Araştırma Makalesi/Research Article **Doi: 10.47136/asbuhfd.916253**

THE DISRUPTIVE DEVELOPMENT of COMMUNICATION TECHNOLOGIES: IS WEB 2.0 a REASSURANCE FOR or a THREAT to the CORE PRINCIPLES of DEMOCRATIC VALUES in RESPECT of HUMAN RIGHTS LAWS?

İletişim Teknolojilerinin Yıkıcı Gelişimi: Web 2.0, İnsan Hakları Kanunları ile ilgili Demokratik Değerlerin Temel İlkeleri için bir Güvence mi yoksa Tehdit mi?

Bilge Kaan GÜNER*

[*] Research Fellow, Research Chair on the Law of Artificial Intelligence Universität Tübingen, Juristische Fakultät, e-mail: bilge.guener@uni-tuebingen.de
Orcid: 0000-0001-6792-2817.

Makale Gönderim Tarihi/Received: 15.04.2021.

Makale Kabul Tarihi/Accepted: 10.07.2021.

Atıf/Citation: Güner, Bilge Kaan. "The Disruptive Development of Communication Technologies: Is Web 2.0 a Reassurance for or a Threat to the Core Principles of Democratic Values in Respect of Human Rights Laws?" *ASBÜ Hukuk Fakültesi Dergisi* 3, no. 2 (2021): 501-527.

Abstract

Data is flying around us and there is a constant flow. Data traffic, based on a predictable and controllable system, is promising with its contributions to many areas of life and the solutions it offers to social problems. With the growth of technology, the internet continues to facilitate communication channels that are an integral part of our lives. The widespread applications of algorithms using artificial intelligence (AI) and the gradual increase in the use of 'Internet of Things' (IoT) technologies are stunning examples of how the internet has become a ubiquitous part of everyday life and how it permeates our lives.

While the extensive use of digital platforms benefits human rights, facilitating greater diversity of voices, greater access to information, and stronger social movements than ever before, there is also an increase in the abuse of society by malicious actors. Political microtargeting campaigns, mass spread of disinformation, foreign intervention in elections, and polarized 'echo chambers' during election periods, cyber techniques used directly or indirectly by such actors or institutions, we are subjected to destructive information bombardment. Therefore, within the framework of international human rights, there is a need for new local or international legislation to guide digital technology. However, due to the complexity of the problem, a multidimensional approach is needed to deal with cyber techniques that threaten democracy. Finding adequate solutions to disruptive cyber techniques is directly linked to maximizing accountability in the context of digital technology.

The purpose of this article is; It is an overview of why regulations that will solve this problem are vital while addressing the current and possible consequences of the algorithmic accountability problem in digital platforms created by governments and various institutions. In light of these, the first part of this article will attempt to explain current cyber techniques and how digital platforms facilitate their use. Then, the adequacy of current approaches to the disruptive aspects of technology will be examined within the scope of relevant human rights laws. Finally, the article will be concluded with a multidimensional approach to ensure internet freedom and protect democracy and rights.

Keywords: Accountability, Democracy, Disinformation, Micro-targeting, Human Rights.

Öz

Veriler etrafımızdan uçuşup gidiyor ve sürekli bir akış var. Öngörülebilir ve denetlenebilir sisteme oturtulmuş veri trafiği hayatın birçok alanına katkısı ile toplumsal problemlere sunduğu çözümler noktasında meydana gelen gelişmeler umut vaat ediyor. Teknolojinin büyümesiyle internet, hayatımızın ayrılmaz bir parçası olan iletişim kanallarını da kolaylaştırmaya devam ediyor. Yapay zekâ (AI) kullanan algoritmaların yaygın uygulamaları ve 'Nesnelerin İnterneti' (IoT) teknolojilerinin kullanımındaki kademeli artışlar, internetin günlük yaşamın nasıl her yerde bulunan bir parçası haline geldiğinin ve hayatımıza ne denli nüfuz ettiğinin çarpıcı örnekleridir.

Dijital platformların yoğun kullanımı insan haklarına fayda sağlarken, daha fazla ses çeşitliliğini, bilgiye daha fazla erişimi ve her zamankinden daha güçlü sosyal hareketleri kolaylaştırırken, kötü niyetli aktörler tarafından toplumun istismar edilmesi noktasında da aynı oranda artış yaşanmaktadır. Siyasi mikro hedefleme kampanyaları, dezenformasyonun kitlesel yayılımı, seçimlere dış müdahale ve seçim dönemlerinde kutuplaşmış 'yankı odaları', bu tür aktörler veya kurumlar tarafından doğrudan ya da dolaylı olarak kullanılan siber tekniklerle yıkıcı bilgi bombardımanı altında kalmaktayız. Bu nedenle, uluslararası insan hakları çerçevesinde, dijital teknolojiye rehberlik edecek yeni yerel veya uluslararası mevzuata ihtiyaç duyulmaktadır. Bununla birlikte, sorunun karmaşıklığı nedeniyle demokrasiyi tehdit eden siber tekniklerle başa çıkmak için çok boyutlu bir yaklaşıma ihtiyaç vardır. Yıkıcı siber tekniklere yeterli çözümler bulunması, dijital teknoloji bağlamında hesap verilebilirliğin azami düzeye çıkarılması ile doğrudan bağlantılıdır.

Bu makalenin amacı; hükümetlerin ve çeşitli kurumların yarattığı dijital platformlardaki algoritmik hesap verilebilirlik probleminin mevcut ve olası sonuçlarına değinirken bu probleme çözüm getirecek regülasyonların neden hayati olduğuna genel bir bakıştır. Bunların ışığında, bu makalenin ilk kısmı mevcut siber teknikleri ve dijital platformların kullanımlarını nasıl kolaylaştırdığını açıklamaya çalışacaktır. Ardından, ilgili insan hakları yasaları kapsamında, teknolojinin yıkıcı yönlerine karşı mevcut yaklaşımların yeterliliği irdelenecektir. Son olarak, internet özgürlüğünü sağlamak, demokrasi ve hakları korumak için çok boyutlu bir yaklaşımla makale noktalanacaktır.

Anahtar Kelimeler: Hesap Verilebilirlik, Demokrasi, Dezenformasyon, Mikro Hedefleme, İnsan Hakları.

INTRODUCTION

The internet, through the exponential growth of technology, continues to facilitate communication channels, which are an integral part of our lives, being unprecedentedly convenient and easy to use when compared to earlier communication media such as the telegraph, radio and telephone. To cite specifics, promising implementations of algorithms that use artificial intelligence (AI) and gradual increases in the use of ‘Internet of Things’ (IoT) technologies are impressive examples of how the internet has become a ubiquitous part of daily life. However, mass dissemination of information through digital platforms hosting user-generated content is a more complicated context in which to assess the benefits and detriments of the internet. For example, more than 2.5 billion people were actively using Facebook as of December 2019, which is far greater than any government's influence on people.[1] The benefits of this intensive use of digital platforms are that they can easily mobilise like-minded people living in different parts of the world and allow people who demand democratic discourse to organize relatively easily, reducing the time, effort and money required to do so.[2] A salient example of the large-scale cyber rebellions in which digital technologies have been associated with social movements and democratic demands is the Arab Spring, although examples of cyber rebellion took place earlier than 2010, such as the rebellion in Estonia in 2007.[3] Although the Estonian cyber-attacks and the Arab Spring are important examples of internal turmoil, there are important differences between them: the cyber-attacks in Estonia originated from external actors and employed (relatively) conventional cyber methods rather than digital platforms.[4] Accordingly, cyber rebellions that, in the main, are not launched through digital platforms are outside the scope of this paper.

While intensive use of digital platforms has brought to benefits to human rights, facilitating a greater diversity of voices, greater access to information and stronger social movements

[1] "Facebook Reports Fourth Quarter and Full Year 2020 Results," https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx.

[2] Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven ; London: Yale University Press, 2017).

[3] Anya Schiffrin, "Disinformation and Democracy: The Internet Transformed Protest But Did Not Improve Democracy," *Journal of International Affairs* 71, no. 1 (2017): 117–26.

[4] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *7th European Conference on Information Warfare and Security 2008, ECIW 2008*, 1 January 2008, 163–68.

than ever before, it has also been exploited by malicious actors, hyper-partisans, politicians and oppressive governments to pursue power.[5] Political micro-targeting campaigns, mass dissemination of disinformation, foreign interference in elections and polarised 'echo-chambers' during election periods are disruptive cyber techniques used by such actors or institutions. In my opinion, we are not dealing with a new facet of human behaviour and the pursuit of power when we examine the rapid proliferation of use of the internet and digital platforms for such purposes, we are just looking at new ways of doing the same thing more intensely by using the internet. As such, international human rights could be applied as a general framework without the need for new (domestic or international) legislation to guide digital technology. However, by itself this general framework is inadequate to deal with cyber techniques that threaten democracy owing to the complexity of the issue. For this reason, a multi-dimensional approach is needed to tackle this problem. Otherwise, so long as adequate solutions to disruptive cyber techniques cannot be found, the positive impact of digital technology in rendering governments more accountable will remain an illusion. In view of this, the first part of this paper will attempt to describe current cyber techniques and how digital platforms facilitate their use. Then, within the scope of relevant human rights laws, the adequacy of existing approaches against disruptive aspects of technology will be examined. Finally, I conclude by suggesting a multi-dimensional approach to ensure the freedom of the internet, and protect democracy and rights.

[5] Kate Jones, *Online Disinformation and Political Discourse: Applying a Human Rights Framework*, 2019.

I. CURRENT CYBER TECHNIQUES AND THE CONTRIBUTION OF DIGITAL PLATFORMS

The widespread commercialization of the internet was a watershed moment, not only creating competitive, private network infrastructures but also exposing new business models that include online technologies.[6] One of the services that entered our lives with these new business models is digital platforms, the best known products of Web 2.0. "Surveillance" is a central aspect to this new business model between internet users and digital platforms, which depend on a symbiotic relationship.[7] Users were willing to use social networking platforms, but reluctant to pay for them, so digital platforms decided to offer their services for free, as they need to 'grow large quickly' to harness network effects effectively. Accordingly, these service providers started to implement an advertisement-based business model that aims to collect data based on users' online behaviour and to publish advertisements informed by the information obtained.[8]

A. Online Political Micro-targeting

Micro-targeting is a more sophisticated form of the advertisement-based business model. It is used by digital

[6] Barry M. Leiner et al., "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (7 October 2009): 22–31, https://doi.org/10.1145/1629607.1629613.

[7] Bruce Schneier, "News: Surveillance Is the Business Model of the Internet: Bruce Schneier - Schneier on Security," Last modified: April 10, 2021, https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html.

[8] John Naughton, "The Evolution of the Internet: From Military Experiment to General Purpose Technology," *Journal of Cyber Policy* 1, no. 1 (2 January 2016): 5–28, https://doi.org/10.1080/23738871.2016.1157619.

platforms or intermediaries and consists of three phases: 'collection of personal data' and amalgamation with correlative sources for analysing; 'classification of users' to fit within a particular profile; and sending 'individually tailored advertisements' to reach potential consumers.[9] Although computer-based techniques for collecting personal data and profiling potential voters have been used by political parties in the United Kingdom since 2004, micro-targeting has started gaining popularity as a political tool owing to its deceitful potential to prompt life-changing decisions.[10] Political micro-targeting can have many different objectives, including persuasion, encouragement or even demobilising (swing voters, in particular).[11] Political campaigns have intensified the application of micro-targeting through third-party platforms or special services of digital platforms such as Facebook's "lookalike audience". To cite specifics, the Cambridge Analytica scandal, in which a company that set itself up to work on political campaigns by applying sophisticated analysis to massive datasets without the permission of users, is a stunning example of how micro-targeting can affect elections in major democracies such as the UK and the USA.[12]

[9] Tom Dobber, Ronan Ó Fathaigh, and Frederik J. Zuiderveen Borgesius, "The Regulation of Online Political Micro-Targeting in Europe," *Internet Policy Review* 8, no. 4 (31 December 2019), https://doi.org/10.14763/2019.4.1440.

[10] Bethany Shiner, "Big Data, Small Law: How Gaps in Regulation Are Affecting Political Campaigning Methods and the Need for Fundamental Reform," *Public Law*, 28 October 2018.

[11] Dobber, Ó Fathaigh, and Zuiderveen Borgesius, "The Regulation of Online Political Micro-Targeting in Europe."

[12] Brian Tarran, "What Can We Learn from the Facebook-Cambridge Analytica Scandal?" *Significance* 15, no. 3 (June 2018): 4–5, https://doi.org/10.1111/j.1740-9713.2018.01139.x.

Although the extent to which extent micro-targeting affects election results is uncertain, as many commentators have pointed out, it poses significant risks for society and for individuals because of the way it has been implemented. These techniques breach individuals' right to privacy by accessing personal data, even sensitive personal data, without permission. Also, they use this information to confuse individuals' thoughts, emotional states and opinions and intend to affect citizens' views and opinions and thus change their voting behaviour. Personal thought needs to be protected with no exemptions, as it is considered *forum internum* for individuals. Alegre argues that two of the three basic elements of the international legal framework concerning freedom of thought have been infringed by micro-targeting activities:[13] the prohibitions on 'revealing' and 'manipulating' an individual's thoughts have been infringed by micro-targeting activities. The risks to society stem from the costs of micro-targeting vendors, which could render competition between political parties unfair, further limiting the free flow of political disclosure, aggravating inequality between well-funded parties and poor parties in reaching potential voters.[14]

B. Massive Dissemination of Disinformation

The second deceitful technique used to manipulate the free flow of online information is disinformation. Disinformation could be defined as a dissemination technique aiming to acquire an economic benefit or public harm by knowingly sharing false,

[13] Susie Alegre, "Rethinking Freedom of Thought for the 21st Century," *European Human Rights Law Review*, no. 3 (2017): 221–33.

[14] Dobber, Ó Fathaigh, and Zuiderveen Borgesius, "The Regulation of Online Political Micro-Targeting in Europe."

inconsistent or distorted information.[15] Further, the scope of disinformation goes far beyond fake news and does not include misleading interpretations of reality such as satire and parody, or illegal content such as hate speech.[16] Moreover, methods used by state and non-state actors to spread disinformation and thereby influence elections have increased exponentially and have been observed in many countries during the last five years. For example, Freedom House reports that in 2018 various disinformation techniques were employed during elections in 24 countries.[17]

In May 2018, Twitter reported that its machine learning tools had detected approximately 10 million accounts per week that appeared to be spam or automatic accounts. This figure had been just 3.2 million per week in September 2017.[18] Thus, it appears that mainstream digital platforms are major arteries for far-reaching disseminate of disinformation. In light of these striking examples, the CrossCheck Project, based on collaborative journalistic research, has sought to classify disinformation tactics by several methods.[19] First of all, current disruptive content is

[15] European Comission, "Final Report of the High Level Expert Group on Fake News and Online Disinformation," Text, 12 March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[16] European Comission, "Final Report of the High Level Expert Group on Fake News and Online Disinformation."

[17] Adrian Shahbaz and Allie Funk, "The Crisis of Social Media" (Freedom House, 2019), https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

[18] Yoel Roth and Del Harvey, "How Twitter Is Fighting Spam and Malicious Automation," 2018, https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.

[19] Sed Cubbon, "Evolving Disinformation Tactics in France: Comparing the 2017 and 2019 CrossCheck Projects," First Draft, 25 February 2020,

designed more strategically, to create "astroturfing", which is more subtle so harder to detect than former examples which doctored online content poorly.[20] 'Content recycling' is another method: an example of this is the misleading presentation of outdated television interviews by hiding the date of the original to create a perception of social unrest. 'Content laundering' through unreliable news sites, 'bots' (automated accounts) and 'trolls' is another important problem because it encourages users to innocently share distorted content.[21] 'Memes' that include inflammatory text or images are seen as a vital disinformation method, as they are simple to produce and easy to understand, but it is difficult to follow how they spread.[22] Other obtrusive disinformation methods include repurposing satirical content for divisive ends, impersonating authentic news sites and politicians, and using alternative digital platforms such as VK and 'closed' peer-to-peer distribution networks.

Disinformation techniques have been used with objectives including malicious distortions of the truth relating to delicate issues such as immigration to provoke emotional reactions and polarise society, thereby directly linked to breaches of freedom of thought. Besides, expeditious spread of disinformation about particular political actors might deter them from standing for election, and this could be seen as a detrimental effect of disinformation on the right to participate in public affairs and to vote.[23] No consensus has yet been reached on the removal of harmful content. Each digital platform states it is trying to deal with this problem in different ways. Nevertheless, a narrow interpretation should be put on what restrictions of freedom of

https://firstdraftnews.org:443/latest/evolving-disinformation-tactics-in-france-comparing-the-2017-and-2019-crosscheck-projects/.

[20] Cubbon, "Evolving Disinformation Tactics in France."

[21] Jones, *Online Disinformation and Political Discourse*.

[22] Cubbon, "Evolving Disinformation Tactics in France."

[23] Jones, *Online Disinformation and Political Discourse*.

expression and freedom of information should be permissible in order to protect individuals from disinformation, applying within the scope of measures to be taken and tailored for each specific case.

C. Foreign Interference

At the outset of the Arab Spring, many scholars such as Philip Howard were optimistic that digital technology would prove a tool to help the world to be more democratic.[24] However, no significant progress in democratic development has been made among countries where the Arab Spring occurred except Tunisia, and the consequences of the social uprising have been a devastating civil war, especially in Syria, Yemen and Libya.[25] After the Arab Spring, repressive governments started looking for counter-approaches, driven by the fear of possible cyber rebellions in their own countries that could arise from use of the internet. For example, authoritarian regimes have tried to curb the effectiveness of the internet during social unrest by shutting down foreign websites, restricting mobile phone connectivity and blocking social media platforms and apps.[26]

On the other hand, some countries that were made aware of the impact of the internet on society have started to use this as a route to intervene in other countries' domestic affairs by supporting non-state agencies. One salient example of foreign interference is the Internet Research Agency (IRA), a Russia-based establishment that has made constant cyber-attacks, first targeting Ukrainian and Russian citizens in 2014, then the 2016

[24] Schiffrin, "Disinformation And Democracy."

[25] Matthew J. Flynn, "Cyber Rebellions: The Online Struggle For Openness," *Journal of International Affairs* 71, no. 1.5 (2018): 107–14.

[26] Shahbaz and Funk, "The Crisis of Social Media."

US election and lately the Brexit process.[27] The Disinformation Report issued by New Information highlighted the extent of cyber tactics carried out by the IRA to influence the thoughts of voters in the US election, by presenting figures for the number of users of IRA's various mainstream digital platform accounts between 2014 and 2017. To quote specifics, harmful and manipulated content stemming from the IRA had been seen by 126 million Facebooks users, 20 million Instagram users and 1.4 million Twitter users.[28] Foreign interference of this kind has had similar objectives to disinformation techniques, to take advantage of societal divisions by deploying deliberately misleading content through the internet in order to take advantage of vulnerabilities in states' information ecosystem.[29]

D. Polarised Echo-chambers (Daily Me)

Nicholas Negroponte, a technologist from MIT, foresaw as early as 1995 that individuals would have their own 'the Daily Me' in future (our present).[30] The concept of Daily Me was based on the idea that news sources would be personalised to become packages communicating what people want to see.[31] With the widespread use of digital platforms, it would not be wrong to say that we have approached the Daily Me when we take into consideration that many people use these platforms as sources of the news they prefer to read. Giving priority to what people want

[27] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency," *U.S. Senate Documents*, 1 October 2019, https://digitalcommons.unl.edu/senatedocs/2.

[28] DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 30–34.

[29] DiResta et al., "The Tactics & Tropes of the Internet Research Agency," 99.

[30] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2018), https://doi.org/10.2307/j.ctv8xnhtd.

[31] Sunstein, *#Republic*, 1.

to see in their social media accounts may seem a positive development at first glance. However, the customisation of news feeds using the dedicated algorithms of digital platforms has several important problems. First of all, the business model of digital platforms is advertising-based, and the way they increase profit is by increasing the average time users spend on their sites and ensuring they interact with more ads.[32] For this reason, algorithms that regulate the news fed to digital platforms should be seen not just as an innovation that provides more freedom to its users, but also as a marketing tactic to reach out to more advertisers.[33] The announcement of Facebook's new algorithm that regulates news feeds and sorts the content into the order its users prioritise is an important example.[34] Personalisation of news feeds based on posts a user has 'shared', the pages they follow, the content they interact with the most, reveals that machine-learning tools endeavour to know a lot of things about users and thus personal attributes or emotions could easily be uncovered.[35] For this reason, this issue is directly linked to the rights to privacy and to freedom of thought.

Another important problem with the personalisation of news feeds on digital platforms is the creation of 'echo-chambers', because it brings people who think alike closer together and reduces the opportunity to be exposed to divergent perspectives.[36] The essence of pluralist democracy is the

[32] Jones, *Online Disinformation and Political Discourse*, 34.

[33] H. Akin Unver, "Digital Challenges To Democracy: Politics Of Automation, Attention, And Engagement: Politics Of Automation, Attention, And Engagement," *Journal of International Affairs* 71, no. 1 (2017): 127–46.

[34] Adam Mosseri, "Building a Better News Feed for You, About Facebook," 29 June 2016, https://about.fb.com/news/2016/06/building-a-better-news-feed-for-you/.

[35] Sunstein, *#Republic*.

[36] Unver, "Politics Of Automation, Attention, And Engagement."

protection of a heterogeneous structure that hosts a wide range of opinions. So, what happens when individuals only see news and posts in their social media accounts that are close to their own opinions, *per se*? When like-minded people only share the same perspectives, they find it difficult to understand different views, they become more polarized and susceptible to disinformation, and this leads to harmful tribalism, extremism and fragmentation in society.[37] Conversely, enabling people to access different views will allow them to fully enjoy the right to choose, which is classified among the fundamental rights under democracy.

II. ADEQUACY OF EXISTING APPROACHES AND HOW RELEVANT HUMAN RIGHTS LAWS ADDRESS THE PROBLEM

The fact that various actors expose people to cyber techniques that violate many human rights should not mean that the general framework of human rights law is inadequate. However, the core problem stems from regulatory environments seeming unable to perceive potential threats of rapidly evolving technology at the onset and not apparently providing adequate safeguards.[38] This part of this paper will evaluate approaches that comply with the Universal Declaration of Human Rights

[37] Sunstein, *#Republic*.

[38] Jones, *Online Disinformation and Political Discourse*.

(UDHR)[39] and the International Covenant on Civil and Political Rights (ICCPR).[40]

Data protection laws, in line with the right to privacy stipulated in Article 12 of the UDHR and Article 17 of the ICCPR, are the regulations states apply to prevent personal data from being unlawfully harnessed and/or extrapolated using various techniques. For example, the European Union's General Data Protection Regulation (GDPR),[41] the world's most advanced data protection regulation, contains principles governing the processing and transfer of personal data, which provide significant safeguards to the data subject wishing to control how their data is accessed, processed or shared. For this reason, unlawful use of personal data through micro-targeting could be limited by effective application of the GDPR, because political micro-targeting includes various techniques intended to reveal people's political views, which are included among the sensitive personal data under Article 9 GDPR. Since the data subject's political opinion is sensitive personal data, its processing is prohibited, unless consent to do so is explicitly given and other conditions highlighted in Article 9(2) are met. The exemption set out in Article 9(2)(d) also covers political parties, but it does not give them the right to draw inferences about their members' or former members' political views; only the right to process sensitive data in order to contact their members. The other basis under which it is lawful for political parties to process sensitive

[39] "Universal Declaration of Human Rights (1948)," Last modified: April 10, 2021, https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/UniversalDeclarationofHumanRights(1948).aspx.

[40] "United Nations Treaty Collection," Last modified: April 10, 2021, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4.

[41] General Data Protection Regulation [2016] OJ L 119/1.

personal data is with express consent, as specified in Article 9(2)(a) GDPR.

One context in which it is acceptable to draw inferences about a data subject's political views is where explicit consent is obtained from the data subject for this to be done, which is also stated as an exemption in Article 22(4) GDPR.[42] Although the GDPR sets down no clear rules governing micro-targeting, this can be seen as a type of automated decision-making mechanism, which is covered in Article 22 GDPR, since such mechanisms have important consequences for individuals.[43] However, it is uncertain whether Article 22 contains 'the Right to Explain' as a provision or as a right, which raises doubts on whether the GDPR is adequate to regulate micro-targeting.[44] Nevertheless, the GDPR contains important provisions to protect the data subject against illegal micro-targeting and inform them when it is taking place, with specific conditions such as the privacy notice that must be issued if consent is to be explicit. In addition, the UK Election Commission has recommended that the sources of online political adverts be clearly labelled so such adverts would be more intelligible, which is in line with both the transparency principle and the requirement for a privacy notice under the GDPR.[45] A similar transparency principle exists in the EU Code

[42] GDPR, Art. 22(4): *…shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies…*

[43] Normann Witzleb, Moira Paterson, and Janice Richardson, eds., *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting* (Milton Park, Abingdon, Oxon ; New York, NY: Routledge, 2020).

[44] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 2 (May 2017): 76–99, https://doi.org/10.1093/idpl/ipx005.

[45] Dobber, Fathaigh, and Borgesius, "The Regulation of Online Political Micro-Targeting in Europe."

of Practice on Disinformation, and accordingly mainstream digital platforms should explain to their users why they display targeted political advertisements.[46] In this context, some digital platforms have either restricted the promotion of paid political advertising (e.g. Google) or completely banned it (e.g. Twitter).[47]

Another crucial point in using the internet, which is an important tool for participating in political discussions and expressing opinions, is to determine the lawful scope of the freedom of expression. Article 19 UDHR and Articles 19 and 20 ICCPR are the key basis for the freedom of expression, which also includes the rights to receive and to impart information. Freedom of expression is not an absolute right and can be restricted in the cases specified in paragraph 3 of Article 19 ICCPR. However, any restriction of the freedom of speech must be provided by law and it should be necessary and proportional. In view of this, it is possible that the public order may be damaged where public debates are manipulated by providing deliberately distorted information through the internet (disinformation). Also, digital platforms' algorithms that regulate the order in which news feeds appear are likely to create echo-chambers containing like-minded people, and this fragmentation in society could aggravate intolerance of opposing views.[48] Moreover, algorithms that control the flow of news, and widespread disinformation breach the rights to receive and impart information, because these techniques

[46] EU Commission, "Code of Practice on Disinformation" (Shaping Europe's digital future - European Commission, 26 September 2018).

[47] Dobber, Fathaigh, and Borgesius, "The Regulation of Online Political Micro-Targeting in Europe."

[48] Lindsey Andersen, "Human Rights in the Age of Artificial Intelligence," Last modified: April 10, 2021, https://www.exploreaiethics.com/reports/human-rights-in-the-age-of-artificial-intelligence/.

minimise the diversity of information individuals receive on public opinion related topics.[49] Although international human rights treaties such as ICCPR bind states, companies must respect the rules set out in these agreements. If they do not, under Article 2(1) ICCPR states can take the measures necessary to prevent violations of human rights through interference by non-state actors.[50] For example, the German Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) requires social media sites to be removed within 24 hours of flagged content being reported by users.[51] However, current applications used by digital platforms to restrict or prevent dissemination of disinformation are based on 'internal policy', owing to a lack of international regulation on this issue. Besides, the standards that digital platforms use to decide whether to remove content is 'inappropriate' it differs from platform to platform, and how fair their methods are cannot be fully determined since such platforms lack transparency. This ambiguity as to digital platforms' standards could lead to inconsistent and unjust decisions regarding the appropriateness of content and may unintentionally cause breaches of the right to freedom of expression. For these reasons, there is a need for international regulation on the removal of content that amounts to disinformation, which must respect the limits of the right to freedom of expression; and regulation to require digital platforms to be more transparent about the algorithms they use.

Another right affected by cyber techniques is the individual's freedom of thought, which is stated in Article 18

[49] Jones, *Online Disinformation and Political Discourse*.

[50] Simon McCarthy-Jones, "The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century," *Frontiers in Artificial Intelligence* 2 (2019), https://doi.org/10.3389/frai.2019.00019.

[51] Andersen, "Human Rights in the Age of Artificial Intelligence."

UDHR and Article 18 ICCPR. Freedom of expression is an absolute right that is an indispensable instrument for a democratic society, so it must be stringently protected against any interference.[52] However, it is more difficult to identify the extent to which freedom of thought should be protected, as it is relatively difficult to determine the impact of technology on individuals' thoughts compared to the other rights violations stated above.[53] As Alegre argues, technological advances that have the potential to interfere with freedom of thought should be evaluated within the scope of the precautionary principle of The World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), regarding morally unacceptable harms.[54]

IV. RECOMMENDATIONS

It is an undeniable fact that the internet provides great benefit to human life in many fields. The various facilities of the internet that empower individuals to express their views freely and participate in public discourse are important tools to consolidate democratic participation. However, the malicious and surreptitious cyber techniques discussed in this paper have not only affected the benefits that many users derive from the internet but also accelerated the internet's tilting towards a threat rather than an opportunity for democracy.

This situation is a problem both for democratic countries and for citizens of more authoritarian regimes, increasing the pressures on them. For example, some repressive governments have restricted internet access and/or the sites it may access as an

[52] Alegre, "Rethinking Freedom of Thought for the 21st Century."

[53] Alegre, "Rethinking Freedom of Thought for the 21st Century."

[54] Alegre, "Rethinking Freedom of Thought for the 21st Century."

opportunity to quell dissident voices, under the guise of preventing harmful impacts of the internet on internal turmoil.[55] In other regimes, regulation has not been adequate to tackle abusive cyber techniques. In any case, the measures to be taken to protect democracy and rights should reassure users that they are protected not only against existing threats, but also future threats. For these reasons, several measures should urgently be included on the states' agenda to ensure internet freedom as part of protecting democracy, notably on digital platforms.

First of all, international human rights laws should be placed at the centre of the process of drafting any regulation of harmful interferences by cyber techniques (and related guidance) because these rights contain necessary safeguards to protect people against the power of the state.[56] However, actions to be taken against cyber interventions purely in the legal sphere will not be sufficient to deal with complicated structures of cyber technique and their immense and gigantic diffusions. Accordingly, an independent group should be established containing digital platform representatives, researchers, journalists, government officials and lawyers, similar to the high-level expert group set up by the European Commission on Disinformation, to address in detail all dimensions of harmful cyber technique.[57]

Secondly, the inadequacy of existing data protection laws to deal with micro-targeting should be addressed by determining on what basis interference with personal data should be both reasonable and lawful.[58] Also, digital platforms should be

[55] Shahbaz and Funk, "The Crisis of Social Media."

[56] Jones, *Online Disinformation and Political Discourse*.

[57] European Comission, "Final Report of the High Level Expert Group on Fake News and Online Disinformation."

[58] Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 5 October 2018), https://papers.ssrn.com/abstract=3248829.

required to provide comprehensive information (transparency) to users exposed to political paid advertising through micro-targeting, stating why these ads are shown, the source of the ads and what users should do if they wish to avoid seeing these types of ad. Digital platforms should be required to be transparent, not only in micro-targeting, but also in the standards they apply to decide whether content is inappropriate, whether to remove it, and also in the algorithms they use to regulate news feed. Independent external oversight bodies should be established, to decide whether the right to freedom of expression has been violated where content is removed by/from digital platforms, which could help encourage impartial content-related decisions by platforms. Also, digital platforms should notify all users who are unintentionally exposed to disinformation by sharing or liking content containing maliciously distorted information. For instance, Facebook's informing users who interact with fake news about coronavirus could be adapted to the broader disinformation issue.[59]

Individuals' awareness of the harmful effects of cyber techniques could be increased by including education in digital media literacy in schools, enhancing access to information control organizations such as Fact-checking projects, strengthening the diversity of free 'unbound' media and providing transparent datasets to researchers for prospective investigation of harmful cyber techniques. This awareness, together with the openness of digital media, will significantly reduce the potential of individuals to be targeted for unscrupulous interference (whether from inside or outside the home state).[60]

[59] "Coronavirus: Facebook Will Start Warning Users Who Engaged with 'harmful' Misinformation," the Guardian, 16 April 2020, http://www.theguardian.com/technology/2020/apr/16/coronavirus-facebook-misinformation-warning.

[60] Flynn, "Cyber Rebellions."

Human behaviour and the pursuit of power will always contain bad as well as good as long as humanity exists. However, recent technological developments that reveal and even manipulate people's emotions and thoughts have gone far beyond what may be justified in the pursuit of power. As a result, it is crucial to take steps not only to eliminate threats against democracy but also to prevent people from homogenisation

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek aldığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar, etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

BIBLIOGRAPHY

Alegre, Susie. "Rethinking Freedom of Thought for the 21st Century." *European Human Rights Law Review*, no. 3 (2017): 221–33.

Andersen, Lindsey. "Human Rights in the Age of Artificial Intelligence." Last modified: April 10, 2021. https://www.exploreaiethics.com/reports/human-rights-in-the-age-of-artificial-intelligence/.

The Guardian. "Coronavirus: Facebook Will Start Warning Users Who Engaged with 'harmful' Misinformation." 16 April 2020.

http://www.theguardian.com/technology/2020/apr/16/coronavirus-facebook-misinformation-warning.

Cubbon, Sed. "Evolving Disinformation Tactics in France: Comparing the 2017 and 2019 CrossCheck Projects." First Draft, 25 February 2020. https://firstdraftnews.org:443/latest/evolving-disinformation-tactics-in-france-comparing-the-2017-and-2019-crosscheck-projects/.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." U.S. Senate Documents, 1 October 2019. https://digitalcommons.unl.edu/senatedocs/2.

Dobber, Tom, Ronan Ó Fathaigh, and Frederik J. Zuiderveen Borgesius. 'The Regulation of Online Political Micro-Targeting in Europe'. Internet Policy Review 8, no. 4 (31 December 2019). https://doi.org/10.14763/2019.4.1440.

European Comission. "Final Report of the High Level Expert Group on Fake News and Online Disinformation." Text, 12 March 2018. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

"Facebook Reports Fourth Quarter and Full Year 2020 Results." https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx.

Flynn, Matthew J. "Cyber Rebellions: The Online Struggle for Openness." Journal of International Affairs 71, no. 1.5 (2018): 107–14.

General Data Protection Regulation (GDPR). "General Data Protection Regulation (GDPR) – Official Legal Text." https://gdpr-info.eu/.

Jones, Kate. Online Disinformation and Political Discourse: Applying a Human Rights Framework, 2019.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. 'A Brief History of the Internet'. ACM SIGCOMM Computer Communication Review 39, no. 5 (7 October 2009): 22–31. https://doi.org/10.1145/1629607.1629613.

McCarthy-Jones, Simon. "The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century." Frontiers in Artificial Intelligence 2 (2019). https://doi.org/10.3389/frai.2019.00019.

Mosseri, Adam. "Building a Better News Feed for You." About Facebook, 29 June 2016. https://about.fb.com/news/2016/06/building-a-better-news-feed-for-you/.

Naughton, John. "The Evolution of the Internet: From Military Experiment to General Purpose Technology." *Journal of Cyber Policy* 1, no. 1 (2 January 2016): 5–28. https://doi.org/10.1080/23738871.2016.1157619.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective." 7th European

Conference on Information Warfare and Security 2008, ECIW 2008, 1 January 2008, 163–68.

Roth, Yoel, and Del Harvey. "How Twitter Is Fighting Spam and Malicious Automation," 2018. https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.

Schiffrin, Anya. "Disinformatıon and Democracy: The Internet Transformed Protest but Did Not Improve Democracy." *Journal of International Affairs* 71, no. 1 (2017): 117–26.

Schneier, Bruce. "News: Surveillance Is the Business Model of the Internet: Bruce Schneier - Schneier on Security." https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html.

Shahbaz, Adrian, and Allie Funk. "The Crisis of Social Media." Freedom House, 2019. https://freedomhouse.org/report/freedom-net/2019/crisis-social-media.

Shiner, Bethany. "Big Data, Small Law: How Gaps in Regulation Are Affecting Political Campaigning Methods and the Need for Fundamental Reform." Public Law, 28 October 2018.

Sunstein, Cass R. "Republic: Divided Democracy in the Age of Social Media." Princeton University Press, 2018. https://doi.org/10.2307/j.ctv8xnhtd.

Tarran, Brian. "What Can We Learn from the Facebook-Cambridge Analytica Scandal?" *Significance* 15, no. 3 (June 2018): 4–5. https://doi.org/10.1111/j.1740-9713.2018.01139.x.

Tufekci, Zeynep. Twitter and Tear Gas: The Power and Fragility of Networked Protest. New Haven ; London: Yale University Press, 2017.

"United Nations Treaty Collection." https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4.

"Universal Declaration of Human Rights (1948)." https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/UniversalDeclarationofHumanRights(1948).aspx.

Unver, H. Akin. "Digital Challenges to Democracy: Politics Of Automation, Attention, and Engagement: Politics of Automation, Attention, and Engagement." *Journal of International Affairs* 71, no. 1 (2017): 127–46.

Wachter, Sandra, and Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 5 October 2018. https://papers.ssrn.com/abstract=3248829.