EU Fundamental Rights and Digitalisation

Policy brief

Findings of the Jean Monnet NOVA EU project relevant for policy makers

Authors

Dr. Maja Brkan, Associate Professor of EU Law, Faculty of Law, Maastricht University

Valentina Golunova, PhD student, Faculty of Law, Maastricht University

Executive summary

The trend of digitalisation taking place at an extremely fast pace resulted in a gap between the state of technological innovation and relevant legal regulation. In order to ensure effective protection of fundamental rights, it is crucial that EU legal framework is brought in line with the recent digital transformations.

The main objectives of this policy brief are to:

1. describe the societal implications of digitalisation in the EU;
2. reflect on potential threats to fundamental rights posed by digital tools deployed by both public and private actors;
3. recommend changes to the EU legislation that could enhance protection of fundamental rights in the light of digitalisation.

Based on contributions of participants during the NOVA-EU workshop on *Digitalization, Ethics and EU Fundamental Rights,* the EU legislator is advised to:

1. set out limits on the use automated tools for online content moderation and oblige digital platforms to put in place effective safeguards against unlawful interference with freedom of expression;
2. stipulate transparency obligations for media companies which make use of digital tools for content creation in order to preserve integrity of information;
3. increase fairness and transparency of algorithmic decision-making by stipulating the right to explanation of algorithmically-generated outcomes and revising the scope of prohibition of discrimination;
4. elaborate safeguards against unlawful interference with freedom of elections due to political microtargeting, with due regard to propositions made by the European Commission and the European Parliament;
5. define instances in which legal analytics tools may be used by judges to facilitate decision-making;
6. reflect on horizontal application of fundamental rights that can be affected by private actors making use of digital tools;
7. enshrine specific duties incumbent on private actors relating to the use of digital tools under EU secondary legislation.

Introduction

Both public and private entities benefit greatly from the development and implementation of digital technologies. Machine learning algorithms, which constitute one of their most prominent type, are used extensively in many different fields: from powering voice recognition devices and self-driving cars to revolutionising healthcare by increasing accuracy of screenings and selection of medical treatment. While the societal value of algorithms cannot be underestimated, proliferation of such tools has also brought entirely new legal challenges. The use of algorithms can severely compromise effective protection of fundamental rights and freedoms guaranteed by the Charter of Fundamental Rights of the European Union (hereinafter Charter) and the European Convention of Human Rights (hereinafter ECHR). For example, if a person is sentenced to a longer term in prison due to the algorithm's prediction that they are likely to commit another crime in the near future, the individual's right to a fair trial is triggered. In the same vein, if a person's loan application is declined by a bank because it employed an AI-driven tool that predicted a low likelihood of repaying this debt, it can amount to discrimination. The unprecedented nature of legal dilemmas inspired by state-of-the-art algorithmic tools gives rise to fierce debates on the ways in which negative impacts of digital technologies can be addressed.

Objectives

The primary aims of this policy brief are (1) to expose threats to fundamental rights stemming from the use of state-of-the-art technologies, and (2) to point out legal avenues that can be taken by the EU legislator in its pursuit of ensuring adequate protection of fundamental rights in the digital age. Various social phenomena that emerged by virtue of cutting-edge technology are first described. Then, it is explained which novel threats such phenomena pose to protection of particular fundamental rights. Subsequently, policy solutions that can be adopted at the EU level in order to prevent or mitigate risks to enjoyment of fundamental rights are outlined.

NOVA-EU workshop

This policy brief is the outcome of the Jean Monnet project *Innovating and transforming the European Union* (NOVA-EU). Scholars with diverse expertise in the fields of law, political science, and technology convened in Maastricht on the 9th and 10th of January 2020 to take part in NOVA-

EU workshop on *Digitalization, Ethics and EU Fundamental Rights*. Participants made numerous contributions to discussions on controversial topics, including the constitutional questions of digitalization, the role of ethics, regulation of digital platforms, digitalization challenges in judicial proceedings, the impact of artificial intelligence on democracy, problems relating to automated decision-making, and digital aspects of border control. This policy brief highlights the most pressing policy concerns and provides insights into how such issues may be effectively regulated on the level of the EU.

Policy recommendations

1. Freedom of expression

Article 11 of the Charter, which corresponds to Article 10 ECHR, guarantees *'freedom to hold opinions and to receive and impart information and ideas'*. Controversial issues of automated content moderation carried out by Internet intermediaries as well as the use of AI by media platforms, both of which challenge the scope of this provision, are addressed below.

1.1. Automated content moderation

Aiming at combating objectionable content online, many Internet intermediaries currently deploy automated moderation tools. The recourse to these instruments as one of the means of countering defamatory speech and disinformation is also endorsed by both the European Court of Justice[1] and the European Commission.[2] However, while automated tools may be effective for removing repetitive spam messages or materials infringing copyright, their accuracy is potentially lower when it comes to reviewing more complicated content, such as incitement to violence or hate speech. Due to limited capabilities of instruments for automated content moderation to carry out comprehensive semantic and contextual analysis of information published online, their excessive use may result in a disproportionate removal of legitimate content and, consequently, violation of Article 11 of the Charter. **Consequently, it is viewed that the EU legislator should set the boundaries for a permissible use of automated means for content**

[1] Case C-18/18 *Glawischnig-Piesczek* EU:C:2019:821, para 46.
[2] Commission Recommendation on measures to effectively tackle illegal content online, C(2018) 1177 final, p. 12; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: a European approach, COM(2018) 236 final, pp. 10 – 11.

moderation in the secondary legislation. In addition, this brief argues that it is crucial to introduce effective safeguards against its negative impact on freedom of expression, including effective human oversight and the right of users to contest the removal of content.

1.2. Automated journalism

A number of modern media platforms currently deploy not only human journalists, but also tools for automated content production and enabling automated editorial control. However, since the ways in which such 'robot' reporters and editors approach their tasks are not always transparent, it is difficult to establish whether the principle of journalist ethics, such as objectivity and impartiality, are duly respected.[3] In turn, this can result in the interference with the freedom of expression by platforms that implement automated systems for generating or editing content. **Therefore, the EU legislator should introduce additional transparency duties for media platforms that implement AI-driven tools to facilitate their activities.**

2. Prohibition of discrimination

Machine learning algorithms are now widely implemented in many different spheres. Nevertheless, while the use of such AI-driven tools may certainly be beneficial due to the high speed of data processing and the possibility to automated decision-making, it may lead to illegitimate distinctions between individuals, when algorithms are set up inappropriately. The so-called 'algorithmic injustice'[4] that arises whenever a person is denied a parole or rejected by a potential employer without objective grounds could clash with Article 21 of the Charter that bans '*any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'*. The largely equivalent grounds for discrimination are also prohibited by virtue of Article 14 ECHR. Since most algorithms are opaque,

[3] N. Helberger, S. Eskens, M. van Drunen, M. Bastian, J. Moeller, 'Implications of AI-driven tools in the media for freedom of expression' (2019). URL: <https://rm.coe.int/coe-ai-report-final/168094ce8f> (accessed on 7 June 2020).

[4] A. Zimmermann, 'Algorithmic Injustice Beyond Discriminatory Harm' (2017) 165 *University of Pennsylvania Law Review* 633, at p. 635.

which leads to the impossibility to deduce the full logic of a particular AI-driven tools, their use could lead to an unlawful interference with Article 21 of the Charter.

In addition, it has been argued that the circumstance that machine-learning systems draw correlations and inferences within the available dataset can lead to discrimination on grounds other than those regulated by Article 21 of the Charter or Article 14 ECHR.[5] For instance, profiling of individuals while compiling input data may in certain cases amount to a new phenomenon of 'collective discrimination' due to its impact on the entire groups of people.[6] Since individuals subject to algorithmic decision-making are at risk of being discriminated on grounds not enshrined in respective provisions, there is a risk that the respective provisions are obsolete in the machine learning context.

These observations call for a twofold policy response. On the one hand, it is suggested that **the EU legislator reflects upon regulating the right to explanation for individuals who have been affected by a relevant outcome in order to increase transparency of algorithmic decision-making.** On the other hand, the EU policy-maker could **consider whether it is necessary to revive the debate on the scope of the prohibition of discrimination enshrined by the Charter, which would include measures that would seek to prevent newer types of discrimination generated by AI tools**.

3. Freedom of elections

In the age of vigorous political competition, candidates are constantly searching for new ways of attracting supporters and ensuring their supremacy over competitors. Political microtargeting, used as a strategy for reaching out to voters by means of political advertisements customized on the basis of voters' personal data, has become an integral part of many contemporary campaigns.[7] The effectiveness of this practice is attributed to its data-driven nature. It is nowadays possible to customize political advertisements shown to individual voters on the basis of inferences made from basic information about a person. For example, by taking into account a person's date of birth, place of residence and circle of friends, a social media platform may

[5] F. Z. Borgesius, 'Discrimination, artificial intelligence, and algorithmic decision-making' (2018). URL: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> (accessed on 26 February 2020).
[6] J. Mazur, 'Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law' (2018) 3 Erasmus Law Review 178, p. 180.
[7] M. Brkan, 'Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting' (2019) 2 *Delphi* 66, p. 68.

assume which political views this person is likely to have and start offering a very precise targeted political advertisements to induce them to vote for a particular candidate. However, such an intrusive practice may also result in opinion manipulation, in particular if coupled with dissemination of disinformation.[8] It can ultimately have an adverse effect on the value of democracy and the fundamental right to freedom of elections guaranteed by Article 39 of the Charter.[9]

Due to the complexity of this phenomenon, there is a lack of consensus concerning the most effective ways in which political microtargeting may be regulated. One of the suggestions with respect to tackling this problem was provided by the European Commission and the European Parliament, which are in favour of **increasing transparency by providing voters with information about the political party or organisation which financed a particular advertisement**.[10] Nevertheless, even if a person is aware of the fact that they have just been shown a sponsored political advertisement, there is still a high likelihood that their views will be affected by it.

Therefore, another possible solution is **to impose a duty on digital platforms to enable users to opt out of the regime that implies collection and processing of both sensitive and non-sensitive personal data for the purpose of political microtargeting**. However, the disadvantage of this approach is that a large proportion of users of social media or browsers agree to 'default' settings and that those settings usually favour the opt-in regime, which still leaves a great number of voters exposed.[11] The users opting out of political microtargeting are potentialy those with a higher awareness of risks of political microtargeting.

Consequently, a more stringent approach pursued by the European Parliament **is to entirely ban the profiling of voters for the purposes of political microtargeting by political parties and**

[8] M. Crain and A. Nadler, 'Political Manipulation and Internet Advertising Infrastructure' (2019) 9 *Journal of Information Policy* 370, p. 371.
[9] F. Z. Borgesius *et al*, 'Online Political Microtargeting: Promises and Threats for Democracy (2018) 14(1) *Utrecht Law Review* 82, p. 87.
[10] Commission Recommendation of 12 September 2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, C(2018) 5949, point 7; European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)), point 5.
[11] T. Room, I. Stanley-Becker and C. Timberg, 'Facebook won't limit political ad targeting or stop false claims under new ad rules', 9 January 2020, *The Washington Post*. URL: <https://www.washingtonpost.com/technology/2020/01/09/facebook-wont-limit-political-ad-targeting-or-stop-pols-lying/> (accessed on 22 January 2020).

digital platforms.[12] Due to seriousness of threats posed by political microtargeting, this could be the most effective solution for safeguarding democratic values, such as the freedom to shape political views and the right to vote without any external pressure. However, this solution would need to be accompanied with a clear indication which specific personal characteristics cannot serve as a basis for profiling. A possibility would be to prohibit profiling based on special categories of personal data.[13] Another possibility would be to more broadly prohibit any profiling that could lead to identification of political opinion of voters through inferences. However, any prohibition would need to be balanced with the freedom of expression of political parties. In any event, prohibition of profiling for the purposes of *micro*targeting would not amount to the prohibition of non-targeted political advertising altogether, but only to specification of criteria on the basis of which targeted advertisements can (not) be designed.

4. Right to a fair trial

AI-driven tools are being increasingly used by public authorities, including courts and law enforcement authorities. Nevertheless, while such algorithmic instruments have a great potential for dealing with backlogs or improving efficiency of criminal investigation, the lack of clear-cut boundaries for their use may also significantly challenge the standard of protection of Article 47 of the Charter that lays down the right to a fair trial.

The new era of judicial proceedings was marked by the invention of legal analytics, which are data-driven tools for gaining insight into possible outcomes of a legal case on the basis of existing law and preceding jurisprudence.[14] However, the 'black-box' nature of algorithms used in legal analytics may lead to outcomes that were not reasonably anticipated and cannot be logically explained by a judge. This, in turn, can impair the fundamental principle of fairness of court proceedings. Furthermore, the excessive reliance of judges on legal analytics may have an adverse impact on their impartiality as they would be likely to trust algorithmically generated conclusions and avoid reaching their own conclusions. Therefore, it is maintained that **the EU**

[12] European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP)), point 9.
[13] For a definition of special categories of personal data, see 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 (General Data Protection Regulation), OJ 2016 L 119/1, Article 9.
[14] K. D. Ashley, *Artificial Intelligence and Legal Analytics. New Tools for Law Practice in the Digital Age*, (Cambridge University Press, 2017), p. 14.

legislator should specify the types of cases in which the use of legal analytics could be permissible as well as restrict its utilisation in complex cases where an interpretation of a legal norm or extensive analysis of factual background is essential.

5. Fundamental rights and the conduct of private entities

Private sector is currently standing at the forefront of using digital tools to advance their business operations. However, massive deployment of such instruments entails far-reaching negative effects on enjoyment of fundamental rights. For instance, some technology companies implement facial recognition technologies to increase effectiveness of targeted advertising, which gives rise to privacy concerns.[15] AI-powered content recommendation systems that can nowadays be found on many social media platforms serve as another example, as they can interfere with the right of users to receive information and ideas.[16]

According to the conventional approach, the EU fundamental rights can only have a vertical application. It means that an individual can only invoke the Charter provisions vis-à-vis public authorities, such as EU institutions, its bodies and Member States when they are implementing EU law. Even though the existing paradigm of fundamental rights protection has recently been subject to certain changes,[17] it is still uncertain to what extent private bodies are bound by fundamental rights duties. While many private companies accede to various ethical instruments, the latter usually lack a binding force, which impedes effective protection of fundamental rights. The following sections throw light on current issues, such as the lack of a duty to foresee and mitigate risks as well as the rise of private self-regulation, and offer recommendations on possible ways to tackle them.

5.1. Horizontal application of fundamental rights

While the duty to respect and protect fundamental rights has traditionally been attributed exclusively to states, in some cases they can also apply in relationships between private parties. This was confirmed by the European Court of Justice in

[15] S. Monteleone, 'Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?' (2012) 3(3) European Journal of Law and Technology,

[16] J. Möller, D. Trilling, N. Helberger and B. van Es, 'Do not blame it on the algorithm: an empirical assessment of multiple recommender systems and their impact on content diversity' (2018) 21(7) *Information, Communication & Society* 959, pp. 960 – 961.

[17] Case C-414/16 *Egenberger* EU:C:2018:257, paras 76 – 77; Joined cases C-569/16 and C-570/16 *Bauer* EU:C:2018:871, para 89.

Egenberger and *Bauer* cases.[18] However, these judgments only concerned horizontal application of three fundamental rights, namely prohibition of discrimination, the right to paid annual leave, and the right to an effective remedy. In order to afford even more comprehensive protection in the face of digitalisation, **the doctrine of horizontal application of fundamental rights to the conduct of private actors can be further developed.** It is of particular importance to recognise that big technology companies which have a big impact on lives of many individuals must respect basic civil liberties guaranteed by the Charter.

5.2. *Introduction of fundamental rights duties of private parties in EU secondary legislation*

While recognition of horizontal application of fundamental rights can significantly enhance the protection of fundamental rights, the scope of duties incumbent on private entities can still remains unclear. For the sake of legal certainty, specific duties of private parties should also be stipulated explicitly. As private entities are gradually becoming aware of diverse challenges brought by the use of machine learning algorithms, many of them elaborate self-regulatory duties based on codes of conduct and ethical guidelines.[19] However, given that such guidelines lack binding legal nature and cannot be subject to legal enforcement, there is a risk that private parties may remain unaccountable even if they violate fundamental rights. Moreover, an excessive amount of self-regulation results in the lack of coherence among policies pursued by different private actors. Therefore it is viewed that **the EU policy-maker should consult with private entities in order to develop binding secondary legislation stipulating the minimum set of safeguards against the adverse impacts of digital tools on enjoyment of fundamental rights.**

[18] Case C-414/16 *Egenberger* EU:C:2018:257, paras 76 – 77; Joined cases C-569/16 and C-570/16 *Bauer* EU:C:2018:871, para 89.

[19] Artificial Intelligence at Google: Our Principles. URL: <https://ai.google/principles/> (accessed on 22 January 2020); Microsoft, Responsible AI: Establishing guiding principles. URL: <https://aischool.microsoft.com/en-us/business/learning-paths/identify-guiding-principles-for-responsible-ai-in-your-business/responsible-ai-establishing-guiding-principles/responsible-ai-establishing-guiding-principles> (accessed on 22 January 2020).

Conclusion

AI-driven tools are extremely effective for optimizing a large number of tasks and overcoming many current issues, therefore further innovations in this field should be strongly encouraged. Along with that, instruments powered by machine learning algorithms may also become the cause of serious breaches of a wide array of fundamental rights when used irresponsibly by both public and private actors. Due to the complex nature of issues, the means of ensuring effective protection of fundamental rights in the digital age should now be sought not only in the legal, but, in view of the approach of fundamental rights by design, also in the technological domain. Nevertheless, it is the binding secondary law, not just ethics, which must provide clear framework for every innovative undertaking and lay down legitimately established boundaries for the use of AI-driven tools.[20] Even though it is still difficult to envisage any concrete solutions to many current issues and there are many pathways which can be pursued by the EU legislator, it is crucial to take an active stance on this matter to ensure that the provisions of the Charter are not compromised in the era of digitalisation.

[20] K. Yeung, A. Howes and G. Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing' in M. D. Dubber, F. Pasquale and S. Das. (eds.), The Oxford Handbook of Ethics of AI (Oxford University Press, 2019), p. 7.