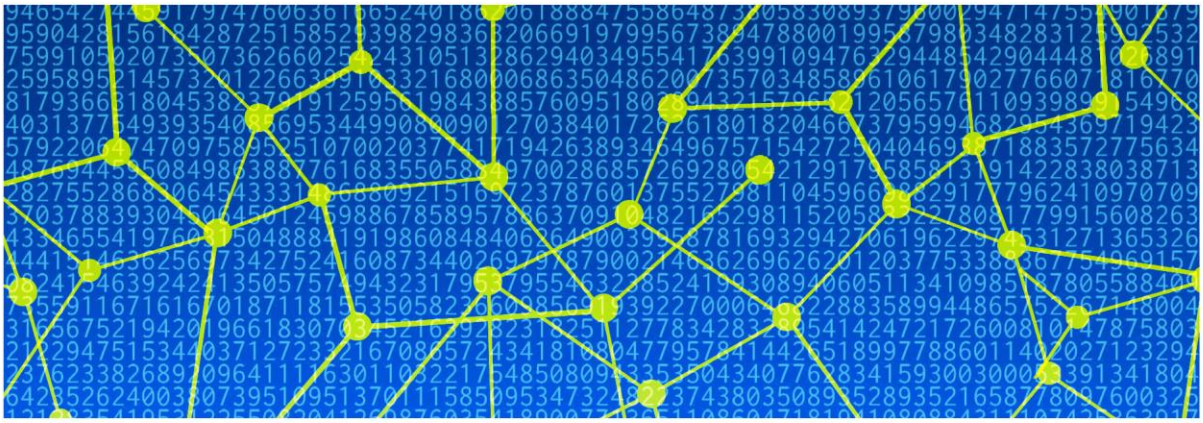

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2018

EDPS Opinion

on online manipulation and personal data

EDPS

19 March 2018

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

Executive Summary

The digitisation of society and the economy is having a mixed impact on civic engagement in decision-making and on the barriers to public involvement in democratic processes.

Big data analytics and artificial intelligence systems have made it possible to gather, combine, analyse and indefinitely store massive volumes of data. Over the past two decades, a dominant business model for most web-based services has emerged which relies on tracking people online and gathering data on their character, health, relationships and thoughts and opinions with a view to generating digital advertising revenue. These digital markets have become concentrated around a few companies that act as effective gatekeepers to the internet and command higher inflation-adjusted market capitalisation values than any companies in recorded history.

This digital ecosystem has connected people across the world with over 50% of the population on the internet, albeit very unevenly in terms of geography, wealth and gender. The initial optimism about the potential of internet tool and social media for civic engagement has given way to concern that people are being manipulated, first through the constant harvesting of often intimate information about them, second through the control over the information they see online according to the category they are put into. Viral outrage for many algorithm-driven services is a key driver of value, with products and applications that are designed to maximise attention and addiction. Connectedness, at least under the current model, has lead to division.

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.

The EDPS has for several years argued for greater collaboration between data protection authorities and other regulators to safeguard the rights and interests of individuals in the digital society, the reason we launched in 2017 the Digital Clearinghouse. Given concerns that political campaigns may be exploiting digital space in order to circumvent existing laws,[1] we believe that it is now time for this collaboration to be extended to electoral and audio-visual regulators.

TABLE OF CONTENTS

1. Why are we publishing this Opinion

i. Intense ongoing public debate

There is currently an intense 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. The major platforms sit at the centre of this ecosystem, gaining disproportionately from the growth in digital advertising, and are increasing their relative power as it evolves. 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. The system rewards sensational and viral content and does not in general distinguish between advertisers, whether commercial or political. Revelations of how deliberate disinformation ('fake news') has been propagated via this system have led to fears that the integrity of democracies may be under threat. Artificial Intelligence systems - the market for which is also characterised by concentration – are themselves powered by data and will - if unchecked - increase the remoteness and unaccountability of the decision-making in this environment.

ii. Relevance of data protection law and political campaigns

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. In their 2005 *Resolution on the Use of Personal Data for Political Communication,* data protection regulators articulated worldwide key data protection concerns related to the increased processing of personal data by non-commercial actors. It referred specifically to the processing of 'sensitive data related to real or supposed moral and political convictions or activities, or to voting activities' and 'invasive profiling of various persons who are currently classified - sometimes inaccurately or on the basis of a superficial contact - as sympathizers, supporters, adherents or party'[2]. The international Resolution called for data protection rules on data minimisation, lawful processing, consent, transparency, data subjects rights, purpose limitation and data security to be more rigorously enforced. It may now be time for this call to be renewed.

EU law on data protection and confidentiality of electronic communications apply to data collection, profiling and microtargeting, and if correctly enforced should help minimise harm from attempts to manipulate individuals and groups. Political parties processing voter data in the EU fall within the scope of the GDPR. The GDPR defines personal data revealing political opinions as special categories of data. Processing such data is generally prohibited unless one of the enumerated exemptions applies. In the context of political campaigning, the following two exemptions are particularly relevant and merit full citation:

> *(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

(e) processing relates to personal data which are manifestly made public by the data subject; [...].

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Recital 56 clarifies para 9(2)(g): '[w]here in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established'.

Several data protection authorities have developed rules or guidelines on data processing for political purposes:

- In March 2014, the Italian Data Protection Authority adopted rules on processing of personal data by political parties. The rules highlighted the general prohibition to use personal data made public on the Internet, such as on social networks or forums, for the purposes of political communication, if this data was collected for other purposes[3].

- In November 2016, the French National Data Protection Commission (CNIL) provided additional guidelines to its 2012 recommendations on political communication, specifying the rules for processing of personal data on social networks. In particular, CNIL underlined that aggregation of personal data of voters in order to profile and target them on social networks can only be lawful if based on the consent as a ground for data processing[4].

- In April 2017, the UK Information Commissioner's Office (ICO) issued updated *Guidance on political campaigning*, which also included guidelines on the use of data analytics in political campaigning. ICO explained that when a political organization commissions a third party company to carry out analytics, then that company is likely to be a data processor, whereas the organization – a controller. Specific provisions of the data protection law governing controller-processor relationship have to be accounted for, in order for the processing to be lawful[5].

The guidelines of the national data protection authorities have a potential of providing additional authoritative interpretation of data protection and privacy law provisions, which account for the differences in the organisation of national political systems[6].

iii. The purpose of this EDPS Opinion

The EDPS vision is to help the EU 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[7]. We have called for the data subject to be treated 'as an individual not simply as a consumer or user' and highlighted ethical issues around the effects of predictive profiling and algorithm-determined personalisation[8]. We have called for responsible and sustainable development of the digital society based on individual control over personal data concerning them, privacy-conscious engineering and accountability and coherent enforcement[9]. The EDPS Ethics Advisory Group in its January 2018 report noted that 'microtargeting of electoral canvassing changes the rules of public speech, reducing the space for debate and interchange of ideas,'

which 'urgently requires a democratic debate on the use and exploitation of data for political campaign and decision-making'[10].

This issue of using information and personal data to manipulate people and politics goes of course well 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[11]. It increases the pervasiveness and persuasiveness of false stories and conspiracies[12]. Research suggests that the manipulation of people's newsfeed or search results could influence their voting behaviour[13].

The EDPS's concern is to help ensure the processing of personal data, in the words of the GDPR, serves mankind, and not vice versa[14]. Technological progress should not be impeded but rather steered according to our values. Respect for fundamental rights, including a right to data protection, is crucial to ensure the fairness of the elections, particularly as we approach the European Parliament elections of 2019[15]. This Opinion is the latest in a series of broad engagements by EDPS on the question of how data protection should be applied to address the most pressing public policy concerns. It builds on the previous EDPS work on Big Data and digital ethics and the need to coordinate regulation of competitive and fair markets[16]. The Opinion will first summarise the process whereby personal data fuels and determines the prevailing cycle of digital tracking, microtargeting and manipulation. It will then consider the roles of the various players in the digital information ecosystem. It will consider the fundamental rights at stake, the relevant data protection principles and other relevant legal obligations. It will conclude by recommending 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.

2. How personal data is used to determine the online experience

'Infonomics' is the term coined in the late 1990s as businesses became interested in the value and monetisability of data[17]. Today visiting a single website results typically in the disclosure of browsing behaviour to over 100 third parties who seek to limit their own legal liability by means of dense 'privacy policies' which can run to hundreds of pages. The decentralised internet of the past has been replaced by walled 'communities' guarded by a few giant tech companies who require those using their services to disclose their identity and personal data. Members of these communities are nudged to remain within the walls and linked third party content can only be accessed inside the frame[18]. Data analytics is used to interpret large datasets to enable businesses and governments more efficiently to understand and influence the behaviour of individuals with regard to their purchases and use of public services. Although techniques are applied for aggregating and anonymising, data analytics relies on the processing of personal data[19].

Online manipulation may be viewed as the culmination of a three-stage cycle from data collection (a form of data processing under EU law) through profiling to microtargeting or personalisation as a form of manipulation which can vary in degree from trivial to seriously harmful[20]. These stages are briefly described below.

i. Data collection

Data collection is a form of data processing under EU law[21]. Personal data are collected from a variety of sources using different dataset merging techniques. Some data is consciously

provided by the individuals, like by filling in an online form. Most data however is observed or recorded automatically, described as 'digital breadcrumbs' deposited unwittingly as a result of individuals' online and offline activities[22]. Such observed data include the times and locations when mobile devices connect with mobile telephone towers or GPS satellites, IP addresses of the terminals, WiFi accesses points, browsing history, 'likes' and 'shares', images collected by digital CCTV systems, purchase history, social media engagement and browsing behaviour across devices[23]. According to a recent study people are much more likely to disseminate, by liking or sharing, information judged 'false' than verified information. Bots and trolls, including those acting on behalf of hostile third states contribute to this further dissemination[24]. A significant category is the data collected from people who take online psychological quizzes which often achieve viral popularity when accessed and shared over social media. A participant's results when combined with personal details available on social media enables intricate personality prediction[25].

Companies use tracking technologies to collect observed data, typically cookies as well as flash cookies, web beacons, device fingerprinting which can track across different devices[26]. Meanwhile the proliferation of connected things and listening devices installed in the home such as smart speakers (the market for which is also already characterised by concentration) presents new possibilities to observe real-time individuals' most private behaviour[27]. When messages and content targeted at an individual based on profiling elicits a reaction from that individual, the reaction is in turn monitored, which creates additional data for collection and use to refine the profile and future targeting.

ii. Profiling

Collected personal data is examined to segment people according to precise profiles. There exists a myriad of traits which can be measured and which can be used to infer user preferences from a user profile, such as age, gender, location and so on[28]. The major social media provider is estimated to have used over 52 000 personal attributes to classify people's interests and attributes. Statistical methods are then used to generate analytical information or to predict future behaviours or development[29]. Automated profiling identifies patterns that are invisible to the human eye[30]. The more user data is available about a person, and the longer a user can be profiled, the richer become the inferences which can be derived from the person's profile[31]. More advanced profiling practices allow scoring or assessing people against benchmarks of predefined patterns of normal behaviour. An example of such applications is a hiring software that analyse an applicant's voice in order to evaluate 'language proficiency, fluency, critical thinking, and active listening'[32]. Another example is how typing patterns on a computer keyboard serve as a ground for predicting person's confidence, nervousness, sadness, and tiredness. A particular feature of such inference is that highly sensitive data like a person's emotional state can be predicted from seemingly non-sensitive information, such as his keystroke dynamics[33].

Big Data combined with behavioural science enables inferences about even deeper personality portraits. Some data analytics companies specialise in assessing individuals based on five personality traits known as the 'Big Five' or OCEAN, using data gathered from online personality tests (see above), a technique reported to have been exploited by campaigners during 2016 US Presidential elections and UK Brexit referendum[34]. These assessments are then supplemented with additional characteristics, including values and needs, likes and shares[35]. Profiling serves also to identify other people who might be potentially interested in a product and service, namely the 'lookalike' audience and customers held by the major social media platforms[36].

The quality of the new knowledge created as an outcome of profiling is subject to debate. Certain studies show that data mining techniques can predict one's personality more accurately than most of their friends and family[37]. Others consider profiling as situational and inherently probabilistic[38]. In any case, the impact of profiling on person's life is not negligible, as the created knowledge is further used to make decisions (automated or not) about a person or a group of people.

iii. Microtargeting and manipulation

Decisions based on profiling personalise an individual's informational environment with a high degree of personalisation, a practices referred to as microtargeting[39]. It may consist in a more personal message to a segment of people sharing certain traits or even potentially determine the prices for products or services. It may consist in how social media platforms determine which content that appears on individual news feeds and in what order.

Companies in the business of selling digital ad space profit from the placing of targeted content irrespective of any ethical considerations: there is no distinction made between a good or bad click from a target demographic[40]. These microtargeting activities may have little effect on some individuals, but the complexity of the technology, low levels of trust and the avowed intentions of several important tech players point towards a culture of manipulation in the online environment[41]. This manipulation may occur as a result of the business strategies chosen by market players themselves, or because of the actions of individuals and states seeking to use platforms intermediaries to disrupt or subvert markets and public discourse.

Moreover, the intention behind the design of devices and software has been to induce addictive behaviour. Features like auto-play, endless newsfeeds, notifications and 'streaks' (unbroken reciprocation of messages or image sharing) are, according to a number of former employees in the tech industry, deliberate attempts to maximise attention through microtargeting towards users, especially children, similar to the techniques used by the gambling industry[42]. Web-based services which have achieved network effects explicitly appeal to people's 'fear of missing out' if they do not regularly check the app[43].

Manipulation also takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual but which is determined in order to maximise revenue for the platform. This is akin to the 'secret menus' used to steer users of ecommerce sites and the 'dark patterns' used to dissuade decisions less desirable from the platform's perspective (such as declining to add additional items, like insurance, to a shopping cart).

The major platforms admitted in 2017 that over 125 million inviduals in the United States had been reached by 'divisive' content – ads and messages from fake accounts. Further reports released just before the publication of this Opinion have alleged a far more widespread degree of intrusion, although the precise effects on actual voting behaviour remain unknown[44]. A more significant and chronic form of manipulation may however be the chilling effect upon freedom of expression which results from the constant surveillance which characterises the digital ecosystem[45].

3. The Digital (mis)information ecosystem

Manipulation and misinformation are as old as humankind but with rapid digitisation they have become matters of pressing social, legal and ethical importance. It had been hoped and expected that new forms of civic engagement would flourish as more people connected to the

internet – through on line campaigns, crowdsourcing and caused-based communities on social media[46]. Currently however the sustainability of microtargeting is subject to heated debates[47].

Manipulation by means of microtargeting presupposes the existence and access to the databases with a variety of data points about individuals, and intellectual property solutions in the form of analytical algorithms that can draw inferences and predictions about people using these data. It is a multi-layered process where two groups of actors interact:

- The advertising ecosystem which relies on the collection and analysis of personal data as the prevailing business model.
- Non-commercial advertisers.

A third big player is emerging in Artificial Intelligence which further blurs the lines of accountability. This complex broad digital ecosystem, composed of businesses and organisations which may have been regulated in the past by different areas of law (consumer law, electoral law, media law, competition law, etc.), makes it more challenging to assign legal responsibility to each of them, to enforce existing rules and to ensure that individuals have recourse to an effective remedy where abuses occur.

i. Platform intermediaries at the centre of digital advertising

A very small number of giant companies have emerged as effective gatekeepers of the digital content which most people consume. They occupy a commanding position among a variety of other actors including advertising businesses, data brokers and data analytics companies. In the 2015 EU citizenship consultation, more than seven out of 10 respondents (72%) said they use internet platforms as a source of information. In Europe, currently more than a third of advertising spend is spent on digital channels surpassing TV advertising (although there are significant differences between regions). In the UK, one of the more advanced digital markets, more than 50% of every advertising pound spent goes to online channels[48].Newspapers (63%) and TV (62%) were the second and third most popular sources of information on EU matters[49]. Most search traffic has migrated to smartphones where the biggest company has 97% market share. Advertisers who use one of the two major platforms, described as a 'duopoly' on grounds that they are reported to account for between 80% and 99% of all revenue growth from digital advertising, cannot control where their advert is placed. Opaque algorithms have placed such ads on sites displaying racist, incendiary or scurrilous content, which has led to a number of large advertisers withdrawing from programmatic ad marketplaces, where software is used to buy and sell advertising[50]. In many countries, one of the two biggest tech companies has become the only gateway to the internet[51]. There is less capital investment in start-ups (down 40% since 2015) indicating that investors see less scope for disruption in the concentrated market[52].

Data analytics could help individuals navigate through the increasingly noisy information environment. However, the reality has been to tip the balance of benefits away from individual, deepening informational asymmetry in favour of owners of proprietary algorithms. By limiting exposure to certain information, for instance in job advertisements, on the basis of person's gender or inferred health status, they may further perpetuate discriminatory attitudes and practices[53]. In effect, the forum for public discourse and the available space for freedom of speech is now bounded by the profit motives of powerful private companies who, due to technical complexity or on the grounds of commercial secrecy, decline to explain how

decisions are made. The few major platforms with their extraordinary reach therefore offer an easy target for people seeking to use the system for malicious ends.

ii. Non-commercial advertisers

Advertisers are not limited to commercial players seeking customer insights[54]. Governments, political and ideological movements, political parties, campaigns, political candidates, and other cause-driven organisations have always sought to spread their message, rally volunteers, recruit donors and otherwise influence public opinion and build communities both online and offline. They have been referred to as 'non-commercial advertisers' as their aim is not to sell or promote a commercial product or service, but rather to communicate their message in order to influence political, social or other views of the individuals and to encourage - or discourage - support for a cause or to vote in an election [5556].

Until recently non-commercial advertisers had access to only limited data about their constituency. Now they have begun to exploit the same targeted internet advertising system used by commercial entities by mining the reactions and discussions on social media in real time and to aggregate data and, extract 'value' from these data, such as inferences about personality traits and likely voting behaviour of the electorate. Many governmental institutions, political and other interest groups have dedicated websites, which to a larger or to a lesser extent use tracking technologies discussed above. They also have an active presence on the social media and make use of targeting (advertising) tools offered by the online businesses[57]. Non-commercial advertisers interact with the social media platforms, such as 'fan pages' or 'groups' on social media which provide integrated advertising and publishing tools. Fan page administrators can obtain viewing statistics, and choose audiences among fan page followers and among all platform users on the basis of demographics, interest, behaviour or other criteria in order to better personalize the platform messages. They can then customise messages to be served back to audiences according to profile and location[58]. How these tools are used varies between countries and types of organisation[59]. In any case there is thus a blurring of the lines between 'commercial' and 'political' data: whereas traditional political research looked at voter registration and party affiliation, data analysts now process any information revealing personality traits.

Political campaigns are increasingly relying on Big Data analytics to influence opinions and voting through targeted messages or online advertising 'impressions'. In many cases the alleged aim is to target people with misleading information[60]. The ability of AI and Big Data to influence significantly democratic processes, certainly outside the United States, is contested. Available empirical evidence from political campaign practices in the Netherlands and Germany show little engagement with microtargeting practices due to practical limitations, which include lack of expertise, funds, particularities of the local jurisdiction, or the legal framework itself[61]. On the other hand the ongoing investigation by the UK Information Commissioner, with a parallel investigation conducted by the Electoral Commission, into alleged data protection abuses in campaigning during the Brexit referendum is scrutinising the activities of 30 organisations including political parties and campaigns, data companies and social media platforms[62]. Regardless of their effectiveness there is a clear interest from non-commercial advertisers to explore the targeting techniques initially developed for the commercial sector[63].

iii. Artificial Intelligence

Throughout this digital ecosystem, automated systems are increasingly mediating communication between individuals, companies and states as well as producing new machine-generated content. Artificial Intelligence is used for fine-grained surveillance, to monitor, filter, and censor messages sent between users of messaging applications[64]. Machine-learning algorithms aim to maximise attention and likes, making media susceptible to manipulation[65]. Social media bots which distort news or foment anger or dissent may be autonomous or controlled by humans[66]. More sophisticated applications of Artificial Intelligence, like deepfakes, speech simulation and automated news reporting, are likely to increase with its potency in this ecosystem as they become cheaper to deploy, unless countermeasures are deployed successfully. The automatic tailoring of messaging already prevalent in the commercial space could, where applied to the political sphere, in theory involve a political candidate's or party's webpage adjusting its content according to the known political preferences of the visitor. It could also creates obstacles for quality research and accountability initiatives aiming to track how political candidates are holding on to their promises once they are at the office lead to involve[67].

Artificial Intelligence is scalable and so these trends are potentially limitless. The relationship between technology and politics is symbiotic, with access to and adeptness at using technology determining the balance of power between states and between regimes and protest movements[68].

4. Fundamental rights and values at stake

Microtargeting and online manipulation appear to compromise substantially a number of rights and freedoms set down in Charter of Fundamental Rights of the EU.

i. Data protection and other freedoms

Privacy and protection of personal data are fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU Article 7 protects a right to respect for private and family life, home and communications, whereas Article 8 established a separate right to the protection of personal data. The indispensability of personal information to the digital information ecosystem puts these two rights under obvious pressure.

Privacy and personal data protection are placed among the 'freedoms' of the EU, which include freedom of thought, conscience and religion, freedom of expression and information, and freedom of assembly and association (Articles 10, 11 and 12). These are also clearly at stake due to the ability of the major platform intermediaries either to facilitate or to impede information dissemination. For instance, content which is not indexed or ranked highly by an Internet search engine is less likely to reach a large audience or to be seen at all. Alternatively, a search algorithm might also be biased towards certain types of content or content providers, thereby risking affecting related values such as media pluralism and diversity. This is particularly the case in the context of allegedly dominant online search engines[69].

ii. Media pluralism

Contained with Article 11 of the Charter is the requirement for the freedom and pluralism of the media to be respected. A Resolution of the European Parliament in December 2017 referred to the 'concentration of power of media conglomerates, platform operators and internet intermediaries risk[ing] negative consequences for the pluralism of public debate and access to information'. The Council of Europe committee of experts is also preparing a recommendation on media pluralism and transparency of media ownership.

There is evidence that this concentration and elimination of local journalism facilitates the spread of disinformation[70]. Social media has been used to encourage people to vote, to vote for a particular candidate, and to discourage from voting altogether ('digital gerrymandering'). The major social media provider itself has encouraged voters to exercise their vote, and there is nothing to preclude them from doing the opposite. In comparison with the mainstream media outlet covering a news story, there is no trace or record of an editorial decision, only the results of filtering performed by an algorithm. Online intermediaries could in theory make it easier for a political party which their business or ideological interests align with to reach their supporters or vice versa, with former social media employees recently claiming to have been involved in keeping conservative issues from trending on the site[71]. Whether allegedly dominant online platforms may (deliberately or not) use their power to influence voting or not is less the point than the fact that they – in principle – have the ability to influence political decision-making processes[72].

EU competition rules permit Member States to intervene under Article 21(4) of the Merger Regulation to protect media plurality. There have been calls for a redefinition of these rules in the light of the disruption caused by platform intermediaries and concentration in the market.

iii. Free elections

In addition, Article 3 of Protocol I to the European Convention of Human Rights guarantees everyone a right to free election. Freedom, fairness and transparency are recognized as key principles of democratic elections[73]. In the EU context Article 39 of the Charter guarantees the right to vote in European Parliament elections. Generally, free elections are those where candidates can compete without any obstacles erected by the authorities, where the electorate has genuine options and a free access to information concerning those options. Fairness of elections can be prejudiced if there is a state interference resulting in inequality of chances for the runners in the electoral race. The principle of electoral transparency is not met if the voters have no freedom to seek, receive and impart information about the process and the candidates, including about the source and spending of financial support received by a candidate or a party[74]. These rights are also therefore challenged by online manipulation.

5. Relevant legal frameworks

The complexity of the digital information ecosystem invokes a range of regulatory sectors which until now have had little reason to interact. This section outlines the relevance of fundamental rights before outlining the relevant sectors of regulation under EU law namely, data protection, the principle of media pluralism, audio-visual.

i. Data protection rules and principles

In the EU data protection rules have been conceived as contributing to the respect of all fundamental rights and freedoms, not only data protection[75]. Specific rules governing the

processing of personal data are laid down in Regulation 2016/679 ('the GDPR') which from 25 May 2018 replaces Directive 95/46/EC[76]. The GDPR requires that any processing of personal data - any information relating to an identified or identifiable natural person - respects data processing principles, including lawfulness, fairness and transparency, purpose limitation, data minimisation and others. Personal data revealing political opinions is considered to be a 'special category of personal data' meriting a higher level of protection. Processing of these data is generally prohibited, unless one or more of the enumerated exceptions appl.[77]. A legal person, including political parties and civil society organisations, or a natural person, such as an independent political candidate, processing personal data in the course of professional activity is bound to follow the GDPR.

The GDPR is particularised and complemented by Directive 2002/58/EC ('ePrivacy Directive'), currently under review. The Directive lays down specific rules to protect the confidentiality and security of electronic communications, including safeguards against intrusions into privacy by unsolicited communications for direct marketing purposes. The notion of 'direct marketing' is not defined in the Directive, though some argue that it would extend to the appeal for funds or support for a political cause, encouraging individuals to vote or not to vote for a political party or a candidate, requesting donations via e-mails, social networks, and other means of electronic communication[78]. Since 2009, the ePrivacy Directive requires any party that stores or accesses information, such as a tracking cookie, on a person's device, to obtain the consent of that person, unless an exception applies[79].

Scope

The GDPR primarily applies to controllers and processors established in the EU[80] and controllers and processors established outside the EU if they offers goods and services to persons in the EU or monitor their behaviour taking place within the EU[81]. Whereas governmental institutions, political or cause-driven movements operating in the EU members states are commonly established on their territory, digital business they employ might be incorporated either on the territory of the EU member states or in the third countries. Some companies would have branches and subsidiaries in the EU, others may not have stable arrangements present in the Union. For instance, there are reports of EU-based campaigns relying on the insights provided by non-EU based data analytics companies, which specialize in profiling of persons to predict their personal preferences and political attitudes[82]. Such activity would be considered as monitoring of behaviour of persons for the purpose of the GDPR. This means that data analytics companies established outside the Union, engaged in profiling of the person in the EU, would be subject to the GDPR and obliged to comply with the rules pertaining to fairness (including an appropriate legal basis for processing), transparency of processing, profiling and other requirements. The GDPR would often also apply to the companies engaged in the profiling of the natural persons residing outside the Union, if they have branches, subsidiaries or other establishments on the territory of the EU. For this purpose, the citizenship or residence of the profiled persons is irrelevant. Hence, GDPR has a potential to extend legal protection like the right to information, access to personal data and to rectification to the persons in non-EU countries[83].

Controllers and accountability

Considering the multiplicity of actors and activities involved in the digital information ecosystem, it can be difficult to identify all controllers and processors and ensure an appropriate allocation of responsibility under the GDPR[84]. Therefore, when a non-commercial advertiser outsources Big Data analytics to other companies, careful consideration should be given to

where control over processing of personal data actually lies – that will have implications for compliance and liability under the GDPR. If Big Data outsourcing is conducted in a controller-processor relationship, where the non-commercial advertiser determines the purposes and means processing, and the data analytics company processes the data exclusively on its behalf, then GDPR requires them to have a contract or another legal act in place regulating their relationship[85]. However, the existence of such a contract would not automatically mean that the company doing the data analysis is really a processor. A company is likely to be a processor, for instance, insofar as it carries out data analytics on behalf of a political party for the purposes of a specific election, while the political party in determining the purpose of processing is likely to be the controller. The greater the freedom that company has to decide what data to collect and how to apply its analytics techniques, the more possible the company will be considered a joint controller[86].

The relationship between the platform and the organisations using its services is a matter of a legal challenge currently pending before the CJEU[87]. In the Advocate General's opinion, both the platform and the creator of a fan page should be considered as controllers[88]. The opinion considers any political party, candidate or ideological movement which has a presence on the social network by virtue of a fan page, and is thus able to influence 'in a specific way which [advertising] tool is put to use' by using filters to define a personalised audience and designate the categories of people whose personal data will be collected by the social media company. Such a company would have all the responsibilities of the controller under the GDPR, including the obligation to identify a legal basis for the processing, to inform individuals about processing of their data, and to demonstrate compliance with the GDPR[89].

Purpose limitation

The purpose limitation principle requires that the purpose of the collection of personal information should be specified at the time of collection. The information may not be further processed in a manner incompatible with those purposes. Whenever there is a change of purpose it must be specified[90].

Data analytics involve methods and usage patterns which neither the entity collecting the data nor the data subject considered or could have even imagined at the time of collection. Algorithmic processing of personal data creates possibilities to generate new data. When a data subject shares a few discrete pieces of data, it is often possible for those data to be merged, generating second and even third generations of data about the person[91].

For example, limited information about supporters of a political party held in its databases, or basic information about members of an organization, provided by them directly, could be merged with data about individuals' purchasing behaviour obtained from data brokers[92]. By using tools provided by the social media platforms, these data can be combined by demographic information (e.g. data about family status) and information on individual behaviour and interests. By applying data analytics methods discussed above, the interested political campaign or membership-based organisation may infer psychological profiles and detailed political preferences about single individuals from seemingly unrelated and non-sensitive sets of data.

The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting

the trust in digital environments and services[93] [94]. Hence the crucial importane of purpose limitation as as principle of data protection law.

Therefore, legitimate processing by non-commercial advertisers as well as the parties to the advertising ecosystem would require in the first place a legal basis for processing such as consent of the individuals concerned. Explicit consent would be essential for processing any sensitive information which reveals political or religious views, and consent will not be valid if it is made a condition for using the service.

They would need to inform the data subjects of the future forms of processing they will engage in and closely monitor their practices to assure they did not exceed the permitted boundaries of processing within those stated purposes[95].

ii. Audio-visual media rules

The EU's Audiovisual Media Services Directive is currently under review. It covers EU-wide coordination of national legislation on all audiovisual media, that is both traditional TV broadcasts and on-demand services. Among the objectives of the review is to tackle 'hate speech' and secure media pluralism. Meanwhile political advertising on TV is usually subject to regulation in the EU and there are impartiality requirements imposed on public broadcasters. However no equivalent regulation exists for the use of algorithmic predictions of preferences and voter behaviour that may have equally if not more powerful an impact[96]. As a result, there have been renewed calls for traditional media responsibility standards to be applied to social media platforms. These platforms act, as a result of their decisions on what news to display to whom, as news editors with responsibility for its trending topics. The question follows, whether social media platforms, through their algorithms that rank and curate third-party submissions, exert a form of editorial control traditionally performed by media professionals and therefore engage specific media responsibilities[97].

For a long time, broadcasters were required to exercise restraint in publication of opinion poll findings and also enforce quiet periods prior to election day ("blackout"). In some cases, the regulation of political advertising extended to rationing of time for parties on public broadcasters in order to level the political playing field to larger and smaller political parties and candidates [98]. However, the move to 'digital narrowcasting' where political campaigns are increasingly taking place online, with the use of analytical and microtargeting tools discussed above, raises questions about the application of broadcasting rules to the major platforms and challenges the audio-visual and media authorities to understand how they operate.

iii. Electoral regulations

In EU Member States national campaign regulations impose requirements for disclosure of donations and/or candidates' spending on political campaigns[99]. Even when such rules apply equally to online and offline (traditional) campaigning, the reliance by the parties on the third-party digital advertising services and social media tools is making application of these rules more difficult. For example, the reported spending on campaign materials may not provide sufficient details about spending on digital advertising and associated services, e.g. targeted ads on social media, analytics services, creation of voter databases, engagement with data brokers. The messages disseminated online, including via social media, rarely include an imprint stating who has published them, thus depriving voters from a possibility to identify who is spending money on trying to influence them at the elections[100]. A lack of transparency

about these practices may have negative implications for fairness and freedom of decision-making process.

iv. Consumer protection

Under the EU Charter of Fundamental Rights, consumers are entitled to a high level of consumer protection. Insofar, two distinct rationales underlie European consumer law: to empower consumers as sovereign market actor, giving them the rights and information necessary to act in that role, and to protect consumers in situations where they are the weaker party in commercial dealings, and not able to take the protection of their rights, (economic) interests and safety into their own hands[101].

The EU has duly adopted various measures for the protection of users of products and services wherever in the internal market they are supplied or consumed[102]. One of these instruments, the Unfair Commercial Practices Directive, prohibits misleading, aggressive and otherwise unfair commercial practices[103][104] [105]. Such practices are outlawed in the context of business-to-consumer commercial practices. Political and ideological targeting and advertising falls outside the scope of the consumer law. However activities which amount to manipulating persons with misinformation, personalising political arguments based on intrusive personal profiles bear obvious similarities to the abuses addressed in consumer law[106]. International human rights law tends to distinguish between recipients of political and commercial targeting[107]. Nevertheless, as indicated in the above mentioned Resolution on the Use of Personal Data for Political Communication, 'although political communication sometimes shares many of the characteristics of promotional activity, it has some characteristics that are distinct from commercial marketing'[108].

v. Competition law

In our 2014 Preliminary Opinion on Privacy and competitiveness in the age of big data, and later, in our 2016 Opinion on coherent enforcement of fundamental rights in the age of big data, we argued that competition law had a crucial role in ensuring the accountability of dominant players in the market and protecting democracy against excessive market power. There is evidence that concentration has provided an easy target for malicious operators within the 'ecosystem' that sustains microtargeting. The interests of individuals should be better reflected in assessing the potential abuse of dominance or the mergers of companies, which may have accumulated significant informational power[109]. For example, in December 2017, the German competition authority issued a preliminary legal assessment in the abuse of dominance proceeding against Facebook. It held that Facebook was abusing this dominant position by making the use of its social network conditional on its being allowed to limitlessly amass every kind of data generated by using third-party websites and merge it with the user's Facebook account[110]. As microtargeting can be reliant on the personal data collected by this social media network, the findings of the Bundeskartellamt are also relevant in the context of this Opinion.

Grounds for intervention under the data protection, consumer protection and competitions laws to address potential negative implications of microtargeting for individuals' fundamental rights were discussed by the respective regulators at the second meeting of the Digital Clearinghouse[111]. It was decided to further consider it as an area of possible collaboration between the regulators, also including electoral and media authorities. The EDPS will coordinate this effort further, also taking into account the ongoing work of the European Commission,[112] and the national regulatory authorities[113].

6. Recommendations

Online manipulation is a complex problem and there is any simple solution. No single arm of regulation is able to tackle it alone. This Opinion has argued however that data protection must be a big part of the solution. We make below five recommendations for action drawn from data protection law and where independent data protection authorities can bring a valuable contribution, beginning with completing the reform of data protection framework and enforcing it rigorously, regulators attempting to reach a collecting understanding of the issue, building on existing measures at national and EU level for cooperation with other regulators, self-regulation and greater individual empowerment.

I. Complete and enforce data protection rules

It is crucial to reinforce protection of special categories of data, the principles of transparency, purpose limitation and data minimization, and safeguards against unlawful profiling and automated decision-making.

The EU privacy and data protection framework would be incomplete without a legal tool to protect the right to private life guaranteed by Article 7 of the Charter of Fundamental Rights. The proposed ePrivacy Regulation has a potential to de-incentivise constant tracking and manipulating of individuals.

For this purpose, we have already advised to the legislator to include the following additions to the proposed Regulation[114]:

- a complete and explicit ban on so-called 'tracking walls';
- an explicit prohibition on the practice of excluding users who have ad-blocking or other applications and add-ons installed to protect their information and terminal equipment;
- a confirmation that processing of data for purposes of providing targeted advertisements cannot be considered as necessary for the performance of a service; and
- a requirement for browsers and other software of operating systems to offer by default controls that make it easy to express or withhold consent to tracking.

The EDPS will continue to support with the European Parliament and the Council with a view to ensure a speedy finalisation of the new legislation and create incentives for a sustainable baseline for respecting privacy and data protection[115]. We believe that in doing so, the EU will open opportunities for new business models and for more privacy friendly technologies and businesses, which would help to circumvent the risks posed by the underlying ecosystem for microtargeting.

II. Regulators should aim for a collective diagnosis of the problem

Data analytics offers unprecedented possibilities to profile individuals in order to score, rank, assess their behaviour and make informed decisions about them. It personalises people's experiences and information exposure in order to influence their behaviour and choices, whether in terms of their purchasing decisions as consumers or as citizens engaged in civic life[116]. The challenge is to harness technology in ways that help people engage more freely and effectively in civic decision-making. It is to manage the risks of undue manipulation and contest the idea of an individual as a quantified self[117] .

Data protection authorities and all concerned regulators need to understand the local practices of microtargeting, including to what extent political and ideological movements engage in profiling and targeting of individuals, what sources of personal data they rely on and what tools they employ to profile and target them. Although some global and regional trends can be identified, the variation in the institutional frameworks, social and legal conditions render it necessary for the authorities to conduct country-specific inquiries[118]. Much effort has already taken place at national level, and the Commission is leading work to identify solutions[119]. Regulators can consider existing guidelines from data protection authorities on political campaigning and the scope to extend them to other social and ideological movements involved in profiling and targeting of individuals with non-commercial messages. In particular, the notion of public interest under data protection law and how it is distinct from the private interests of companies or political movements is key to addressing abuses and manipulation occurring in the online political space.Regulators should work together to build on this.

III. Regulators should cooperate across sectors

Current responses to 'fake news' need to be supported through more interagency cooperation[120].

Firstly, antitrust and privacy are converging as authorities realise that much structural abuse is the result of distortions in an overconcentrated digital market. Antitrust has a crucial role to play in policing the behaviour of dominant companies and using merger control to avoid harmful longer term effects of mergers.

Secondly, cooperation between data protection and consumer protection regulators could potentially investigate the underlying ecosystem which facilitates political microtargeting, i.e. online services provided by advertising industry, data brokers, data analytics companies and social media platforms[121]. Under consumer protection law, they can qualify both as 'traders' in their own right,[122] and as profiling and targeting service providers to third parties. It is thus possible, for data protection and consumer protection authorities to consider standards for transparency and intelligibility of contractual terms and online services in particular requiring companies to be more transparent about their decision making in data processing operations[123].

The synergies could also address potential persuasiveness of behavioural targeting by looking into 'fairness' of certain features of these online services[124] which primarily aim at persuading customers to provide more personal information in order to obtain more granular profiling data, and offer more nuanced targeting capabilities thus increasing the value of the service to advertisers (both commercial and political).

Thirdly, cooperation with electoral regulations has become essential. There are exemptions in data protection and ePrivacy rules covering political activity and the public interest, and regulators need to work together to ensure that manipulation is not allowed to escape regulation. As indicated in the Resolution on the Use of Personal Data for Political Communication, "existing data protection and privacy commissioners could play an increasing role in planning coordinated actions also in cooperation with other supervisory authorities competent in the fields of telecommunications, information sector, opinion polls and electoral activities"[125]. Indeed, data protection law, electoral law and audio-visual law share common principles, such as transparency and fairness, and cooperation between the respective regulators, especially during the electoral period, could enhance their coherent application and strengthen the protection of individuals against potentially unfair microtargeting practices.

An EU research project carried out in 2013, noted a lack of coordination between the data protection regulators on the question of data processing for political campaigning purposes[126]. Apart from one notable exception[127] on the application of data protection and audio-visual law during political campaigning, there also seem to be no active cross-regulatory cooperation between data protection, electoral and media authorities on the national or EU level. However, in the context of political campaigns, regulators in all three areas of law – data protection, electoral and media – seem to face challenges in applying shared principles of 'transparency' and 'fairness' to the new realities of political campaigning, which involves tracking, profiling and targeting individuals online. Reports submitted by political parties detailing their campaign spending and investigations by electoral authorities, may provide valuable information to the data protection authorities about data collection and processing practices which political campaigns engage into (with or without assistance of the third parties). This may further feed into the assessment of their compliance with the GDPR requirements, including accountability, lawfulness, transparency and fairness of data processing. Data protection authorities have an intimate knowledge about the functioning of the digital advertising ecosystem, which they could share with the audio-visual authorities in order to assist them with the application of political advertising rules to the online environment. These are just a few examples of the potential benefits that a more active cooperation between the regulators could bring.

As we have argued in our previous Opinion, regulatory authorities in each area of law have limited competences and thus limited tools at their disposal. For example, data protection authorities can only address lawfulness, transparency and fairness of profiling and targeting as far as processing of personal data is concerned[128], the fairness and truthfulness of the personalised messages is not for the data protection law to regulate. Consequently, and given the potential risks of microtargeting extending beyond the scope of the right to data protection, into the domains of freedom of speech and information, equality and free elections, there is a need to explore the prospects of cooperation between data protection and other regulators.

IV. Self-regulation and codes of conduct should be encouraged

Online manipulation is too systemic, too existential in its threat to fundamental rights and values, to leave it to industry to solve. However self regulation has an important role to play.

Under the GDPR, national supervisory authorities, the European Data Protection Board, the EU Member States, and the Commission are required to encourage the drawing up of codes of conduct 'intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises' [129]: As indicated by the Working Party 29, adherence to a code of conduct may go towards demonstrating transparency. Codes 'may be drawn up for the purpose of specifying the application of the GDPR with regard to fair and transparent processing, information provided to the public and to data subjects, and the protection of, children, amongst other issues'[130]. In addition, drawing up a code of conduct may inspire political parties, campaigns, and other social and political-cause driven association to discuss on the ethical dimension of data processing, such as decisions by particular controllers not to engage in certain data processing operations[131].

V. Empower individuals to exercise their rights including collective action

Encryption, apps and browser extensions which aim to uncover targeting, along with other security measures for the protection of personal information are a barrier to manipulation.

Data brokers, advertising networks, social network providers and other digital business actors have ever more complete files on individuals participating in today's digital society, and individuals are losing control over the digital footprints they leave behind. Targeted, profiled and assessed by actors often beyond their control or even knowledge, individuals may feel helpless and need to be empowered to take control of their identity. Even where formally having been given some form of a 'notice' and opportunity to 'consent' to general terms and conditions, individuals often find themselves inside a system designed to maximise the monetisation of personal data, which leaves no real choice or control to individuals[132].

Transparency is only part of the solution - the reasoning behing the bipartisan Honest Ads Act, which would merely require buyers of online political advertisements to reveal their identities.

Different surveys report that around 75% of consumers have no confidence in how social media brands and marketing companies' handle their data.[133] Less than 2 out of 10 Europeans feel that they have complete control over the information they provide online, while every third believes that he has no control over it at all[134].

We have already called on the digital businesses that invest a lot of effort into finding innovative ways to make use of personal data, to use the same innovative mind-set when implementing data protection principles[135]. Our 2016 *Opinion on Personal Information Management Systems* explored the concept of technologies and ecosystems aiming at empowering individuals to control the sharing of their personal data ('personal information management systems' or 'PIMS' for short). We have analysed the potential of PIMS to put users in control of their personal information, and suggested to the Commission and the Member States to take the steps in order to foster research and development and deployment to market in the area of PIMS.

To make fundamental rights 'practical and effective[136], any *ex ante* legal, policy and technological safeguards put in place by the controllers and processors, have to be accompanied with the *ex post* right to effective remedy for those, whose rights and freedoms were violated[137] As microtargeting by and large relies on the automated decision-making processes it lends itself to particular challenges for persons' ability to obtain effective remedy. These include the opaqueness of the decision itself, its basis, whether the individuals have consented to the use of their data in making this decision, or are even aware of the decision affecting them[138]. The individuals may face challenges accessing their personal data because of procedural obstacles[139], or, due to the information asymmetry between controllers and processors, assessing the comprehensiveness of the information they receive in response to the access requests. The difficulty in assigning responsibility for the decision also complicates individuals' understanding of whom to turn to address the complaint[140]. In addition, there is a number of obstacles for individuals' seeking judicial redress in general[141].

In light of these and other obstacles to the effective exercise of the rights under the GDPR, the Regulation, in comparison with the Data Protection Directive, envisions additional ways to exercise this right. In particular, Article 80 of the GDPR provides for the right for the data subject to 'mandate a not-for-profit body, organisation or association', under certain conditions, to exercise certain rights on the data subject's behalf, as well as for the possibility for Member States to provide that these organisations may perform similar functions independently of a data subject's mandate, at their own initiative. Although the introduction of this right should be acknowledged as a great achievement[142], to give a full effect to the right to an effective remedy, the EDPS recommends the following:

- For the EU legislature: to introduce an explicit provision for collective redress and effective remedies or otherwise clarify the text of the ePrivacy regulation (e.g. by explicitly confirming the applicability of Article 80 of the GDPR) ensuring full availability of the collective redress mechanisms, as they are available under the GDPR[143].

- For the Member States when exercising their discretion with respect to the implementation of Article 80(2) of the GDPR: to provide in their national legislation a legal standing for the not-for-profit public interest bodies, organisations or associations active in the field of the protection of data subjects' rights and freedoms, to lodge complaints to the supervisory authority and exercise other data subjects rights stipulated in this Article, independently of a data subject's mandate.

EDPS believes that such approach would contribute to a more coherent and equal enforcement of data subject rights in practice across different EU jurisdictions. This is especially important in the context of sensitive data processing practices such as profiling and automated decision-making of individuals, which, when unlawful, non-transparent, or unfair, may adversely affect the exercise of civil rights of millions. For instance, a data breach of voter database resulting in exposure of voter's profiles with insights about their personality, lifestyle, and psychological profiles, may be regarded as a particularly grave infringement of the right to the respect to private life. The availability of opt out collective redress mechanism[144] may allow public interest organizations to address this infringement, even if individuals, due to the reasons described above, may not be in position to pursue legal action against the data controller and/or processor[145].

7. Conclusion

Online manipulation poses a threat to society because filter bubbles and walled communities make it harder for people to understand each other and share experiences. The weakening of this 'social glue' may undermine democracy as well as several other fundamental rights and freedoms. Online manipulation is also a symptom of the opacity and lack of accountability in the digital ecosystem. The problem is real and urgent, and is likely to get worse as more people and things connect to the internet and the role of Artificial Intelligence systems increases. At the root of the problem is partly the irresponsible, illegal or unethical use of personal information. Transparency is necessary but not enough. Content management may be necessary but cannot be allowed to compromise fundamental rights. Part of the solution, therefore, is to enforce existing rules especially the GDPR with rigour and in tandem with other norms for elections and media pluralism.

As a contribution to advancing the debate, in spring 2019, EDPS will convene a workshop where national regulators in the area of data protection, electoral and audio-visual law will be able to explore these interplays further, discuss the challenges they are facing and consider opportunities for joint actions, also taking into consideration the upcoming European Parliament elections.

This Opinion has argued that technology and behaviour in the market is causing harm because of structural imbalances and distortions. We have called for adjusting the incentives to innovate. The tech giants and pioneers have benefited until now from operating in a relatively unregulated environment. Traditional industries and basic concepts of territorial jurisdiction, sovereignty and also social norms including democracy are affected. These values depend on a plurality of voices, and equilibrium between parties. No single player or sector can tackle this

alone. Protection of data is part of the solution and perhaps a bigger part than expected. It is not enough to rely on the good will of ultimately unaccountable commercial players. We need now to intervene in the interests of spreading more fairly the benefits of digitisation.

Brussels, 19 March 2018

Giovanni BUTTARELLI

European Data Protection Supervisor

NOTES

[1] See, for instance, http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html [accessed 18.3.2018].
[2] Resolution available here https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf [accessed 18.3.2018].
[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267"Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" published in the Official Gazette of the Italian Data Protection Authority number 71 on 26.03.2014 [doc. web n. 3013267].
[4] https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" published by the Commission Nationale de l'informatique et des libertés (French National Commission of Informatics and Liberty) 08.11.2016.
[5] https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].
[6] According to Article 57(1)(d) of the GDPR, each supervisory authority shall on its territory [...] promote the awareness of controllers and processors of their obligations under this Regulation.
[7] See Leading by Example: The EDPS Strategy 2015-2019 , p.17. 'Big data,' in our view, 'refers to the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions. One of the greatest values of big data for businesses and governments is derived from the monitoring of human behaviour, collectively and individually, and resides in its predictive potential; EDPS Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology, 11.9.2015, p. 6.
[8] Profiles used to predict people's behaviour risk stigmatisation, reinforcing existing stereotypes, social and cultural segregation and exclusion, with such 'collective intelligence' subverting individual choice and equal opportunities. Such 'filter bubbles' or 'personal echo-chambers' could end up stifling the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish; EDPS Opinion 4/2015, p. 13 (references omitted).
[9] EDPS Opinion 7/2015 Meeting the challenges of big data, p.9.
[10] Report of the EDPS Ethics Advisory Group, January 2018, p.28.
[11] See for example The Economist, How the World Was Trolled (November 4-10, 2017), Vol. 425, No 9065, pp. 21-24.
[12] Allcott H. and Gentzkow M., Social Media and Fake News in the 2016 Election (Spring 2017). Stanford University, Journal of Economic Perspectives, Vol. 31, No. 2, pp. 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf, p. 219.
[13] In one of the experiments, social platform users were told how their friends had said they had voted, which prompted statistically significant increase of segment of the population (0.14% of the voting age population or about 340 000 voters) to vote in the congressional mid-term elections in 2010; Allcott H. and Gentzkow M., Social Media and Fake News in the 2016 Election (Spring 2017), Stanford University, Journal of Economic Perspectives, Vol. 31, No. 2, pp. 211-236., p.219) In another study, the researchers claimed that differences in Google search results were capable of shifting voting preferences of undecided voters by 20%; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles?. Internet Policy Review, 5(1). DOI: 10.14763/2016.1.401, p. 9.
[14] Recital 4 to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter 'GDPR'.
[15] As stated by the European Court of Human Rights in the case of Orlovskaya Iskra v. Russia, Free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system. The two rights are inter-related and operate to reinforce each other: for example, freedom of expression is one of the "conditions" necessary to "ensure the free expression of the opinion of the people in the choice of the legislature". For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely. In the context of election debates, the unhindered exercise of freedom of speech by candidates has particular significance" (references omitted from the text), para. 110. http://hudoc.echr.coe.int/eng?i=001-171525.
[16] 2014 - Preliminary Opinion on 'Privacy and Competitiveness in the Age of Big Data'; 2015 - Opinion 4/2015 Towards a new digital ethics. Data, dignity and technology; 2015 - Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability; 2016 - Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data.

[17] http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf, U.S House of Representatives Committee on Energy and Commerce hearing entitled 'Algorithms: How Companies' Decisions About Data and Content Impact Consumers' 27.11.2017 p. 2.

[18] https://www.wsj.com/articles/its-time-to-bust-the-online-trusts-1509487518 (CF NYC article, Yelp article WSJ) The Wall Street Journal 'It's Time to Bust the Online Trusts' 31.10.2017.

[19] Some of the data created does not relate to individuals. It is data derived from activities like the analysis of weather patterns, space exploration, scientific testing of materials or designs or the risks associated with securities trading in financial markets. But a large proportion is the data we create ourselves or that is created about us (The Information Accountability Foundation, Origins of Personal Data and its Implications for Governance" see http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf).

[20] Based on the framework offered by https://biblio.ugent.be/publication/8541057. For more information also see: https://www.maastrichtuniversity.nl/sites/default/files/mcel_master_working_paper_20172_mondschein_2.pdf .

[21] Article 4(2) GDPR.

[22] Schwartz, E., Finding our way with digital bread crumbs, MIT Technology Review, 18 August 2010; Article 29 Working Party Guidelines on the right to data portability, WP 242.

[23] Report of the Special Rapporteur on the right to privacy, 19.10.2017, paras. 31-32; WP29 opinion on behavioural advertising, pp. 7, 10-11.

[24] Facebook revealed recently that during the 2016 presidential election more than 62,000 users committed to attend 129 events organized by Russian trolls, such as rallies for adverse groups Heart of Texas and United Muslims of America that drew their separate audiences to the same place at the same time; source. 'When a false report about potential ballot tampering in Sicily started to spread online on voting day, Twitter users retweeted the misinformation roughly 1,000 times, according to an analysis by EU DisinfoLab. Yet on Facebook, the same story was shared more than 18,000 times — and that's only on public Facebook pages. How that misinformation spread within Facebook users' private pages (and, notably, who helped to circulate it) remains unknown;' **source.**

[25] The Atlantic- The Dark Side of That Personality Quiz You Just Took, 13.7.2017. https://www.theatlantic.com/technology/archive/2017/07/the-internet-is-one-big-personality-test/531861/.

[26] WP29 opinion on device fingerprinting. For the overview of different tracking technologies see Mondschein, C., The Regulation of Targeted Behavioural Advertising in the European Union, MCEL Master Working Paper 2017/2. In 2017, a method was published allowing to track a person across multiple browsers on the same device; Browser Fingerprinting Tech Works Across Different Browsers for the First Time, 24.2.2017, https://spectrum.ieee.org/tech-talk/telecom/internet/new-online-fingerprinting-technique-works-across-browsers [accessed 18.3.2018].

[27] Helberger, N, Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law, 6.2. 2016, p. 3.

[28] Monschein, p.9.

[29] Vermeulen, G., Lievens, E., eds., Data protection and privacy under pressure : transatlantic tensions, EU surveillance, and big data, 2017, p. 316.

[30] Kaltheuner, F. and Bietti, E., Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR, IRP&P, p.3. 3.

[31] Mondschein, p.11.

[32] Kaltheuner, F. and Bietti p. 5.

[33] Kaltheuner, F. and Bietti p. 4.

[34] OCEAN, an acronym for openness, conscientiousness, extroversion, agreeableness, neuroticism. See for example, Grassegger, H. and Krogerus, M. The Data That Turned the World Upside Down, Stanford Public Policy Program, 28.1.2017; Polonski, P., How artificial intelligence conquered democracy, 8.8.2017, http://theconversation.com/how-artificial-intelligence-conquered-democracy-77675 [accessed 18.3.2018].

[35] e.g. . IBM Watson 'Leveraging cognitive computing and social media data to generate deep constituent insights' https://www01.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/Jalal%20Mahmud%27s%20Presentation/$file/Jalal%20Mahmud%27s%20Presentation.pdf.

[36] See report of U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Communication and Technology and the Subcommittee on Digital Commerce and Consumer Protection, 27.11.2017, hearing entitled 'Algorithms: How Companies' Decisions About Data and Content Impact Consumers'. At least one data protection authority has cast doubt on the legality of using 'Custom Audiences' from customer lists to create 'lookalike audiences' without the consent of the individuals concerned; Press release from Bavarian data protection authority (Bayerisches Landesamt für Datenschutzaufsicht), Facebook Custom Audience bei bayerischen Unternehmen, 4.10.2017.

[37] The effectiveness of these predictions were assessed in one of the experiments performed by the Stanford researchers. They have found that "by mining a person's Facebook "likes," a computer was able to predict a person's personality more accurately than most of their friends and family. Only a person's spouse came close to matching the computer's results." The computer predictions were based on which articles, videos, artists and other

items the person had liked on Facebook. https://news.stanford.edu/2015/01/12/personality-computer-knows-011215/.

[38] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, Journal of Information Rights, Policy, and Practice 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' p. 9 Vol 2, No 2 (2017).

[39] Microtargeting is a term of recent currency used increasingly to refer to anytime a sampling process is based on detailed segmentation of the target audience, mostly in online commercials to create personalised messages or offers and correctly estimate their impact. In the political context, the term was firstly used during American election campaign lobbying; Barbu, O., Microtargeting in social media: definitions and ethical issues, Studia Universitatis Babes- Bolyai Ephemerides. 58, 2013, pp. 83-90. To differentiate from commercial microtargeting, term 'political microtargeting' has been defined as the use of different communications (mail, phone, canvassing, direct mail, and social media advertising, etc.) to communicate and build a relationship with prospective voters'; Bodó, B. & Helberger, N. & de Vreese, C. (2017), Political microtargeting: a Manchurian candidate or just a dark horse?. Internet Policy Review, 6(4). DOI: 10.14763/2017.4.776. See also Colin J. Bennett; Voter databases, microtargeting, and data protection law: can political parties campaign in Europe as they do in North America?, International Data Privacy Law, Volume 6, Issue 4, 1 November 2016, Pages 261–275.

[40] Damian Tambini cited in Pennycook and Rand, The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings, 2017.

[41] One successful tech entrepreneur and lecturer stated in an article in 2012 entitled 'The art of manipulation': 'We build products meant to persuade people to do what we want them to do. We call these people "users" and even if we don't say it aloud, we secretly wish every one of them would become fiendishly addicted'; https://techcrunch.com/2012/07/01/the-art-of-manipulation/ [accessed 18.3.2017].

[42] See for example, Tim Wu, The Attention Merchants, 2017; Roger McNamee, Why not regulate social media like tobacco or alcohol?, https://www.theguardian.com/media/2018/jan/29/social-media-tobacco-facebook-google [accessed 18.3.2017]; https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/ [accessed 18.3.2017].

[43] See for instance https://www.psychologytoday.com/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo [accessed 18.3.2017].

[44] Stories were published on 17.3.2018 alleging improper access to and use of data from 50 million Facebook profiles; New York Times, How Trump Consultants Exploited the Facebook Data of Millions; Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.

[45] See for instance report by National Telecommunications and Information Administration of the United States Department of Commerce, 'Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities', 13.5.2016.

[46] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 European Commission 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' [SWD82016) 172 final] 25.5.2016.

[47] Examples of engagement include organizing or participating in online social campaigns or petitions, building cause-based communities on social media, involving citizens in online the allocation of local budgets, drafting and review of legislation, crowdsourcing policy ideas. For more examples see: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE253/RAND_PE253.pdf, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF373/RAND_CF373.pdf.

[48] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9 March 2017), https://rm.coe.int/16806fd666, p. 8.

[49] http://ec.europa.eu/justice/citizen/document/files/2015_public_consultation_booklet_en.pdf, p. 11.

[50] See for example, Digiday UK Interview with Guardian Media CEO 19.12.2017; FT, Advertisers' challenge to Facebook and Google https://www.ft.com/content/d43fd706-0fec-11e8-8cb6-b9ccc4c4dbbb 12.02.2018.

[51] A critical study on this initiative is Global Voices AdVox, Global Free Basics in Real Life: Six case studies on Facebook's internet "On Ramp" initiative from Africa, Asia and Latin America, 27.7.2017.

[52] CNBC, Seed funding slows in Silicon Valley, 1.8.2017; https://www.cnbc.com/2017/08/01/seed-funding-slows-in-silicon-valley.html [accesed 18.3.2018].

.[53] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, p. 9. There are scholars who are less optimistic about the potential of personalized communication. They suggest that targeted online advertising has failed to achieve a click-through rate on ads higher than 0,5 perc, and thus, it seems that "the technology is still insufficient" to substantially influences a person's behaviour. https://policyreview.info/articles/analysis/should-we-worry-about-filter-bubbles, p. 10.

[54] The insights obtained from Big Data analytics can be used for a variety of purposes, including making hiring decisions, credit scoring, evaluation of asylum claims, identifying and suspending fake social media accounts. For the overview see *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, pp. 4-6.

[55] https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00035/544506-00035.pdf, The Progress & Freedom Foundation 'Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech' p. 18 07.12.2009.

[56] Ibid., also see https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, p. 3 and 5. See also ideas for practical application of data analytics and AI in the public domain: https://medium.com/@drpolonski/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first-7b1257cb4285.

[57] See e.g. p. 29, http://webbut.unitbv.ro/Bulletin/Series%20V/BULETIN%20I/03_Biea.pdf; p. 12, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.

[58] https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f Medium, 'Cambridge Analytica: the Geotargeting and Emotional Data Mining Scripts' 13.10.2017.

[59] https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting Internet Policy Review 'Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques.' 31.12.2017.

[60] P 3, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

[61] https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, Computational Propaganda Research Project, Working Paper No. 2017.11, Computational Propaganda Worldwide: Executive Summary p. 8. Samuel C Woodley and Philip N. Howard, University of Oxford.

[62] https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/ Information Commissioner's Office, 'The Information Commissioner opens a formal investigation into the use of data analytics for political purposes' 17.05.2017, and 'Update on ICO investigation into data analytics for political purposes', 13.12.2017, Elizabeth Denham, Information Commissioner.

[63] Researchers in the field of voter microtargeting assume that data-driven campaigning and microtargeting techniques associated with it will increasingly penetrate European political landscape. See e.g. https://academic.oup.com/idpl/article-abstract/6/4/261/2567747?redirectedFrom=fulltext, p. 262.

[64] Jason Ng, 2015 https://citizenlab.ca/2015/07/tracking-censorship-on-wechat-public-accounts-platform/

[65] Marwick and Lewis 2017.

[66] Brundage, M., The Malicious Use of Artificial Intelligence:Forecasting, Prevention,and Mitigation; p:45.

[67] See O'Neil, C, Weapons of Math Destruction, 2016, p. 195.

[68] Brundage, p.44.

[69] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, p. 36.

[70] See for example, Moore; M:; Tech Giants and civic power; Centre for the Study of Media, Communication and Power, April 2016.

[71] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9 March 2017), https://rm.coe.int/16806fd666, p. 13.

[72] Ibid.

[73] http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2010)037-e European Commission for Democracy through Law (Venice Commission), 'Report on the timeline and inventory of political criteria for assessing an election' p.4, Study no. 558/2009, Strasbourg, 21.10.2010.

[74]http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf London School of Economic, Media Policy Brief 19 'The New Political Campaigning' p.6. March 2017.

[75] Recital 2, GDPR.

[76] The analysis presented in this Opinion is based on the GDPR.

[77] Article 9 of the GDPR.

[78] The Commission's Proposal for an ePrivacy Regulation states that 'messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties' as well as 'messages sent by other non-profit organisations to support the purposes of the organisation' fall within the scope of 'direct marketing': recital 32, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017 COM(2017) 10 final. The UK Information Commissioner's Office Guidance on Political Campaigning extends the definition of direct marketing to the activities of political campaigning.

[79] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF. Official Journal of the European Union L337/11 Directive 2009/136/EC of 25 November 2009. Fore more information about difference in implication of this provision, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[80] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, Recital 22, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. 2017/0003 (COD).

[81] Article 3(2).

[82] See e.g. http://www.telegraph.co.uk/news/2017/02/24/exclusive-tiny-canadian-company-helped-swing-brexit-vote-leave/; https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns.

[83] For the example of such application see https://medium.com/personaldata-io/quick-guide-to-asking-cambridge-analytica-for-your-data-52f9e74bd059; https://www.theguardian.com/technology/2017/oct/01/cambridge-analytica-big-data-facebook-trump-voters When asked if Cambridge Analytica would provide American voters with all 5000 data points in their profile if they request under UK data protection law, their CEO Alexander Nix incorrectly said the law didn't apply to Americans.

[84] See a similar problem in the context of mHealth: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf.

[85] Article 28(3) of the GDPR.

[86] ICO Big Data guidance, p. 5.

[87] Preliminary request to the CJEU in the case C-210/16, http://curia.europa.eu/juris/document/document.jsf?text=&docid=181773&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

[88] See AG opinion in the case C-210/16, http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN.

[89] See AG opinion in the case C-210/16, para. 57 http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN.

[90] Article 5(1)(b).

[91] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, pp. 32-33.

[92] For example, to understand what information political parties in Germany possess about the voters, see here: https://policyreview.info/articles/analysis/restrictions-data-driven-political-microtargeting-germany.

[93] 'Incompatible: The GDPR in the Age of Big Data' Tal Z. Zarsky pp. 1006-1007, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.

[94] Ibid., p. 34.

[95] 'Incompatible: The GDPR in the Age of Big Data' Tal Z. Zarsky pp. 1008-1009, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.

[96] Ibid., pp. 47-48.

[97] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, p. 40.

[98] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9 March 2017), https://rm.coe.int/16806fd666, p. 6.

[99] London School of Economics 'Media Policy Brief 19: The New Political Campaigning' pp. 9, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.

[100] Political finance regulation at the June 2017 UK general election 'Report on the UK Parliamentary General Election held on 8 June 2017' November 2017 pp. 12-15,

https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/237550/Political-finance-regulation-at-the-June-2017-UK-general-election-PDF.pdf.

[101] Common Market Law Review, Vol, 54 (2017), Issue 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law, p. 7, https://www.ivir.nl/publicaties/download/CMLR_2017.pdf.

[102] EDPS Preliminary opinion, p. 23.

[103] Article 6(1).

[104] This could be in breach of Article 6(1)(a) and Annex I No 7 UCPD, p. 149 of Consumer protection policies, strategies and statistics http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf.

[105] By presenting fake 'likes' to consumers, a trader may mislead consumers about its own reputation or the reputation of its products or services, possibly causing consumers to take transactional decisions they would not have taken otherwise. Article 6 of the Directive, http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf, p. 144.

[106] For example, recent research suggests that success on social media can have a self-reinforcing effect. Each Facebook profile and post contains a lot of "social information": every user can immediately see the apparent success or non-success of certain posts and profiles by looking at the number of shares, likes and followers which Facebook always provides. A high number of interactions can thus signal the high importance and validity of certain messages […] Many public figures, especially politicians, have hundreds of thousands of fake followers on Twitter. Facebook on the other hand has fewer automated profiles, although their number is still estimated to be around 65 million (Facebook had close to two billion total profiles by March 2017)", http://www.delorsinstitut.de/2015/wpcontent/uploads/2017/04/20170419_SocialNetworksandPopulismDittrich.pdf.

[107] EctHR has recognized that the national authorities have a broader margin of appreciation when determining hte necessity and proportionality of interference with commercial speech (see e.g. Markt intern Verlag GmbH and Klaus Beermann v. Germany, 20 November 1989; Krone Verlag GmbH & Co. KG v. Austria (No. 3), 11 December 2003, paragraph 31), whereas freedom of political debate deserves a higher level of protection, and interference with it can be justified by weighty reasons only (see e.g. Lingens v. Austria, 8 July 1986).

[108] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/1170616, Garante per la Protezione dei Dati Personali, Resolution on the Use of Personal Data for Political Communication, see preamble. [doc. web n.1170616].

[109] EDPS opinion on the coherent enforcement in the age of big data, p. 14.

[110] From the press-release of the competition authority: "We are mostly concerned about the collection of data outside Facebook's social network and the merging of this data into a user's Facebook account. Via APIs, data are transmitted to Facebook and are collected and processed by Facebook even when a Facebook user visits other websites. This even happens when, for example, a user does not press a "like button" but has called up a site into which such a button is embedded. Users are unaware of this. And from the current state of affairs we are not convinced that users have given their effective consent to Facebook's data tracking and the merging of data into their Facebook account. The extent and form of data collection violate mandatory European data protection principles.", https://webgate.ec.europa.eu/multisite/ecn-brief/en/content/germany-bundeskartellamt.

[111] https://edps.europa.eu/sites/edp/files/publication/17-11-30_statement_2nd_meeting_dch_en.pdf Second meeting of the Digital Clearinghouse, Brussels 27.11.2017.

[112] https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_en European Commission 'Public consultation on fake news and online disinformation' 13.11.2017-23.02.2018.

[113] E.g. https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.

[114] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf, Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) p. 16-17.

[115] https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en European Data Protection Supervisor, A crucial moment for communications privacy. 27.09.2017.

[116] More information about different profiling practices: privacy international submission, pp. 4-6.

[117] https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf, European Data Protection Supervisor, Opinion 1/2015 Mobile Health *Reconciling technological innovation with data protection* para. 32.

[118] https://policyreview.info/articles/analysis/restrictions-data-driven-political-microtargeting-germany, Internet Policy Review 'Restrictions on data-driven political micro-targeting in Germany' p. 2. 31.12.2017.

[119] Reference to expert group report.

[120] See for example Expert group report ; for overview of strategies Dead Reckoning: Navigating Content Moderation after "fake news"', February 2018; Macron draft law requiring online platforms to reveal when items labelled as information are sponsored; UK **; Germany**.
[121] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf, Common Market Law Review, Vol.54 (2017), Issue 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law p. 28.
[122] http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf, p. 143. Equally, under the data protection law, depending on the data processing activity at stake, they can qualify as both controllers and processors.
[123] EDPS Preliminary opinion, p. 35.
[124] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf Common Market Law Review, Vol.54 (2017), Issue 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law P.20-22.

[125] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/1170616 Garante per la Protezione dei Dati Personali, 'Resolution on the Use of Personal Data for Political Communication'. [doc. web n. 1170546].

[126] http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II-Repository_CNIL_UJI_October-2016.pdf, Phaedra II 'Guidance on political campaigning' p. 2. October 2016.
[127] https://www.cnil.fr/sites/default/files/atoms/files/guide_cnil_et_csa.pdf. CNIL 'Pluralisme dans les médias audiovisuels. Règles informatique et Libertés'. Also, most recently, ICO stated that it cooperates with the Electoral Commission in their investigation into data analytics for political purposes, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.

[128] EDPS Opinion on the coherent enforcement in the age of big data, p. 11.
[129] This power is not limited to the supervisor authorities, but also extends to the Member States, the supervisory authorities, the Board and the Commission.
[130] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 p. 19.
[131] From the empirical research on the use of political-micro targeting techniques by the Dutch political parties: „Opinion Meeting the challenges of big data (7/2015)Especially D66 and the seniors' party 50PLUS take a principled stance against the collection of data and the use of PBT. Where D66 presents itself as a privacy champion and therefore will never gather and use information about (groups of) voters, 50PLUS campaign leader 6 warns about the risk of irresponsible use of the data gathered by the "almost stalking of people", which he calls "morally irresponsible". (https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting).
[132] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf Opinion 9/2016 EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data, Para 1.

[133] Press Release: European and Middle Eastern consumers deeply conflicted over piracy and security priorities, 17.05.2017.https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968.
[134] European Commission, Data Protection. Rules for the protection of personal data inside and outside the EU. http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf .
[135] Opinion on 'Meeting the challenges of big data", p. 29; also https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf, p. 14.
[136] On the 'practical and effective' doctrine, see https://academic.oup.com/hrlr/article-abstract/5/1/57/606751 *Human Rights Law Review*, Vol.5, Issue 1 'The Creativity of the European Court of Human Rights', 01.01.2015.

[137] Article 47(1) of the Charter of Fundamental rights. The Court of Justice enshrined the right to effective remedy in its judgment of 15 May 1986 as a general principle of Union law (Case 222/84 Johnston [1986] ECR 1651; see also judgment of 15 October 1987, Case 222/86 Heylens [1987] ECR 4097 and judgment of 3 December 1992, Case C-97/91 Borelli [1992] ECR I-6313).
[138] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-

september-2017/168075f8e9, pp. 41-42. See also WP29 opinion on profiling and automated decision-making, p. 5.

[139] E.g. MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, pp. 41-42.

[140] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, pp. 41-42.

[141] Directorate General for Internal Policies, 'Overview of existing collective redress schemes in EU Member States' See e.g. p. 9, http://www.europarl.europa.eu/document/activities/cont/201107/20110715ATT24242/20110715ATT24242EN.pdf.

[142] During the process of drafting of the GDPR, EDPS advised the legislator, in light of clear obstacles to obtaining redress in practice, to provide individuals with a possibility to be represented by bodies, organisations and associations in legal proceedings. See Opinion 3/2015 'Europe's big opportunity', EDPS recommendations on the EU's options for data protection reform, p.6. https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf.

[143] EDPS Opinion on the proposal for ePrivacy regulation.

[144] The possibility for a representative body to launch a collective action on behalf of non-identifiable victims (opt-out).

[145] With respect to opt-out collective redress BEUC indicated the following, "It has been shown in various cases that opt-out is much more effective than opt-in (on average, only around 1% of all harmed consumers opt-in). It is difficult to get consumers to sign-up to an opt-in action, given that they are required to do so at the start of proceedings, before they know if it will be successful. Opt-out collective redress successfully functions in Portugal, the Netherlands, partly in Spain. It is allowed in Belgium and the UK (in the latter, for competition damages private claims, and introduced very recently, so still too early to evaluate)," http://www.beuc.eu/publications/beuc-x-2017-086_ama_european_collective_redress.pdf. For the overview of collective redress mechanisms available across Europe, see https://www.opensocietyfoundations.org/sites/default/files/litigation-kosa-hungary-thirdparty-20170201.pdf. Notably, in the Recommendation on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, the Commission determined that the recourse to opt-out collective redress mechanisms may be justified "by reasons of sound administration of justice", see Article 21, , Commission Recommendation of 11.06.2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (2013/396/EU) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2013_201_R_NS0013.