - Executive Summary

71. European Union Agency for Fundamental Rights. 2018. BigData Discrimination in data-supported decision making

72. European Commission. 2019. European Elections 2019 – Political Report

73. CERT-EU. 2019. Election Hacking Bulletin

74. United Nations Educational Scientific and Cultural Organization. 2019. Elections and media in digital times

75. Zalc, Becuwe, Buruian. 2019. The 2019 Post-Electoral Survey Have European Elections Entered a New Dimension

76. European Parliament. 2019. A pro-European - and young - electorate with clear expectations

77. European Commission. 2019. Flash Eurobarometer 478 How do we build a stronger, more united Europe? The views of young people

78. European Commission. 2019. Special Eurobarometer 486 Europeans in 2019

79. European Commission. 2019. Special Eurobarometer 489 Rule of law

80. European Commission. 2018. Standard Eurobarometer 90 Media use in the European Union

81. European Commission for Democracy through law (Venice Commission). 2018. The impact of the information disorder (disinformation) on elections

82. European Commission for Democracy Through Law (Venice Commission). 2018. Code of good practice in electoral matters, Guidelines and explanatory report (Adopted by the Venice Commission AT its 52nd session – 2002)

83. Rapid Response Mechanism Canada. 2019. Open data analysis - European Parliamentary Elections: Comprehensive Report

84. Organization for Security and Co-operation in Europe. 2017. Political advertising and media campaign during the pre-election period: A Comparative Study

85. Ministry of the Interior and Kingdom relations Democracy and Governance. 2019. Aan de Voorzitter van de Tweede Kamer der Staten- Generaal: Policy means for protecting democracy against disinformation

86. Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation. 2019. Progress Report - November 2019

87. European Commission for Democracy Through Law (Venice Commission). 2019. Joint Report on Digital Technologies and Elections (CDL-AD(2019)

88. Dutch Ministry of Interior and Kingdom Relations. 2019. Letter to the House of Representatives on policy means for protecting democracy against disinformation

89. Council of Europe. 2017. Online media and journalism - challenges and accountability (Resolution 2143 (2017)

90. Committee of Ministers of the Council of Europe. 2007. Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns

91. Committee of Ministers of the Council of Europe. 2016. Recommendations and Declarations of the Committee of Ministers of the Council of Europe

in the field of media and information society

92. Electoral Administration Team of the UK Cabinet Office. 2018. Protecting the Debate:

Intimidation, Influence and Information

93. a) Lupiáñez-Villanueva et al. 2018. Study on the Benefits and Drawbacks of Remote Voting + Technical Appendices

b) Faulí et al. 2018. Study on the benefits and drawbacks of remote voting solutions - Presentation of Main findings

94. European Committee of the Regions. 2019. Draft Opinion - Action Plan against Disinformation

95. Finck. 2019. Artificial Intelligence and Online Hate Speech

96. European Commission. 2019. First Annual Self-Assessment Reports on the Code of Practice of Disinformation

97. European Union Agency for Fundamental Rights. 2019. Data Quality and artificial Intelligence – mitigating bias and error to protect fundamental rights

98. European Union Agency for Fundamental Rights. 2019. Facial recognition technology: fundamental rights considerations in the context of law enforcement

99. European Union Agency for Fundamental Rights. 2019. Artificial Intelligence, Big Data and Fundamental Rights (project report not published)

100. European Union Agency for Fundamental Rights. 2020. E-media Toolkit on Migration

101. European Commission. 2019. Recommendation

on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949 final

102. European Commission. 2020. Tackling COVID-19 disinformation - Getting the facts right (JOIN (2020) 8 final)

103. a) European Commission. 2020. Report on the 2019 elections to the European Parliament (COM (2020) 252 final)

b) European Commission. 2020. Report on the 2019 elections to the European Parliament (SWD (2020) 113 final)

104. International Republican Institute. 2019. Democracies under pressure - a global survey

105. Kofi Annan Commission on Elections and Democracy in the Digital Age. 2020. Protecting Electoral Integrity in the Digital Age

106. Lim. 2020. Disinformation as a Global Problem – Regional Perspectives

107. Hegelich, Serrano. 2019. Microtargeting in Germany for the 2019 European Elections

108. Davis, Livingston, Hindman. 2019. Suspicious Election Campaign Activity on Facebook

109. European Regulators Group for Audiovisual Media Services. 2019. Assessment of the Implementation of the EU Code of Practice on Disinformation

110. Yannakoudakis. EESC. 2018. Protection of personal data in the context of EP elections

111. EESC. 2017. Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion)

112. Privacy International. 2020. Challenging Data Exploitation in Political Campaigning

113. Privacy International. 2020. Public opinion about data-driven election campaigning in the UK

114. Geller. Politico. 2020. Some states have embraced online voting. It's a huge risk.

115. Esposito, Tse, Entsminger, Jean. MIT Insights. 2020. AI in the election industry demands transparency

116. European Economic and Social Committee. 2020. The effects of campaigns on participation in political decision-making

117. Madiega. 2020. Reform of the EU liability regime for online intermediaries

118. Joint Research Centre. 2020. Understanding Citizens' Vulnerabilities (II): From Disinformation to Hostile Narratives

119. Joint Research Centre. 2019. Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda

120. European Committee of the Regions. 2019. Artificial Intelligence for Europe

121. European Committee of the Regions. 2019. Digital Europe for All: delivering smart and inclusive solutions on the ground

122. European Committee of the Regions. 2019. Tackling online disinformation: a European Approach

123. European Committee of the Regions. 2019. Action Plan against Disinformation

124. European Parliament. 2019. Activity Report of the Committee on Constitutional Affairs - 8th Parliamentary Term (July 2014 - June 2019)

125. European Parliament and AFCO. 2020. Institutions and foreign interferences

126. European Parliament. 2019. Opinion on the Conference on the Future of Europe 10.12.2019

127. European Commission. 2020. First baseline reports – Fighting COVID-19 disinformation Monitoring Programme

128. European Commission. 2020. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement

129. European Commission. 2020. Disinformation: EU assesses the Code of Practice and publishes platform reports on coronavirus related disinformation

130. European Data Protection Board. 2020. Guidelines 8/2020 on the targeting of social media users

131. Democracy Reporting International. 2019. Guide for civil society on monitoring social media during elections

132. European Commission, Joint Research Centre. 2020. Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis

133. Garnett, James. 2020. Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity

134. Loeber. 2020. Use of Technology in the Election Process: Who Governs?

135. Pal. 2020. Social Media and Democracy: Challenges for Election Law and Administration in Canada

136. Huckle, White. 2017. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains

137. Sathiaraj, Cassidy, Rohli. 2017. Improving Predictive Accuracy in Elections

138. Kruikemeier, Sezgin, Boerman. 2016. Political Microtargeting Relationship between Personalised Advertising on Facebook and Voters' Responses

139. European Commission, Joint Research Centre. 2018. Artificial Intelligence - A European perspective

140. European Commission, Joint Research Centre. 2019. The Future of Government 2030+: A Citizen Centric Perspective on New Government Models

141. European Commission, Joint Research Centre. 2019. The Future of Government 2030+: Policy implications and recommendations

142. European Union. 2012. Consolidated Version of the Treaty on European Union

143. European Parliament, Council of the European Union. 2002. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

144. European Parliament, Council of the European Union. 2000. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

145. European Parliament, Council of the European Union. 2018. Directive (EU) 2018/ 1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio visual media services in view of changing market realities

146. European Commission. 2018. Recommendation on measures to effectively tackle illegal content online (C(2018) 1177 final)

147. European Commission. 2020. White Paper on Artificial Intelligence - A European approach to excellence and trust (COM(2020) 65 final)

148. European Commission. 2019. Building Trust in Human-Centric Artificial Intelligence (COM(2019) 168 final)

149. European Commission. 2018. Artificial Intelligence for Europe (COM(2018) 237 final)

150. European Commission. 2018. Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)

151. European Commission. 2018. Towards a common European data space (COM(2018) 232 final)

152. European Data Protection Supervisor. 2018. Opinion 3/2018 on online manipulation and personal data

153. European Commission. 2016. Code of Conduct on Countering Illegal Hate Speech Online

154. European Union. 2000. The Charter of Fundamental Rights of the European Union (CFR) [2012], OJ C 326/391 (Art. 8, 11, 39, 40 and others) (2000/C 364/01)

155. Terzis et al. 2020. Disinformation and Digital Media as a Challenge for Democracy

156. Broadband Commission for Sustainable Development. 2020. Balancing Act Countering Digital Disinformation While Respecting Freedom of Expression

157. Civitates. 2019. 2019 Annual Report

158. Council of Europe. 2001. Convention on Cybercrime

159. Council of Europe. 2017. 1289th meeting - Democracy and Political Questions

160. DebunkEU. 2020. 70 % of the information about the NATO exercise Defender 2020 was misleading

161. DebunkEU. 2020. Breaches in regulation for political ads on social media pose a risk on electoral transparency-annotated

162. DebunkEU. 2020. COVID-19 related disinformation becomes a tool to promote anti-Baltic narratives

163. DebunkEU. 2020. Disinformers take an advantage of COVID-19 crisis

164. DebunkEU. 2020. Election fraud in Belarus brought a surge of pro- Kremlin propaganda

165. DebunkEU. 2020. Irrelevant and insignificant depiction of the Baltics in pro-Kremlin media

166. DebunkEU. 2020. Latvia had the widest spread of COVID-19 related disinformation in May-annotated

167. DebunkEU. 2020. NATO drills, COVID-19 rules , alleged interference in Belarus used to target the Baltics and Poland

168. DebunkEU. 2020. Negative communication creates an impression of no real political choice in Lithuanian elections

169. DebunkEU. 2020. Negative posts on Facebook sought to discredit democratic processes in Lithuania

170. DebunkEU. 2020. Political unrest in Belarus keeps fuelling disinformation against Baltic states

171. DebunkEU. 2020. Russian media Belarusian opposition is anti-Russian and is selling itself to the West

172. DebunkEU. 2020. Softening criticism towards Lukashenko in pro- Kremlin media - fading power of the Belarusian regime

173. DebunkEU. 2020. US organisation expands its cooperation with Lithuanians in the fight against Chinese disinformation

174. DebunkEU. 2020. With a dramatic surge of COVID-19 cases, Baltic states may be facing the second wave of infodemic

175. Democracy Reporting International. 2020. Lessons Learned Social Media Monitoring during Humanitarian Crises

176. Election Observation and Democratic Support. 2016. Compendium of International Standards for Elections

177. Election-Watch.eu. 2019. Elections to the European Parliament Election Assessment Mission - Final Report

178. Election-Watch.EU. 2020. Rapid Assessment Covid-19 & Elections in Europe

179. EU DisinfoLab. 2020. Covid-19 Disinformation Narratives, Trends, and Strategies in Europe

180. EU DisinfoLab. 2019. The Suavelos galaxy - a showcase of uninhibited racism

181. European Commission. 2020. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan

182. EU DisinfoLab. 2019. Voter suppression campaigns in Spain No contéis conmigo #Yonovoto (Don't count on me #Idon'tvote)

183. EU DisinfoLab. 2020. How two information portals hide their ties to the Russian news agency InfoRos

184. Who Targets Me. 2020. How to take a "gold standard" approach to political transparency and policy

185. European Centre for Electoral Support European Partnership for Democracy. 2016. EURECS A European response to electoral cycle support

186. European Centre for Electoral Support. 2018. Opportunities and Challenges in the Use of Technology in Elections Experience from West and Southern Africa

187. European Centre for Electoral Support. 2020. Delivering Electoral and Democracy Support Under COVID-19 ECES Preparedness and Responses

188. European Citizen Action Service. 2019. Digital Democracy Day 2019 Report on Harnessing the Potential of Technology in Elections

189. European Citizen Action Service. 2019. Online Disinformation Finding the Silver Bullet in the Digital World

190. European Economic and Social Committee. 2019. Societies outside Metropolises the role of civil society organisations in facing populism

191. European Free Aliance. 2016. 2019 Manifesto

192. European Partnership for Democracy. 2020. Universal Advertising Transparency by Default

193. Finnish Ministry of Justice. 2020. National Democracy Program 2025 plan of action

194. Gibson et al. 2016. A review of E-voting the past, present and future

195. Groupe d'Experts Belge sur les fausses Informations et la Désinformation. 2018. Rapport du Groupe d'Experts Belge sur les fausses Informations et la Désinformation

196. Huotarinen et al. 2020. Election Information System life cycle assessment (Finnish Ministry of Justice)

197. International Foundation for Electoral Systems. 2018. Cybersecurity in Elections, Developing a Holistic Exposure and Adaptation Testing

198. Kofi Annan Foundation. 2019. The Internet's Challenge to Democracy Framing the Problem and Assessing Reforms-annotated

199. Kofi Annan Foundation. 2020. The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age

200. Krimmer, Duenas-Cid, Krivonosova. 2020. Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly?

201. Krimmer, Duenas-Cid, Krivonosova. 2020. New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?

202. Krimmer. 2012. The evolution of e-voting why voting technology is used and how it affects democracy

203. Krimmer. 2016. Constitutional Constraints for the Use of Information and Communication Technologies in Elections

204. Krimmer. 2016. Internet Voting in Austria History, development and building blocks for the future

205. Lie Detectors. 2018. European Commission's drive to tackle Fake News and Digital Disinformation needs fast action on education and independent funding guarantees

206. Moravian Land Movement. 2020. Long-term program

207. Organization for Security and Co-operation in Europe. 2010. Election Observation Handbook (Sixth edition)

208. Organization for Security and Co-operation in Europe. 2013. Handbook for the Observation of New Voting Technologies

209. Organization for Security and Co-operation in Europe. 2020. Alternative voting methods and arrangements

210. Organization for Security and Co-operation in Europe. 2020. Human Dimension Commitments and State Responses to the Covid-19 Pandemic

211. Roscoe. 2020. What are we to do about microtargeting

212. The European Consumer Organisation. 2020. BEUC's comments on the EDPB's Guidelines on the Targeting of Social Media users

213. The European Consumer Organisation. 2020. BEUC's Response to the European Commission's White Paper on Artificial Intelligence

214. United Nations Development Programme European, Commission, Institute for Democracy and Electoral Assistance. 2007. Joint Training on Effective Electoral Assistance

215. United Nations. 1948. Universal Declaration of Human Rights (Preamble)

216. Wahlbeobachtung.org. 2020. Social Media Monitoring Early Parliamentary Election- Final Report

217. Zuiderveen Borgesius et al. 2018. Online Political Micro-targeting: Promises and Threats for Democracy