EUROPEAN DATA PROTECTION SUPERVISOR

Summary of EDPS Opinion on online manipulation and personal data

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2018/C 233/06)

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 audiovisual regulators.

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

([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].

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' ([1]). 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 ([2]).

— 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 ([3]).

([1]) 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].

([2]) 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 26.3.2014 [doc. web n. 3013267].

([3]) 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) 8.11.2016.

— 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 ([1]).

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 ([2]).

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 ([3]). 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 ([4]). 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 ([5]). 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' ([6]).

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 ([7]). It increases the pervasiveness and persuasiveness of false stories and conspiracies ([8]). Research suggests that the manipulation of people's newsfeed or search results could influence their voting behaviour ([9]).

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 ([10]). 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

([1]) https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].

([2]) 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.

([3]) 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.

([4]) 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).

([5]) EDPS Opinion 7/2015 Meeting the challenges of big data, p. 9.

([6]) Report of the EDPS Ethics Advisory Group, January 2018, p. 28.

([7]) See for example The Economist, How the World Was Trolled (November 4-10, 2017), Vol. 425, No 9065, pp. 21-24.

([8]) 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.

([9]) 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.

([10]) 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'.

approach the European Parliament elections of 2019 ([1]). 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 ([2]). 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.

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 audiovisual 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

([1]) 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.

([2]) 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.