

Between Anarchy and Censorship

Public discourse and the duties of social media

Judit Bayer

No. 2019-03, May 2019

CEPS Papers in Liberty and Security in Europe offer the views and critical reflections of CEPS researchers and external collaborators on key policy discussions surrounding the construction of the EU's Area of Freedom, Security and Justice. The series encompasses policy-oriented and interdisciplinary academic studies and comment on the implications of Justice and Home Affairs policies within Europe and elsewhere in the world.



This paper has been prepared as part of the ENGAGE II Fellowship Programme, with support by the Open Society Initiative for Europe (OSIFE). The Fellowship Programme involves academic, civil society and think tank actors from Central and Eastern Europe, the Western Balkans and Eastern Partnership countries. It engages selected fellows in EU-level policy debates on the rule of law in domains such as rights and security, foreign and economic affairs. The programme entails training, study visits, public events and the publication of policy papers. See the penultimate page for more details about the ENGAGE II Fellowship.

The programme is coordinated by the CEPS Justice and Home Affairs Unit and includes several CEPS senior research fellows. This publication has been written under the supervision of Sergio Carrera, Head of CEPS Justice and Home Affairs Unit.

Judit Bayer is Professor of Media Law and International Law at the Budapest Business School, University of Applied Sciences.

Unless otherwise indicated, the views expressed are attributable only to the author in a personal capacity and not to any institution with which she is associated. This publication may be reproduced or transmitted in any form for non-profit purposes only and on the condition that the source is fully acknowledged.

Contents

- Executive summary 2
- 1. Problem setting..... 4
- 2. The new public sphere 6
 - 2.1 Features of social media communication7
- 3. Media vs social media..... 8
 - 3.1 The newly emerged functions of social media platforms8
 - 3.2 Similarities of social media and traditional mass media..... 10
- 4. Existing legal regulation of social media platforms..... 12
 - 4.1 The responsibility structure of the e-Commerce Directive 12
 - 4.2 The German Network Enforcement Act..... 13
 - 4.2.1 The notice-and-notice system vs notice-and-takedown 15
 - 4.3 Case law of the CJEU and ECtHR on the responsibility of intermediary service providers..... 15
 - 4.3.1 *L'Oréal v eBay* 15
 - 4.3.2 *Delfi v Estonia* and *MTE & Index v Hungary* 16
 - 4.4 The principle of immunity for third-party content 17
 - 4.5 The limits of self-regulation 18
- 5. Conclusions 18
- 6. Recommendations 19
 - 6.1 Definition of platform providers 20
 - 6.2 Recommendations in the realm of media regulation – Classical principles applied to social media 21
 - 6.2.1 Diversity, pluralism and impartiality 21
 - 6.2.2 Identification of advertisements, notably political advertisements 23
 - 6.3 New, internet-specific regulatory principles 25
 - 6.3.1 Administering platforms..... 25
 - 6.3.2 Protecting privacy and personal data..... 28

Between Anarchy and Censorship

Public discourse and the duties of social media

Judit Bayer

CEPS Paper in Liberty and Security in Europe No. 2019-03, May 2019

Abstract

Social media platforms have become powerful enough to cause perceptible effects in societies on a global scale. They facilitate public discussion, and they work with excessive amounts of personal data – both activities affecting human rights and the rule of law.

This specific service requires attention from the regulator: according to this paper, a new legal category should be created with clear definitions, and a firm delineation of platforms' rights and responsibilities.

Social media companies should not become responsible for third-party content, as this would lead to over-censorship, but they should have the obligation to create and maintain safe and secure platforms, on which human rights and the rule of law are respected. In particular, they should maintain the transparency and viewpoint-neutrality of their services, as well as protect the personal data of their users. The paper sheds light on the similarities and differences from traditional media, and sets out detailed policy recommendations.

Executive summary

The internet's vast opportunities to facilitate free speech had been thought to advance the level of democratic participation and a discussion based on reason, instead of self-interest or political power. Social media platforms have become powerful enough to cause perceptible effects on the political discourse on a global scale. Their impact has reached a level that threatens democratic processes and social stability.

Providing platforms has become a successful business model in several industries, but in media it has an outstanding significance due to its impact on the formation of public opinion. Their activity has some resemblance to traditional media, but even more important are the differences: they do not edit content although algorithmically organise it, they work with excessive amounts of personal data and their market is more concentrated. However, they are still expected to neutrally transmit ideas without imposing their own agenda, and to facilitate public discourse on a larger scale than ever before in the history of mankind.

This paper argues that platform providers, and among them social media companies, should be given a specific place on the map of service providers. Their particular role indirectly compromises basic fundamental rights, democratic public discourse and the rule of law. These responsibilities call for a new pattern of regulation, which clearly defines their rights and obligations. For example, social media companies should not be accountable for third-party content, because as private entities they cannot ensure the constitutional safeguards that are necessary to respect freedom of expression. But they can be responsible for creating and maintaining a safe and secure framework through administering the platform's communication environment, which can include prioritising diversity, identifying advertisements, protecting users' personal data and empowering users through transparent algorithms. Such a detailed approach is recommended because the problem is more fluid than just regulating illegal or harmful content. Flooding the conversation with the help of bots and trolls with irrelevant or false information, attacking persons with a troll army to discourage their communication or targeting individual users with tailored and therefore manipulative information cannot be tackled by regulation of content. The main research questions are (i) what are the responsibilities of social media and (ii) to whom should it be accountable?

The following recommendations involve the extension of existing legal principles to platform providers, among them social media platforms:

- 1) The e-Commerce Directive should be amended with a new definition of platform providers, including a basic definition of the extent of their rights and obligations.
- 2) Platform providers must not apply viewpoint discrimination in their algorithmic structuring of content or in any action as part of administering their platforms.
- 3) Content selection algorithms should offer options for users, and foster diversity.
- 4) Interoperability would be needed to prevent the formation of monopolies; dominant market powers must have legal responsibilities.

- 5) All advertisements, including political advertisements, should be clearly distinguishable from voluntary content. Existing rules on political and public issue advertising are to be extended to any publication method, with special regard to online media, including social media. Advertisers must be identifiable for users.
- 6) Other recommendations are specifically addressed at the new functions of platform providers:
- 7) Platforms should ensure – by technological means of supervision or verification – that accounts are registered by human individuals rather than by artificial intelligence or bots; otherwise, bots, virtual personalities, trolls and influencers (political parties, NGOs, communication agencies) should be identified as such.
- 8) Implementation of the General Data Protection Regulation has to consequently and meticulously be enforced; this may need to be assisted by interpretative guidelines.
- 9) Platform providers should have explicit responsibility for protecting their users' personal data, including the prevention of hacking and leaks, as well as illegal activity that compromises the protection of personal data on their platforms, and for informing users about the processing of their data and effectively offering users the right to opt out of data processing.

1. Problem setting

Deliberative democracies are built on the free exchange of information, and an uninhibited public discourse. An open public discourse is one of the basic conditions of democracy, because this is how citizens can discuss their common matters, form political opinions and ultimately reach a political decision (e.g. voting in elections).¹ The relation between freedom of expression, the right to receive information and informed participation in a democracy clearly illustrates the triangular nature of democracy,² according to which democratic processes, the rule of law and human rights are “inherently and indivisibly interconnected, and interdependent on each of the others”.³

Social media companies have become key actors in the formation of public opinion. The popularity of social media has contributed to the crisis of journalism and traditional media, it has accelerated social movements (e.g. #MeToo, Black Lives Matter) and contributed to political changes, as shown by the Arab Spring and by the 2016 US elections. Social media appears to be a powerful instrument to promote connection and communication for those who devote time and resources to use it. Its rules and principles have been formed mainly by market interests until this year. In 2018, the General Data Protection Regulation (GDPR)⁴ as well as other tools and regulations worldwide tried to tackle the adverse effects that are regarded as being caused by social media companies. But what is their responsibility really, and to whom are they accountable?

This paper argues that online platform providers, and among them social media platforms, offer a new package of services by aggregating information and providing a bridge between supply and demand – whether it is goods like those on eBay, transport like Über, tourism like Airbnb or content like that on Facebook or Instagram.⁵ Social media services are particularly different from traditional media services, as explained below. The rights and obligations attached to this new structure of services are not governed by a legal framework.

This complex type of new service requires a new pattern of regulation. The current schemes of self-regulation and the old scheme of mass media regulation would either be insufficient to

¹ Bayer et al., “Disinformation and propaganda – Impact on the functioning of the rule of law in the EU and its Member States”, Study for the Policy Department C: Citizens' Rights and Constitutional Affairs, 2019, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf), pp. 11, 52.

² Ibid., at p. 61.

³ S. Carrera, E. Guild & N. Hernanz, “The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU, Towards an EU Copenhagen Mechanism”, Study, CEPS, Brussels, 2013.

⁴ General Data Protection Regulation (Regulation 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), <http://data.europa.eu/eli/reg/2016/679/oj>.

⁵ See also in: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Online Platforms and the Digital Single Market Opportunities and Challenges for Europe”, COM/2016/0288 final.

tackle the problem, or violate the principles of free expression. In the first case, the financial incentive may prove to be more attractive than meaningful self-restriction. In the other case, to mitigate the risk of being fined, social media companies are inclined to delete even constitutionally protected expressions, without the constitutional safeguards of limiting the fundamental right of free expression. The German Network Enforcement Act, (Netzwerkdurchsetzungsgesetz, GNDG, 2017) is an experiment in this regard, where the state outsourced censorship to social media platforms, obliging them to remove criminally prohibited content. This censoring activity remains opaque and unaccountable to an independent body, with no data on how effectively it protects the rights of citizens. In addition, removing criminally illegal content solves only a minor share of the problems in the public discourse. More details about the GNDG are below in section 4.2.

Distorting the public discourse with the help of artificial amplification mechanisms, aggressive distribution and manipulation techniques reaches beyond the problem of ‘illegal content’. This is why focusing on content regulation alone would not deliver sufficient results.

The most influential social media company, Facebook, has repeatedly been used as the vehicle for political manipulation, and the strategic abuse of personal data: in the Cambridge Analytica scandal the personal data of approximately 87 million Facebook users was processed without the users' consent and utilised to create psychographic profiles, which were then used for targeted political campaigning. This illustrates why the protection of personal data can be a cornerstone for the protection of human rights and the rule of law in the realm of new technologies. While traditional services, such as banks, law firms and medical service providers, are obliged to treat personal data confidentially, the new IT services are not subject to such regulation. Until the GDPR, they appeared to treat internet users' personal data as their own.⁶

While Facebook, Inc.'s public relations focus on its cooperativeness, with repeated apologies and promises to create a safe place, these fall short of being accountable for its actions, which is not possible until its responsibilities are legally defined. For example, the prohibition of discrimination in conveying its services, whether based on gender or viewpoint or the explicit obligation to protect users' personal data, among others, should be declared in its regard.

The reach and impact of these new actors may be even larger than that of the biggest traditional media enterprises ever known. They affect societies even though they are not editors of content – but they do set the rules of transmission, defining how widely a message can be heard and which users will encounter it. Their practices have profoundly impacted public discourse, which forms the foundation of democratic societies. This significant power of platform providers justifies state intervention.

Besides the frames of responsibility, also the directions of accountability of platform providers need to be defined. The diverse set of obligations of platform providers could be supervised by

⁶ J. Zittrain, “Engineering an Election” (20 June 2014), *Harvard Law Review Forum*, Vol. 127, 2014, p. 335; Harvard Public Law Working Paper No. 14-28, available at SSRN: <https://ssrn.com/abstract=2457502>, at 340.

independent authorities with appropriate competences to enforce the obligations, such as the authorities for data protection, electoral commissions, authorities responsible for consumer protection, competition or telecommunications.

Freedom of expression can be limited only under narrow conditions: among others, only laws can prescribe limitations, these must be capable of achieving a legitimate social goal that is necessary in a democratic society, and the limitation should not affect the essential content of the right. In addition, only courts are entitled to enforce any such limitation. To ease the enormous caseload of courts, self-regulatory bodies like the complaints commissions and press boards, which are operated by the national media authorities in some EU member states, could decide, and judicial remedy should be granted against their decisions.

2. The new public sphere

The public sphere is the physical or virtual community space where citizens share and exchange their views and opinions on matters of public interest.⁷ Such public discourse serves the formation and discussion of political decisions. A democracy is built on public discourse, the successor of the ancient 'agora'.

In the age of the traditional mass media, much of this public discourse was centrally organised by media actors, content was distributed in forms of hierarchical pyramids from a few centre points to the masses of people. Mass media content represented the elites' culture, and the cycle of content production involved several layers of control.

Social media has fundamentally changed this structure: it has created a horizontal, interactive discursive space for the public. Even though dominant actors of the mainstream media still exist, currently they enjoy no privilege among the many other players of this deliberative space where all users play with equal chances. Every individual has the chance to build a popular social media profile or launch a blog or online journal. This was celebrated once by the early cyber-optimists for providing equal opportunities to all views, and for elevating democracy to a higher level. Indeed, the political discussion has become wider, more inclusive and colourful: the online discourse has enabled many minority views to be heard for the first time. This has led to public recognition of the sufferings of war, revelations of sexual abuse and domestic violence, to name a few. But in recent years, the drawbacks of these same features have also been experienced.

A public sphere that goes global is inducing noticeable changes in social and political actions. Online information campaigns have become used as strategic warfare by certain states. Some states choose to close their communication borders, like China, North Korea, Bangladesh and Iran. Liberal states keep their media spaces open, which therefore can be penetrated and shaped by anyone, including foreign citizens, entities or other states.

⁷ J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, MIT Press, 1991 (Sixth edition).

The attention economy and the characteristics of social media favour short, simple and emotional messages, rather than rational deliberation, which provides a fertile ground for populist messages. While a cause-and-effect relationship can be debated, we can observe that democratic processes and values are being challenged,⁸ in which social media discourse also plays a role.

2.1 Features of social media communication

Among the many other changes in global society, the new media environment is one of the accelerators that generates social changes. The most important characteristics are listed below.

- 1) There are no entrance barriers for publication: anyone can have any number of accounts, even anonyms. This enables the creation of fake profiles as well.
- 2) There is insufficient privacy protection: while anonymity is possible, it is the exception – the average user is exposed and taken advantage of by more powerful users.
- 3) There is no differentiation between individual and company users, with no separation between private, commercial or political content; nor is the identification of sponsored content ensured.
- 4) The communication is horizontal and networked, with no central distribution hub, reactive and interactive.
- 5) Moderation, supervision and control are technically possible, but their legal circumstances need clarification. Platform providers facilitate interaction with their algorithms. They also provide tools for users to amplify their own content. These tools may amend how content is perceived by other users, and thus they affect the market and in our case, the public discourse.
- 6) The reach is global: the boundaries of online communities' discussions are fluid. Their reach is not limited to the relevant political community – anyone can participate, including from other communities. The possibility for external influence, and even manipulation, has manifestly grown.⁹

These characteristics have transformed the communication market in many respects, of which two are pointed out below.

- **Platforms connect users and knock out old gatekeepers.** The function of platform providers has been enabled by the P2P technology of the web: platforms aggregate and redistribute information. Similar to search engines, auction sites, booking or dating sites,

⁸ F. Fukuyama, *Identity: The Demand for Dignity and the Politics of Resentment*, Farrar, Straus and Giroux, 2018.

⁹ While there were previous examples of social manipulation (e.g. the Iranian coup d'état, 1953), the online environment offers far more convenient tools to carry out such.

they knock out traditional gatekeepers whose job was to collect and process content, and to make matches between supply and demand. They serve as new gatekeepers only if the market is too concentrated – and such is the case with social media (see below). This is a new function and it cannot be squeezed into existing categories of media.

- **Platforms have created a global village.**¹⁰ Social media puts **different types of communication into the same basket**: private and public, voluntary¹¹ and sponsored, amateur and professional communications. Without the separation of these types of communication, legal obligations for professional, public and sponsored content are difficult to enforce – especially if they can hide behind anonymous and fake accounts. Private individual communication deserves a higher level of constitutional protection; however, individuals with large social networks can turn their private messages into publicly held views within an hour. This can even turn into action: casualties occurred in India as a consequence of fake WhatsApp messages shared among private individual messaging groups.¹²

3. Media vs social media

3.1 The newly emerged functions of social media platforms

Social media's role and functions are significantly different from those of the traditional mass media. Below the major differences and similarities between traditional media and social media are listed.

Platforms are not editors. Traditional media actors exercise editorial functions over the content distributed. As editors, they define what can be published in the media, and what prominence should be given to each aspect of content. Most of the content that they distribute is created by professional journalists or advertising agencies that also carry responsibility for the content. But the decision on what is published – even regarding small advertisements or readers' letters – is entirely the responsibility of the editor. In contrast, social media platforms do not produce or edit content. No matter how powerful social media platforms may appear, their role is limited to conveying and facilitating communication, with the added value of amplification. Users expect that platforms do not alter or remove posts, unless reported by the user community.

¹⁰ The term "global village" was originally coined by Marshall McLuhan, but gained new meaning in the online age: distances are meaningless, rumour and gossip spreads with the speed of light, privacy gets easily compromised. M. McLuhan, *Understanding Media: The extensions of Man*, MIT Press, 1994 [1964].

¹¹ The adjective "voluntary" is used to describe content that is not sponsored or not published for commercial or marketing purposes.

¹² "How WhatsApp helped turn an Indian village into a lynch mob", 19.7.2018, <https://www.bbc.com/news/world-asia-india-44856910>; "India lynchings: WhatsApp sets new rules after mob killings", 20.7.2018, <https://www.bbc.com/news/world-asia-india-44897714>.

Expectation of impartiality. An editor may set the tone of the media product, and choose to favour one or another political side.¹³ Social media companies also have the technical possibility to give preference to opinions representing a certain viewpoint on their platforms. However, a systematic favouring of one political view would be unacceptable from dominant social media platforms. Users would expect social media to neutrally transmit the content of all users without discrimination – but this is not a legal obligation at the moment. Users can count on the goodwill of the largest social media actors (Google, Facebook) whose owners declare their commitment to democratic values. But Chinese and Russian social media platforms (WeChat, Vk.com, Ok.ru) are on the rise; mergers and acquisitions can also lead to changes in the ownership and user policies of social media platforms. Even though Mark Zuckerberg diligently appeared before the US and EU parliamentary bodies, recent revelations show that Facebook likewise did not refrain from using disinformation and manipulation as marketing devices.¹⁴

Algorithmic design. In contrast to traditional mass media, which conveys primarily content created by professional journalists, entertainers or politicians, social media facilitates the participation of **masses of individual citizens**. While theoretically this could fulfil the dream of an ideal state of public discourse, it has been found that the ‘marketplace of ideas’ is distorted by small aspects of software: algorithms and bots. These give more prominence to certain content and less to others – as well as selecting which content is offered to which users. The spontaneously posted views of individuals cannot compete with the industrialised tailoring and dissemination techniques. On the positive side, these enable small start-up companies, NGOs and individuals to ‘boost’ their posts with a small amount of money, and to utilise the demographic targeting offered by Facebook.

Dependence on personal data. Social media is in a position to be able to collect an excessive amount of **personal data**. The user data is utilised to perfect the algorithms used to personalise the newsfeed based on personality traits and history, in order to maximise user attention so that the time spent on the platform grows.¹⁵ For advertisers, this is a great revolution: they can get to know their potential customers and offer personalised advertising to all of them, thereby attracting even more customers. From the perspective of social media platforms, users’ personal data is their asset; however, even users make use of one another’s personal data, when they surf the platform and view other users’ activity.

Ownership concentration. Social media is significantly more concentrated than traditional media. It has more users, more revenues and owns bigger stakes of the market.¹⁶ Facebook

¹³ Note that the Anglo-Saxon type of media aims to be objective (Hallin-Mancini), even though this is usually unsuccessful. Mediterranean types of media outlets openly confess and represent their political inclinations.

¹⁴ “Facebook policy chief admits hiring PR firm to attack George Soros”, *The Guardian*, 22 Nov. 2018, <https://www.theguardian.com/technology/2018/nov/21/facebook-admits-definers-pr-george-soros-critics-sandberg-zuckerberg>.

¹⁵ The average daily time spent on social media was 116 minutes a day in Oct. 2018 (www.brandwatch.com).

¹⁶ See the numbers at: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.

had 2.234 billion users in 2018, Instagram, at 6th place, had 1 billion. The time spent on social media is comparable to television: 40 minutes daily on YouTube, plus 35 minutes on Facebook on average.¹⁷

Even though some of the social media companies are behemoth, it is unrealistic to expect that several competing social media companies provide parallel services in the same user segment, because their main value is exactly the size of their accessible social network – unless the interoperability of parallel platforms is ensured. The competing social media companies – Twitter, Pinterest, Snapchat and LinkedIn – offer slightly different services. Also, they attract various age groups: Facebook is most popular with the older generation, while the younger generation prefers Instagram (also owned by Facebook, Inc.) and Snapchat (owned by Alphabet, the parent company of Google and YouTube). A majority of users are registered with several platforms and regularly use several different ones.¹⁸ Research suggests that this has positive effects on the public discourse.¹⁹

The huge social impact and the level of concentration may raise the idea of imposing public service obligations on giant companies, such as diversity, 'must carry' rules and the obligation to conclude a service contract without discrimination. Following a more beaten track, fusion control by a rigorous competition authority could be considered to confront large company families (Facebook–Instagram or Google–YouTube–Snapchat).²⁰

3.2 Similarities of social media and traditional mass media

Despite the substantive differences, some **similarities** may be noted between social media and traditional mass media that can justify regulatory intervention.

- 1) Television and radio were regulated more strictly than the printed press partly because of their "pervasive effect".²¹ The early internet was regarded as a medium that induces more conscious consumption, called "pull", as opposed to the "push" type of television.²² Nevertheless, streaming video and especially the handheld devices have radically changed

¹⁷ Although television still takes the lead, this is largely caused by a demographic fact: older people watch significantly more television compared with youngsters, who spend more time on social media platforms. See the statistics at <https://www.nielsen.com/us/en/insights/news/2016/television-is-still-top-brass-but-viewing-differences-vary-with-age.html>. See also: "How Much Time Do People Spend on Social Media?" [Infographic], 2017 <https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic>.

¹⁸ "Social Media Use in 2018", <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>.

¹⁹ "Social media usage that involves participation in several networks reduces mass political polarization and echo chambers", see at: <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf>, p. 27.

²⁰ "66 Facebook acquisitions – the complete list 2018", <https://www.techwyse.com/blog/infographics/facebook-acquisitions-the-complete-list-infographic/>.

²¹ *Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726 (1978).

²² *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002); L. Lessig, "What Things Regulate Speech: CDA 2.0 vs. Filtering", https://cyber.harvard.edu/works/lessig/what_things.pdf. See also: "Two eras of the internet: pull and push", 21.12.2014, <http://cdixon.org/2014/12/21/two-eras-of-the-internet-pull-and-push/>.

the way – and the level of consciousness – in which their content is consumed. The objective of the content selection algorithms is to make the service **addictive** and maximise user-engagement time.²³ Today's social media encounters can be intrusive – especially the related ads – and addictive for users, which justifies protection of the individuals.

- 2) Social media has a **significant social impact** also at the level of societies. While the cause and effect of individual events cannot be proven scientifically, reference to the Arab Spring revolutions as the "Facebook revolution" by academics,²⁴ and the repeated compromises of personal data by Facebook are signs of this. Actions of disinformation and manipulation have been proven²⁵ and their impact on democracy – although not scientifically proven – can be a cause for concern.

Cause and effect have been very much contested in media effect theory as well.²⁶ The correlation between violent audiovisual content and harm for youth is still debated, but this has not prevented legislators globally from restricting such content on mass media.

- 3) Social media platforms are also a **vehicle for free expression** and public discourse. It could be examined whether having an online profile is an element of the right to free expression. If a social media platform as dominant as Facebook denied registration for a user without a justified reason, that would substantially limit the user's possibility to get his or her ideas across to the audience. It should be considered whether dominant social media platforms have a duty to provide their services to customers without discrimination.

²³ European Data Protection Supervisor (EDPS), Opinion on online manipulation and personal data, 3/2018, p. 13, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

²⁴ See for example: M. Ben Moussa, "From Arab Street to Social Movements: Re-theorizing Collective Action and the Role of Social Media in the Arab Spring", *Westminster Papers in Communication and Culture*, Vol. 9, No. 2, 2013, pp. 47-68, (2), 47, <https://doi.org/10.16997/wpcc.166>; S. Harlow, "It was a 'Facebook revolution': Exploring the meme-like spread of narratives during the Egyptian protests", *Revista de Comunicación*, 12 (2013), pp. 59–82; or A. Bruns, T. Highfield & J. Burgess, "The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their Networks", *American Behavioral Scientist*, Vol. 57, No. 7, 2013, pp. 871–898, <https://doi.org/10.1177/0002764213479374>.

²⁵ S. Bradshaw and P.N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation", Online Supplement to Working Paper 2018.1, Computational Propaganda Project, Oxford Internet Institute, 2018, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct_appendix.pdf; S. Bradshaw and P. Howard, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation", Working paper no. 2017.12, University of Oxford, 2017, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>; E. Brattberg and T. Maurer, "Russian Election Interference – Europe's Counter to Fake News and Cyber Attacks", Carnegie Endowment for International Peace, Washington, 2018; I. Brodnig, "7 types of misinformation in the German election", 2 November 2017, <https://firstdraftnews.org/7-types-german-election/>.

²⁶ See the contesting theories of Harold Lasswell (bullet, 1927), Paul Lazarsfeld (two-step influence, 1948), Joseph Klapper (selective perception, 1949), George Gerbner (cultivation, 1969), McCombs and Shaw (agenda-setting, 1972), Herman and Chomsky (framing, 1988), Dayan and Katz (performative effect, 1992) – to name a few.

The listed similarities can provide a basis for imposing certain restrictions and obligations on social media platforms.

4. Existing legal regulation of social media platforms

4.1 The responsibility structure of the e-Commerce Directive

The question of liability for third-party content emerged already in the 1990s, especially in the UK and the US. In the *Godfrey v Demon* internet case, the internet service provider refused to remove the allegedly defamatory statement (the case ended finally with a settlement).²⁷ After a series of legislative and judicial developments in the US, the EU drafted the e-Commerce Directive,²⁸ which set out a clear structure of liability for the transmitted content. The Directive aimed at liberalising online commercial activity, but also at "constitut[ing] the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information". According to this, those hosting third-party content are not liable as long as they have no actual knowledge about its illegal nature, and when they obtain such knowledge, they act expeditiously to remove or to disable access to the information (the notice-and-takedown regime). The service providers are not obliged to monitor content that they transmit and search for signs of illegal activity (Article 15).

Just after the e-Commerce Directive was passed in 2000, technological innovation changed the internet's potential so immensely that it was dubbed 'Web2.0'. Since about 2003, this has enabled lay individuals to publish content through user-friendly platforms, which has become the default mode of communication on today's internet. This technology is used in hundreds of other services: Über, eBay, Airbnb, Tinder, blogmotors, etc. These services all aggregate and classify information, making it possible for customers to get to the service directly, without a human agent.²⁹ Another layer of service providers has central operators who actively select and edit the content provided. Amazon, Booking.com and eBay differ from each other like *The Sun Online* differs from Facebook, in that the latter has no central editor, while the former does.

No generally agreed term has been crystallised yet to name the latter type of service provider:³⁰ they are sometimes called platform providers, intermediary service providers or "internet

²⁷ *Godfrey v Demon Internet Service* [2001] QB 201.

²⁸ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

²⁹ N. Helberger, J. Pierson and T. Poell, "Governing online platforms: From contested to cooperative responsibility", *The Information Society*, Vol. 34, No. 1, 2018, pp. 1–14, <https://doi.org/10.1080/01972243.2017.1391913>.

³⁰ The European Council Decision (March 2018) called them "social networks and digital platforms", another instrument "hosting services that allow[s] the upload of third party content", adding that "such providers of information society services include social media platforms". See the Proposal for a Regulation on preventing the dissemination of terrorist content online.

intermediaries",³¹ and a subgroup of them are called "video-sharing platform provider[s]" by the 2018 Audiovisual Media Services Directive (AVMS) Directive, although the Commission appears to have developed the term "online platforms",³² as in "those online platforms"³³ and "online platforms that distribute content".³⁴ This paper uses the wording 'platform providers' to designate **those services that convey third-party content with value added services, of which 'social media' is a subcategory.**

The e-Commerce Directive's narrow definition is not capable of including these platform providers, because Article 14(1) applies only to the storage of information, with the condition that "this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of **nor control** over the information which is transmitted or stored" (recital 42).³⁵

The Directive also empowers member states (recital 48) to require service providers that host information provided by users to apply duties of care in order to detect and prevent certain types of illegal activities. Thus, for example, the GNDG can rely on this empowerment. On another note, creating a diverse regulatory environment within the EU would counter the purpose of the Directive and the interests of the EU not only as a market, but also as a Union of democratic societies.

In sum, the e-Commerce Directive envisages that service providers should be liable for cooperating and applying duties of care to prevent certain types of illegal activities, but excludes that they should be directly liable for content which they transmit or store. Still, the wording of the Directive excludes direct applicability to platform providers, which emerged a few years after its creation.

4.2 The German Network Enforcement Act

Germany has introduced a controversial new law aimed at the enforcement of German criminal content restrictions on social media platforms.³⁶ The GNDG is based on the notice-and-takedown system: upon notice, the service provider is obliged to remove the content. The law orders the removal of content that appears to be contrary to certain sections and subsections of the German Criminal Code (listed in the GNDG). The law's subjects are those social media platforms that have at least 2 million registered users within Germany. A new element of the GNDG is to introduce strict rules for the notice system, including a transparent procedure to handle user complaints, short deadlines, reporting obligations and considerable fines. Content

³¹ Council of Europe Committee of Experts on Internet Intermediaries.

³² https://ec.europa.eu/digital-single-market/en/glossary#Online_Platforms.

³³ Commission Recommendation on measures to effectively tackle illegal content online.

³⁴ Communication from the Commission on tackling online disinformation.

³⁵ See also: C-324/09 *L'Oréal and others v eBay*, judgment of 12 July 2011.

³⁶ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, <https://germanlawarchive.iuscomp.org/?p=1245>.

found to be "manifestly illegal" should be removed within 24 hours, and within 7 days in other cases. The fines for not complying with the mentioned obligations are considered relatively high: up to €50 million, depending on which obligation was violated.

The significance of the GNDG has been the introduction of very short deadlines for the removal of notified content, the threat of meaningful fines, the prescription of transparency and the demand to report data for the assessment of its operation.

The GNDG can be criticised for 'outsourcing censorship': the state seemingly gets relieved of the cost of dealing with illegal content – but this takes a toll on freedom of expression. Private companies cannot ensure the same safeguards for fundamental rights as independent courts. The notice-and-takedown procedure urges platforms to err on the side of caution to avoid high fines. The contributor of ambiguous content has no options for defending his or her post and preventing removal – this could be exploited for political or other motivations.

The day after the GNDG came into effect (in January 2018), anti-migrant hate speech posted by the far-right AfD (Alternative für Deutschland)³⁷ was removed from Facebook, stirring the first controversy. The satirical newspaper *Titanic* posted a parody of the AfD post in which it used the same contested word (*Barbarenhorden*) and its account was temporarily suspended. This is a clear signal that the GNDG's operation is not without ambiguity.³⁸ Even despite the reporting obligation, little is known about what types of content are reported, what is removed and how exactly the decisions are taken. A further reason for criticism is that GNDG enforcement is supervised by the German Federal Office of Justice, which directly reports to the minister of justice, whereas the rule of law would be satisfied by supervision that is independent from the government.

The majority of criticism affecting the GNDG is that of the *notice-and-takedown* system (see below in detail). This procedure, which is now the dominant instrument against illegal content, can be regarded as moderately chilling, as it puts a burden on intermediaries and on content providers – with the winners being those who send the notice. Research has identified recent cases of **malevolent** notice-and-takedown practices, in order **to suppress legitimate voices** online. Both human-operated and automated accounts have been used to **falsely mass-report** legitimate content or users in Armenia, China, Ecuador and Russia.³⁹ The noticed content or accounts are temporarily suspended, even if the platform provider eventually reinstates them.

It should also be noted that users of platform services encounter material almost exclusively of their online friends, and they always have the option to **silence a feed that they do not like**.

³⁷ F. Pergande, "Ein Gesetz gegen die AfD?", *Frankfurter Allgemeine Zeitung*, 8.1.2018, <http://www.faz.net/aktuell/politik/inland/netzdg-ein-gesetz-gegen-die-afd-15378459.html>.

³⁸ "Bundesregierung will NetzDG überprüfen", *Zeit Online*, 8.1.2018, <http://www.zeit.de/digital/internet/2018-01/netzwerkdurchsuchungsgesetz-bundesregierung-soziale-netzwerke-berichte>.

³⁹ S. Bradshaw and P.N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation", Computational Propaganda Project, University of Oxford, 2018, p. 12.

4.2.1 *The notice-and-notice system vs notice-and-takedown*

The notice-and-takedown system pressures service providers to judge whether content is lawful or not.⁴⁰ This carries the threat of over-censorship, and fails to provide the constitutional safeguards of free expression. In addition, it is regularly abused by malicious noticers seeking to have their competitors' content removed or suspended.⁴¹

A system that pays more respect to the freedom of speech is already applied in the UK's Defamation Act 2013 Section 5, and in the Copyright Modernization Act, or Bill C-86 of Canada.⁴² Under the so-called **notice-and-notice regime**, the service provider should forward the notice to the actual content provider, if that is possible (or otherwise, remove the content). This system encourages users, who are the real providers of the questionable content, to bear responsibility for their own content and to settle their disputes individually. In Canada, even this regime was quickly exploited by alleged copyright holders, who pressured users into paying a small sum as a settlement, until legislative amendment excluded this possibility.⁴³

The UK Defamation Act 2013 took note of the uncontrollable volume of online user-generated content, acknowledging that it leads to a higher threshold needed for triggering the judicial system. It recognised that the provider should not be expected to decide on the illegal nature of the content, and therefore introduced a well-designed procedure to facilitate dialogue between the content provider and the complainant.⁴⁴

4.3 Case law of the CJEU and ECtHR on the responsibility of intermediary service providers

4.3.1 *L'Oréal v eBay*

In *L'Oréal v eBay*,⁴⁵ the Court of Justice of the European Union (CJEU) found that eBay, referred to as an "intermediary service provider", was not entitled to rely on the exemption from liability provided by Article 14 of the Directive, because its activity was not confined to technical and automated processing of the data relating to the offers that it stored, but it played an active role – providing the customer with assistance consisting in particular of optimising the

⁴⁰ See, e.g. the German Network Enforcement Act.

⁴¹ This can have substantial influence in the last days of an election campaign. See also: J. Bayer, "Liability of Internet Service Providers for Third Party Content – A comparative analysis with policy recommendations", *VUW Law Report Special Edition*, Wellington, New Zealand, 2007, pp. 1-109.

⁴² See <https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca02920.html>.

⁴³ See more in "Canadian Government Banning Settlement Demands in Copyright Notice-and-Notice System", 30 Oct. 2018, <http://www.michaelgeist.ca/2018/10/noticesystemfix/>.

⁴⁴ See a detailed explanation in: P. Bárd and J. Bayer, "A comparative analysis of media freedom and pluralism in the EU Member States", Study for the LIBE Committee, PE 571.376 EN, 2016, <http://www.europarl.europa.eu/supporting-analyses>.

⁴⁵ C-324/09 *L'Oréal and others v eBay*, judgment of 12 July 2011.

presentation of the offers or promoting them. It further declared that it is for the national courts to carry out this assessment.

The argumentation of the Court is not conclusive enough to draw conclusions on whether or not intermediary service providers could in theory be subject to the e-Commerce Directive.⁴⁶ Although the Court was silent on this issue, through *argumentum a contrario* we may conclude that eBay would not be subject to the Directive.

4.3.2 *Delfi v Estonia and MTE & Index v Hungary*⁴⁷

The Estonian online news portal *Delfi* was fined by the national courts for third-party comments, even though it removed them after notice, but the national courts found that Articles 12-14 of the Directive did not apply to *Delfi*. In Hungary, a civil organisation and a news portal were fined for third-party content. In both cases, the European Court of Human Rights (ECtHR) made its decision based on the presumption that the applicants were liable for third-party comments.

Notably, eBay, *Delfi*, *MTE* and *Index* all believed that they could avail themselves of the exemption provided in Articles 14-15 of the e-Commerce Directive, and regarded the questionable content as third-party content for which they bore no liability. The ECtHR did not address the issue of foreseeability⁴⁸ or the attribution of liability.⁴⁹ In fact, the applicants should have invoked the e-Commerce Directive instead of the European Convention on Human Rights as their main claim was that the content was not attributable to them, rather than claiming their right to freedom of expression.

These cases signal a considerable level of insecurity in the legal interpretation of the roles and responsibilities of online service providers for third-party content.

⁴⁶ It did not consider the question that providing assistance to the customer was an automated service offered to any customer, and that it did not entail that the "operator" (yet another term used) received actual knowledge about the items to be promoted or offered for sale. Instead, it referred the decision to the national courts, adding that the national measures should not require an operator of an online marketplace to monitor the goods offered for sale through its platform – but it did not base this opinion on Article 15 of the Directive, which explicitly declares that no such monitoring should be required.

⁴⁷ *Delfi v Estonia* (App 64569/09) ECtHR 2015 and *MTE and Index v Hungary* (App 22947/13) ECtHR 2016.

⁴⁸ Which should have affected the question of "being prescribed by a (foreseeable) law" in the ECtHR judgment. But ECtHR accepted without hesitation that the restriction was foreseeably laid down in law.

⁴⁹ In *Delfi*, the content in question was racial hate speech, and in *MTE and Index* it was insult against a legal person. These conditions played a decisive role in the outcome of the judgments. Further, *Delfi* was profit-oriented, and *MTE* was a non-profit organisation (however, *Index* is also profit-oriented). In the *Delfi* case, the content represented hate speech, and the commenting section brought revenues to the portal, so the Court found that the moderate fine did not violate Article 10. In the *MTE and Index* case, the content itself did not go beyond justified criticism, and at least *MTE* was a non-profit portal of public interest issues.

4.4 The principle of immunity for third-party content

The Council of Europe's Recommendation (2018) on the roles and responsibilities of internet intermediaries held that "States should ensure, in law and in practice, that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store" but they should be "co-responsible, if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature",⁵⁰ also adding that "State authorities should not directly or indirectly impose a general obligation on intermediaries to monitor content".⁵¹ The Recommendation uses the term "internet intermediaries", but from the context it is clear that it focuses mainly on 'platform providers'.

The Council of Europe's "Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms)"⁵² also declared that **states should not impose a general obligation on internet intermediaries to use automated techniques to monitor** information that they transmit, store or give access to.⁵³

The recently passed amendment to the AVMS Directive clarifies that video-sharing platform providers can enjoy the exemptions from liability defined in the mentioned chapters, with reference to the e-Commerce Directive's Articles 12–15.⁵⁴ Also the proposed e-Privacy Regulation includes this text.⁵⁵ These are promising signs, but they do **not clarify the situation** of platform providers, including those social media platforms that are not subject to the AVMS Directive. By now, the situation has matured sufficiently enough to give such platform providers **a place in the legal system**. Their responsibilities should relate to **their actual activities**: the design and usage of algorithms, their handling of personal data, the maintenance of a safe and transparent environment, their conveying activity between advertisers and users, and the amplification of certain content to the detriment of other.

⁵⁰ Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries (adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies) at 1.3.7.

⁵¹ Ibid at 1.3.5.

⁵² "Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications", Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET), <https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10>.

⁵³ Ibid., Recommendation no. 6, p. 46.

⁵⁴ In recital (48), Article 28(a)(5) and (b)(1)

⁵⁵ Article 2: "This Regulation shall be without prejudice to the application of Directive 2000/31/EC1, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive", <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0324+0+DOC+PDF+V0//EN>.

4.5 The limits of self-regulation

The Communication from the Commission on tackling online disinformation encouraged the establishment of the Code of Practice on Disinformation, which came into being in September 2018.⁵⁶ The reflections of the Sounding Board on the Code of Practice signal that the platform providers did not leave their comfort zone when drafting their rules, claiming that the so-called Code "contains no common approach, no clear and meaningful commitments, no measurable objectives or KPIs, hence no possibility to monitor process, and no compliance or enforcement tool: it is by no means self-regulation, and therefore the Platforms, despite their efforts, have not delivered a Code of Practice".⁵⁷ Indeed, the Code of Practice contains very cautious language to make "reasonable efforts" (not even best effort!) towards disclosing "issue-based advertising" and to improve the situation in fields such as the identification of automated bots or the impermissible use of automated systems (points 4, 5 and 6). There are a few clear commitments regarding the differentiation of advertisements from editorial content, which is already a basic principle in most jurisdictions (point 2). The evaluation of the steps taken by the stakeholders by 31 December points out the achievements and even more tasks to be done in the future.⁵⁸

The Code of Conduct on Countering Illegal Hate Speech online⁵⁹ has been evaluated four times since 2016. While steady growth is observed in the ratio of removing reported materials, the reports do not reveal the aspects of decisions taken by the platform. A third of the notices do not receive feedback.⁶⁰

5. Conclusions

Social media exercises a well-reasoned role on the effectuation of citizens' democratic participation in the public discourse. The framework that it offers impacts on how its users share and exchange information. The indirect impact on democratic processes has a potential to debase the rule of law.

Social media does not fit into any of the classical concepts on media actors in the content distribution chain: it does not provide content, but it does more than automatically transmit information. In a few features social media platforms are **comparable** with traditional mass

⁵⁶ Communication from the Commission on tackling online disinformation: A European Approach, Brussels, 26.4.2018 COM(2018) 236 final, p. 7; Code of Practice on Disinformation, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

⁵⁷ The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice, 24 September 2018, <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>.

⁵⁸ https://ec.europa.eu/commission/news/code-practice-against-disinformation-2019-jan-29_en.

⁵⁹

https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf.

⁶⁰ Results of Commission's last round of monitoring of the Code of Conduct against online hate speech, 19.1.2018, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086.

media companies: (i) they have a significant **impact** on individuals (can become addictive) and on society's public discourse; (ii) they serve as a vehicle for **free expression and democratic public discourse**; and (iii) both are profit-oriented, and not likely to respect public interest goals unless they are forced to by law. In several other features they are **distinct**: (i) social media platforms are not editors or publishers (in the legal sense) of content; (ii) rather than defining an editorial line they amplify and **personalise** the content stream through algorithms, which rely on masses of **personal data**; (iii) they have no entrance barriers and **do not separate public from private** communication; and (iv) their market is more **concentrated** than that of media companies.

Social media companies belong in the larger category of platform providers, which has become the dominant online structure of organising activities and is expected to further proliferate in future. Many of these platforms generate unexpected challenges in the affected economic sectors, even beyond the media sector. However, the media scene has outstanding significance because of its effect on society's public discourse.

Consensus appears to have developed in holding social media platforms not responsible for third-party content (as long as they have no actual knowledge) and not obliging them to monitor. But, it is argued, this immunity should be balanced by their diligent administering of the platform's communication environment, including the identification of advertisements and the protection of users' personal data. Platforms must ensure that their environment is trustworthy and safe for every citizen. Content selection algorithms should follow transparent principles, empower users, and prioritise diversity and trustworthiness.

Platforms – these meaningful business actors from eBay to Facebook – should be explicitly defined and their obligations regulated at the EU level.

6. Recommendations

Some of the recommended changes require **amendments of existing laws** to extend their scope on social media platforms. Others call for **a new regulation**, which would lay down basic rights and obligations for platform providers in general, with respect to a new service that is expected to proliferate in future (think of eBay, Über, Airbnb, Tinder, etc.), with safeguards for the protection of consumers and human rights.

The recommendations do not suggest self-regulation: in this area, platform providers have done as much as they can within their market constraints by their terms of services and privacy policies. At this stage of technological and social change, the protection of human rights and democratic public discourse calls for legislative intervention. Because of the international nature of the services, the regulation should take place at the supranational level of the EU and extension of the rules to the global community should be sought. Similar to the GDPR, any rules should extend to foreign service providers as well, with the purpose of effectively protecting all persons within the EU.

The suggestions below are divided under three subtitles: establishing a definition is the basic condition of any further regulation. The other regulatory recommendations are distinguished by whether they can be interpreted in the context of existing media regulation or require a new approach towards platform providers.

6.1 Definition of platform providers

The e-Commerce Directive should be amended with the inclusion of a definition for the new layer of actors, platform providers, being those that provide a platform for third parties to share their content and to carry out various communicative actions. Their immunity for content should be defined in a similar way as that for hosting providers, but instead of solely having the notice-and-takedown procedure, the notice-and-notice procedure should also be enabled (see above). Reference to their responsibilities for attending to their platform and complying with other obligations as regards data protection, etc., may be included. The e-Commerce Directive should serve as a background law for other more specific laws – the GDPR and e-Privacy Regulation – and open the door for inclusion in the AVMS Directive with the given definition.

Platform providers are neither authors nor publishers, but they could be made responsible for the activity that they actually perform: facilitation, dissemination, profiling (or not), managing accounts and cooperating with authorities. Social media is a subcategory within platform providers, and its role and position should also be defined within the media chain.

Suggestions:

- Create a new legal category for platform providers.
- Define their obligation for content through the notice-and-notice procedure.
- Make reference to their other obligations as regards data protection and other laws.

Recommended action: Amend the e-Commerce Directive with a new definition of platform providers.

Responsible actors: EU institutions.

Drawbacks:

- i) The notice-and-notice procedure may not provide the required speed in all cases; therefore, it might be kept as an option. For ‘manifestly’ illegal cases the notice-and-takedown procedure may still be acceptable – especially if safeguards for the protection of freedom of expression are added.

- ii) The new category should be flexible, as the number of platform providers is likely to grow in the future with the advent of the sharing economy. Some platform providers have more central operative control, others have less.

6.2 Recommendations in the realm of media regulation – Classical principles applied to social media

6.2.1 Diversity, pluralism and impartiality

Diversity and pluralism are related in media theory, both leading to the same goal: that citizens can encounter a variety of content from many different aspects. This can be approached from the perspective of ownership as well as the geographical, genre and political diversity of content.⁶¹ While the internet age provides for ubiquity of content, the scarcity of human attention and the technological possibilities of content selection result in less diversity than before (the filter bubble). This does not have to be so: content selection can be tailored according to the will of whoever designs and operates the algorithms. The demand side of diversity relates to how much a user is exposed to various types of content (exposure diversity) – which depends largely on the user and can be improved with increasing awareness and media literacy.

Content selection algorithms should prioritise diversity and trustworthiness, and allow users options regarding their preferences – as is already done by some providers, for example in the privacy settings. Users should be able to choose the level of the required diversity on a slider.⁶²

Concentration of ownership is an issue of concern regarding social media enterprises, especially those most general ones like Facebook and YouTube, which practically do not have competitive alternatives.

Given the nature of the service, users would benefit from alternative services of the same kind only if **interoperability** is ensured, i.e. if connections and communication is enabled between the platforms. If this is not the case, then the incumbent's position should entail specific obligations similar to 'common carriers' or to the regulation of public broadcasters within Europe:⁶³ to ensure diversity, to give preference to high-quality, reliable sources (which are attested by fact-checkers, credibility indices) and public service content, to ensure impartiality,

⁶¹ See more in: P. Bárd and J. Bayer, "A comparative analysis of media freedom and pluralism in the EU Member States", Study for the LIBE Committee, PE 571.376 EN, 2016, <http://www.europarl.europa.eu/supporting-analyses>.

⁶² N. Helberger, K. Karppinen & L. D'Acunto, "Exposure diversity as a design principle for recommender systems", *Information, Communication & Society*, Vol. 21, No. 2, 2018, pp. 191–207, <https://doi.org/10.1080/1369118X.2016.1271900>.

⁶³ See also: R. Caplan and D. Boyd, "Who Controls the Public Sphere in an Era of Algorithms? Mediation, Automation, Power", 5.13.2016, https://datasociety.net/pubs/ap/MediationAutomationPower_2016.pdf, p. 5.

and to respect higher levels of privacy standards, the transparency of algorithms and flexibility of settings for the convenience of users.

Facilitating public discussion is a great responsibility – platform providers have an ethical obligation to transmit users' messages without discrimination (impartiality). While it is accepted that media companies represent content selected according to their political agendas, this would not be accepted from social media platforms. Yet, currently there is no legal obligation to be impartial or prohibition on using algorithms for the promotion of a certain public issue.

On the other hand, niche platform services could exist legitimately (such as Catholic platforms or LGBT dating platforms) provided that they transparently admit it.

Expecting viewpoint diversity is connected to the obligation of impartiality. Above a certain size of the network, both obligations would be highly recommended.

Suggestions:

Algorithms

- Impartiality should be obligatory – platform providers must not apply viewpoint discrimination in their algorithmic structuring of content.
- Content selection algorithms need to include the principle of diversity (offering different views).
- Platforms must inform their users about the content selection principles of their algorithms.
- Users should have options on which principles they would like to use or reject, after receiving easily accessible information, using tools as simple as icons.
- One option should be to prioritise content that is found trustworthy by independent news organisations.
- Changes and experiments with new algorithms must be transparent, and provide easily accessible information to the users.

Concentration of ownership

- Fusion control should be exercised to prevent further concentration.
- The obligation of interoperability must be prescribed in order to promote the emergence of competitors.
- In the case of dominant market power, special public service obligations should be defined for social media platforms.

Recommended actions: Create a specific legal instrument to define the responsibilities of all platform providers, and among them social media providers. The options of appointing an existing competent authority (such as telecommunication and media authorities) or creating a new competent authority should be examined.⁶⁴

Extending the AVMS Directive's scope to include platform providers is considered unsatisfactory for the following reasons:

- i) Only a few provisions of the AVMS Directive would be applicable to social media providers.
- ii) Social media providers are not audiovisual media providers. They share more common features with other platform providers, such as eBay, Tinder and search engines, than with audiovisual media providers. It would be more beneficial to create a **wider** regulation that applies to all platforms. Optionally, the Audiovisual Media Services Directive could open up its scope to include platform providers as it did with YouTube. However, YouTube – although a platform provider – transmits audiovisual content and this somewhat justifies its inclusion.

Responsible actors: EU institutions should draft the recommended rules in consultation with technological experts.

Proposed subject of the obligation: Platform providers.

Drawbacks: Social media companies' freedom to provide services would be moderately restrained by this.

Arguments against the drawbacks: The measurements are necessary in the interest of the principle of pluralism and to ensure a diverse public discourse, for the protection of democratic society.

6.2.2 *Identification of advertisements, notably political advertisements*

Platform providers should be responsible for clearly identifying advertisements and sponsored content as such (the principle of identification). This principle is horizontally applied in advertising regulations, including the AVMS Directive. Social media platforms halt and approve all paid content before putting the advertisement into effect. As opposed to voluntary content, advertisements (including boosted posts) that ensure a revenue stream for the social media platform are moderated and supervised by the platform provider, which **has a higher level of responsibility for them compared with voluntary content**.

Identification of **political advertising and public issue advertising** should also be obligatory. At the same time, platform providers are able to label such content only if their publisher is explicit

⁶⁴ See also the ongoing research project: <https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building>.

about the payment factor and the subject matter of the content. But politicians and political parties can currently use social media on equal terms with private individuals and professional media companies that voluntarily publish politically motivated content as a legitimate exercise of their freedom of expression. Political parties and professional politicians should be regarded as ‘**influencers**’ in respect of political content, which is not independent information even if it is not sponsored. Anonymous accounts hinder the transparency of such influence (see below).

There are fine lines between political advertisements and political jokes, opinion articles, emotional tweets or symbolic political speech, which are understandable only in the local context. **Therefore, labelling political content based on its topic would pose a risk to freedom of expression. Political speech – whether sponsored or voluntary – forms a key part of the free public discourse, but it may be subject to restrictions.**⁶⁵ Informing users about the sources of political content when it comes from committed actors, such as politicians and political organisations, should be a basic requirement.

Using micro-targeting and artificial dissemination methods for political advertising can change the turnout of an election, simply by encouraging certain people to vote and not others.⁶⁶ Artificial dissemination techniques give unfair advantage to the candidate with more financial resources, and therefore their use should be limited.

The recommended principle should be horizontally applicable to all advertisements and not only in the media.

Suggestions:

- All advertisements, including political advertisements, should be clearly distinguishable from voluntary content.
- Amendment is needed of member states' regulation of political and public issue advertising, along with an EU directive for harmonisation and EU-level regulation.
- Existing rules on political and public issue advertising are to be extended to any publication method, with special regard to online media, including social media.
- All procurers of political and issue-based advertisements should be clearly and publicly identifiable by default; if ads are purchased on behalf of third parties, these should also be clearly and publicly identified.
- The obligation to ensure this shall be imposed on the advertisers and on the platform provider as a secondary liability.

⁶⁵ *Animal Defenders International v the United Kingdom*, 48876/08, judgment of 22.4.2013.

⁶⁶ J. Zittrain, “*Engineering an Election*” (June 20, 2014), Harvard Law Review Forum, Vol. 127, 2014, p. 335; Harvard Public Law Working Paper No. 14-28, available at SSRN: <https://ssrn.com/abstract=2457502>.

- Member states should make the necessary amendments to political and public issue advertising so that their safeguarding principles apply also to platform providers. Besides member states' regulation, **EU-level regulation (a directive) is recommended**, with particular relevance to the European Parliament elections.

Recommended action: Either a new piece of legislation for platform providers in general (so that the rules apply to all platform providers and not only to social media) or an amendment of an existing law that regulates advertising is recommended.

Responsible actors: EU institutions and member states. Because of the transborder nature of social media, and the growing interdependence of political and public issues, this problem can be better solved at the supranational level.

Proposed subject of the obligation: Platform providers. Accountability to a competent authority (consumer protection or telecommunication authority) is recommended.

Drawbacks: The labelling of political advertising might induce platform providers to control politically loaded speech that is voluntarily shared by interested citizens. This could have a chilling effect on political communication.

6.3 New, internet-specific regulatory principles

6.3.1 Administering platforms

Part of the chaos in the public discourse arises from the undistinguished mixture of various sources like commercial, political and civil actors, sometimes with multiple accounts, pseudo-accounts, fake accounts or artificial intelligence. Users have the right to know the **source of the information** – especially if it affects public discourse or their legal interests (such as advertisements).

The lines between user content and sponsored content are getting blurred, as not all persuasion comes in the form of paid advertisement, from product placement to influencers. The word 'influencer' is used here with reference to political parties, active politicians, governments and public authorities, NGOs and communication agencies, as well as the new brand of influencers themselves – an expression similar to 'public figure', but its scope is wider and more adapt to the current media environment. People who have a considerable influence on public matters have long been regarded as **public figures**, who have to tolerate a higher level of scrutiny from society.⁶⁷ In the big pond of social media, these 'big fish' should be identified and their identity verified, to minimise attempts to mislead or manipulate users. The aim is to shift the current power relations in which private users are transparent and influencers can

⁶⁷ *Verlagsgruppe News GmbH v Austria* (no. 2) – [10520/02](#), judgment of 14.12.2006.

remain opaque. While anonymity is highly treasured, it allows circumvention of the identification of advertisements.

Commercial platform providers, such as eBay, require identification from their users, differentiate between occasionally active private sellers and professional users, and provide for user feedback on trustworthiness. Even though users utilise pseudonyms, the platform is regarded as a safe environment because users' authenticity is verified. The largest social media platform providers also require verification through an email address or actual postal address and/or mobile text message, and offer the option to create a page for professional users. Theoretically, users could have two or three profiles relating to their different social roles, although currently Facebook allows only one profile per user.

The suggested verification scheme should also specify the safeguards for the protection of personal data. It should ideally distinguish at least three categories: (i) natural persons who act in their private capacities; (ii) natural or legal persons who act in their professional capacities; and (iii) those professional users whose activity is related to public issues, affecting the fundamental rights of individuals (political parties, medical service providers). Ideally, natural persons in their private capacity should not be subject to any verification; however, that would keep a back door open to fake accounts. Therefore, a low level of verification, for example through the eIDAS system,⁶⁸ is recommended as a minimum, and the level of verification should grow from the least to the greatest scrutiny.

Virtual models and virtual politicians⁶⁹ are already among the users of social media: Lil Miquela, a fictitious model, has 1.5 million followers on Instagram, with her colleagues Bermudaisbae and blawko22 trying to catch up. These fascinating technological innovations can be useful (like chatbots), but their usage should not violate human dignity, which requires that bots do not mislead humans regarding their nature, and the principle of fair public discourse also demands that bots do not distort the marketplace of ideas.⁷⁰ A regulative approach could range from simply identifying artificial intelligence as such, to its complete prohibition.

Suggestions:

- Platforms should ensure – by technological means of supervision or verification – that the accounts are registered by human individuals rather than artificial intelligence or bots. Deleting fake accounts should not be regarded as a virtue but as an obligation.

⁶⁸ Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73–114, <http://data.europa.eu/eli/reg/2014/910/oj>.

⁶⁹ “Meet the world’s first virtual politician”, 15 Dec. 2017, <https://www.victoria.ac.nz/news/2017/12/meet-the-worlds-first-virtual-politician>.

⁷⁰ Already envisaged in: European Group on Ethics in Science and New Technologies, “Artificial Intelligence, Robotics and ‘Autonomous’ Systems”, March 2018, http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

- Bots, virtual personalities and trolls should be identified as such.
- Influencers⁷¹ on public issues and in commercial promotion should be identified as such, through a combination of self-identification, a reporting mechanism and monitoring based on the number of followers.
- Users who regularly reach large audiences with public issue content should be regarded as ‘influencers’ (political parties, NGOs, communication agencies and other influencers) and should have a higher level of scrutiny (e.g. verification of the identity).

Recommended action: New rules on the responsibilities of platform providers need to be created. This type of activity did not exist in the traditional media age.

Responsible actors: EU institutions should draft this new rule in consultation with technological experts.

The main objective of the recommended law is to maintain and protect the rule of law, democracy and human rights, through the maintenance of a public discourse that is inevitable for them.

Proposed subject of the obligation: Platform providers. Accountability to a supervisory authority is recommended, for example, telecommunication authorities.

Drawbacks: This recommendation is likely to attract controversy, because of its threat to privacy. The supervision and verification may exercise a chilling effect on users and influencers, particularly on those who represent minority views or are unfavoured by the ruling government, especially in illiberal states.

Arguments against the drawbacks:

- The threat lurks in insufficient or lack of data protection and not in the identification of the user category. The e-Privacy Regulation is expected to provide additional protection for personal data.
- Public figures have been exposed to a higher level of public scrutiny and responsibility. This principle is adapted in the compulsory verification of influencers as such.
- The current technology of some social media companies does not provide effective data security even for the personal data that are hidden according to the users' intention. In addition, autocratic states are inclined to apply secret surveillance against their political opposition in any case, and therefore the profile verification would not be the tipping point.

⁷¹ The word ‘influencer’ is used here with reference to political parties, active politicians, governments and public authorities, NGOs, communication agencies and the new brand of influencers themselves.

Benefits:

- Users would have information about the source of content.
- Influencers who possess better tools to represent their views are distinguished from natural persons who act in their private capacities.
- Differentiating between user categories has a lesser chilling effect on free speech than differentiating on the basis of content.

6.3.2 *Protecting privacy and personal data*

Users' personal data and profiles are utilised to target them with tailored content, in order to maximise their engagement time, but also to manipulate their opinions. This violates users' right to privacy, right to protection of personal data and right to receive information.

The protection of personal data is the most decisive factor in whether future technologies will serve or exploit people and societies. Social media acquires extreme measures of personal data about its users, including sensitive data. The GDPR requires that these are collected with a clear affirmative act establishing a "freely given, specific, informed and unambiguous indication" of the data subject's agreement (recital 32). Furthermore, consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (recital 42). These requirements are not always satisfied: users' options do not always appropriately allow free choice, or clear and concise information. Additionally, users are overwhelmed by consent requests, which results in "consent fatigue".⁷²

Social media activity – liking and sharing – also leaves valuable traces of personal data, which is harvested and processed by advertisers without users being informed or able to opt out.

Industry actors' urge to utilise personal data as the fuel and the currency of social media and advertising business is understandable, but **not justified**. Other professions like doctors, lawyers and investment brokers also deal with masses of sensitive personal information, and they must refrain from monetising these in their own interests – they are obliged to do so by law.⁷³ The attitude towards personal data processing needs to change: ownership of personal data by the data subject should be recognised, and companies that are trusted with the processing of such personal data must treat them confidentially.

The GDPR allows the processing of personal data for direct marketing purposes on an opt-out basis, but the possibility to opt out should be "explicitly brought to the attention of the data subject and presented clearly and separately from any other information" (recital 70).

⁷² See *noyb.eu*, "GDPR: *noyb.eu* filed four complaints over 'forced consent' against Google, Instagram, WhatsApp and Facebook", 25 May 2018, https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

⁷³ J. Zittrain, "Engineering an Election" (June 20, 2014), Harvard Law Review Forum, Vol. 127, 2014, p. 335; Harvard Public Law Working Paper No. 14-28, available at SSRN: <https://ssrn.com/abstract=2457502>, at 340.

Micro-targeting for political advertising has in some cases been based on sensitive information, like "racial or ethnic origin, political opinions, religious or philosophical beliefs" (Article 9), which should not be used for micro-targeting, or only under specific conditions (recital 71) that are not defined in the GDPR. It needs to be clarified – perhaps through the e-Privacy Regulation – that micro-targeting based on sensitive information can take place solely on an opt-in basis. Recital 56 of the GDPR creates a privilege for political parties but only on condition that adequate safeguards are established – and these safeguards have not been worked out yet. Natural persons can avail themselves of the 'household exception' during social networking or online activity if the data processing does not relate to any professional or commercial activity, which emphasises the need for a distinction between private and professional accounts.

In sum, much remains to do to ensure compliance with the GDPR and with the hopefully even more effective e-Privacy Regulation in the future.

Legal responsibility for the lawful processing of personal data may be shared by the platform provider and the user/marketer.⁷⁴

Suggestions:

- **The proposed e-Privacy Regulation should include**
 - explicit reference to 'platform providers' and define social media as a subcategory of them;
 - the prescription that users opt in for targeted advertising;
 - the right of users to get more information about which of their data are used for content selection or micro-targeting, and have the right to exclude some personal data from this process; and
 - the need for users to consent through their own browser settings once, which is applicable to all websites. Also, interpretation of the GDPR allows this, and it could be clarified through guidelines.
- The GDPR's implementation has to be meticulously enforced with special attention to social media platforms, making it clear and unambiguous that
 - sensitive personal data should not be processed for the purposes of profiling and targeting, or only on an opt-in basis; and
 - adequate safeguards for invoking the political privilege should be worked out.

⁷⁴ Case C210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*.

- Platform providers' legal liability for protecting the personal data of their users must be clarified and include
 - prevention of hacking and data leaks;
 - monitoring and prevention of illegal activity that violates the protection of personal data on their platforms; and
 - information for users about which of their data are used for content selection or micro-targeting, and an offer to exclude some personal data from this process.

Recommended actions:

- i) **Include in the e-Privacy Directive reference to 'platform providers' and 'social media'.**
- ii) Supervise implementation of the GDPR, providing interpretations and guidelines, and sanctioning if appropriate. Test cases such as *Brave v Google* deserve special attention as the decision can bring substantial changes to the legal practice.⁷⁵
- iii) **Clarify legal responsibility for personal data by (a) guidelines and (b) the amendment of legislation**, and (c) in the event that a specific legal instrument is set out to delineate the responsibilities of platform providers, it should contain these obligations.

Responsible actors: European Commission, European Data Protection Supervisor and the European Data Protection Board.

Proposed subject of the obligation: Platform providers.

Drawbacks: No meaningful drawbacks were identified, aside from restraining the freedom to provide services.

Argument against the drawbacks: Protection of personal data is a key factor in ensuring a user-friendly environment for technological innovations. In future, the new services and instruments, such as the Internet of Things, virtual realities and artificial intelligence, should be developed with these strong data protection requirements already in mind.

⁷⁵ <https://www.reuters.com/article/us-europe-privacy-complaint/mozilla-co-founders-brave-files-adtech-complaint-against-google-idUSKCN1LS2JL>.

Engage II Fellowship Programme

The ENGAGE II Fellowship Programme is coordinated by CEPS with support by the Open Society Initiative for Europe (OSIFE). This one-year programme aims to involve academic, civil society and think tank actors from Central and Eastern Europe, the Western Balkans and Eastern Partnership countries in EU policy debates. It entails training, study visits, public events and the publication of policy papers. It culminates in the active participation of the selected fellows at the annual CEPS Ideas Lab.

The ENGAGE II Fellowship focuses on the significance of the rule of law in different policy domains, including rights and security, foreign and economic affairs.

The programme is coordinated by the CEPS Justice and Home Affairs (JHA) Unit. It is conducted under the supervision of CEPS Senior Research Fellows Sergio Carrera (Head of the JHA Unit), Cinzia Alcidi (Head of the Economic Policy Unit) and Steven Blockmans (Head of the Foreign Policy Unit).

For the period 2018–19, six highly-qualified Fellowship members were selected:

- Denis Cenuşa, Researcher at the Institute for Political Science and PhD candidate at the Justus-Liebig University in Giessen, and Associated Expert at Expert-Grup, Chisinau
- Judit Bayer, Professor of Media Law and International Law at the Budapest Business School
- Simonida Kacarska, Director and co-founder of the European Policy Institute, Skopje
- Naim Rashiti, Executive Director and Senior Balkan Analyst, Balkans Policy Research Group, Pristina
- Maria Repko, Deputy Director at the Centre for Economic Strategy, Kiev
- Berat Thaqi, Policy Analyst at the GAP Institute, Pristina





ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)