



# CYBERPOLITIKJOURNAL

## Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights

Volume 9, Number 17, 2024



### RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

- Revisiting Academic Writing in Digital Era: Opportunities and Ethical Dilemmas – **Nezir AKYEŞİLMEN, Małgorzata KAMOLA-CIEŚLIK and Ali Salih Hamdan HAMID**
- Personal Data Protection in Times of Health Crisis: Lessons Learned from Future Preparedness – **Alaa SAKKA and Sonny ZULHUDA**
- The Importance of Cybersecurity in Building Consumer Faith in Marketing Strategy - **Jyoti JYOTI**

### OPINIONS / YORUMLAR

- Transhümanizmin Ahlaki Açmazı - **Bilal SAMBUR**
- Sosyal Medya Ekseninde İfade Özgürlüğü – **Fatma Tuba SOYDOĞAN**

### ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

- Diplomacy in Digital Age – **Gül Nazik ÜNVER**
- Space Travel: Ten Short Lessons – **Neslihan TOPÇU**



# **CYBERPOLITIKJOURNAL**

Siber Politikalar Dergisi

---

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights

[www.cyberpolitikjournal.org](http://www.cyberpolitikjournal.org)

i

---



**ABOUT THE JOURNAL****Editor-in-Chief / Editör:** Prof. Dr. Nezir Akyeşilmen (Selçuk University)**Associate Editor / Eş-editör:** Professor Bilal Sambur (Yıldırım Beyazıt University)**Assistant Editors / Yardımcı Editörler:**

Dr. Vanessa Tinker (Cellegium Civitas) (Poland)

Assoc. Prof. Dr. Mehmet Emin Erendor (Adana Bilm ve Teknoloji Üniversitesi) (Turkey)

**Book/Article Reviews - Kitap/Makale Değerlendirme**

Özgün Özger (Association for Human Rights Education)

Adem Bozkurt (Association for Human Rights Education)

Mete Kızılkaya (Association for Human Rights Education)

**Editorial Board:**

Prof. Pardis Moslemzadeh Tehrani ( University of Malaya) ( Malaysia)

Prof. Hüseyin Bağcı (Middle East Technical University) ( Turkey)

Prof. Javid Rehman (SOAS, University of London) (UK)

Prof.Dr. İhsan D. Dağı (Middle East Technical University) ( Turkey)

Prof. Dr. Murat Çemrek(Necmettin Erbakan University)(Turkey)

Prof. Dr. Fuad Jomma ( University of Szczecin)(Poland)

Assist. Prof. Murat Tümay ( School of Law, Istanbul Medeniyet University) (Turkey)

Dr. Carla Buckley (School of Law, University of Nottingham) (UK)

Dr. Lella Nouri (College of Law and Criminology, Swansea University)(UK)

**International Advisory Board:**

Prof. Michael Freeman (University of Essex) (UK)

Prof.Dr. Ramazan Gözen (marmara University)(Turkey)

Prof. Dr. Mohd Iqbal Abdul Wahab ( International Islamic University of Malaysia)(Malaysia)

Prof. Dr. Farid Suhaib ( International Islamic University of Malaysia) ( Malaysia)

Prof Dr Sandra Thompson ( University of Houston)(USA)

Prof Mehmet Asutay ( University of Durham)(UK)



Prof.Marco Ventura(Italia)

Prof. F. Javier D. Revorio (University Lamacha Toledo)(Spain)

Prof. Andrzej Bisztyga (Katowice School of Economics)(Poland)

Prof. Marjolein van den Brink (Netherland)

### **Owner/Sahibi**

On behalf of Association for Human Rights Education / İnsan Hakları Eğitimi Derneği adına

Prof. Dr. Dr. Nezir Akyeşilmen

### **Peer Review**

All articles in this journal have undergone meticulous peer review, based on refereeing by anonymous referees. All peer review is double blind and submission is online. All submitted papers (other than book and article reviews) are peer reviewed.

### **The Journal**

The languages of the Journal are both Turkish and English.

### **ISSN 2587-1218**

*Cyberpolitik* (CP) aims to publish peer-reviewed scholarly articles and reviews as well as significant developments regarding cyber world, cybersecurity, cyberpolitics and human rights.

### **Indexing/Endeksler**

*Cyberpolitik Journal* is being indexed by;

- \* Academia Social Science Index (ASOS),
- \* Scientific Indexing Services (SIS),
- \* Eurasian Scientific Journal Index (ESJIndex),
- \* Index Copernicus International (ICI), (ICV 2017=64.65)
- \* Directory of Research Journal Indexing (DRJI).
- \* JournalITOCs.
- \* Open-Web.info.
- \* Google Scholars



**Issue Referees / Sayı Hakemleri**

Prof.Dr. Bilal Sambur

Assoc. Prof.Dr. Mehmet Emin Erendor

Assoc. Prof.Dr. Murat Tümay

Assoc. Prof.Dr. Yusuf Çınar

Assoc. Prof.Dr. Önder A. Afşar

Assistant Prof.Dr. Ayşegül Sili Kalem

Assistant Prof.Dr. Şerife nesimioğlu

Dr. Gül nazik Ünver

***Cyberpolitik consists of the following sections:***

**Research Articles:** Each Volume would publish a selection of Articles covering aspects of cyber politics and human rights with a broad universal focus.

**Comments:** This section would cover recent developments in the field of cybersecurity, cyber politics and human rights.

**Book/Article Reviews:** Each Volume aims to review books on cyber politics, cybersecurity and human rights.

**Cyberpolitik Award:** Each year one ‘*Cyberpolitik*’ prize will be awarded, for the best article from material published in the previous year.



**CONTENTS / İÇİNDEKİLER**

|  |             |
|--|-------------|
| <b>EDITORIAL PREFACE: BASICS OF THE METAVERSE</b>  | <b>vi</b>   |
| <b>EDİTORYAL ÖNSÖZ: METAVERSİN TEMELLERİ</b>   | <b>viii</b> |
| <b>RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ</b>  | <b>1</b>    |
| REVISITING ACADEMIC WRITING IN DIGITAL ERA: OPPORTUNITIES AND ETHICAL CONSIDERATIONS                   | 2           |
| <b>Nezir AKYEŞİLMEN, Małgorzata KAMOLA-CIEŚLIK and Ali Salih Hamdan HAMID</b>                          |             |
| CONTACT TRACING IN TIMES OF HEALTH CRISIS: PRIVACY AND DATA PROTECTION LESSONS FOR FUTURE PREPAREDNESS | 17          |
| <b>Ala SAKKA and Sonny ZULHUDA</b>   |             |
| THE IMPORTANCE OF CYBERSECURITY IN BUILDING CONSUMER FAITH IN MARKETING STRATEGY                       | 34          |
| <b>Jyoti JYOTI</b>   |             |
| <b>OPINIONS / YORUMLAR</b>   | <b>46</b>   |
| TRANSHÜMANİZMİN AHLAK AÇMAZI   | 47          |
| <b>Bilal SAMBUR</b>  |             |
| SOSYAL MEDYA EKSENİNDE İFADE ÖZGÜRLÜĞÜ   | 51          |
| <b>Fatma Tuba SOYDOĞAN</b>   |             |
| <b>ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ</b>   | <b>76</b>   |
| DIPLOMACY IN THE DIGITAL AGE   | 77          |
| <b>Gül Nazik ÜNVER</b>   |             |
| SPACE TRAVEL: TEN SHORT LESSONS  | 81          |
| <b>Neslihan TOPÇU</b>  |             |
| <b>NOTES FOR AUTHORS / YAZARLAR İÇİN NOTLAR</b>  | <b>84</b>   |



## EDITORIAL PREFACE: ETHICS OF DIGITAL DOMAIN

Dear Readers,

We are proud to present to you the 17th issue of the *Cyberpolitik Journal*. It is a great honor for all of us to continue our journey that we started eight years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this domain within our limitations.

In an era dominated by the omnipresence of technology and interconnected digital ecosystems, the role of digital citizenship education cannot be overstated. The articles featured in the volume 9th and 17th issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from ethical considerations for academic writing brought about by generative AI to Data protection and from ethical dilemma of Transhumanism to the freedom of expression in social media.

In recent decades, the rapid evolution of digital technology has fundamentally transformed the way we live, work, and communicate. As the digital domain continues to expand, it brings with it a myriad of opportunities that promise to enhance our global connectedness, increase access to information, and democratize knowledge. However, alongside these benefits, the digital age also presents significant ethical dilemmas that challenge our moral frameworks and societal norms. As the contributors to this issue of *Cyberpolitik Journal* explore, the ethics of the digital domain are multifaceted and require careful consideration from scholars, policymakers, and practitioners alike.<sup>1</sup>

### **The Confluence of Opportunities and Ethical Dilemmas in Academic Writing**

The article "Revisiting Academic Writing in Digital Era: Opportunities and Ethical Dilemmas" by Nezir Akyesilmen, Małgorzata Kamola-Cieślak, and Ali Salih Hamdan Hamid

---

<sup>1</sup> This editorial preface has been predominantly produced by AI, especially ChatGPT.



sets the tone for this issue by examining how digital tools have reshaped academic writing. On the one hand, the digital era has revolutionized the dissemination of knowledge, making it easier for scholars to access a wealth of information and collaborate across borders. Online platforms, digital libraries, and academic networking sites have democratized access to research and fostered a more inclusive academic community.

Yet, these advancements are not without ethical challenges. The authors delve into concerns such as plagiarism, data privacy, and the pressure to publish in an increasingly competitive environment. The ease of accessing and reproducing information online has made it more difficult to ensure the integrity of academic work, raising questions about the authenticity and originality of digital publications. Moreover, the digital era has also blurred the lines between formal and informal writing, challenging traditional notions of authorship and intellectual property. As academic writing continues to evolve in this digital age, the need for robust ethical guidelines and a commitment to academic integrity has never been more critical.

### **Protecting Personal Data in the Digital Health Landscape**

Alaa Sakka and Sonny Zuhuda's article, "Personal Data Protection in Times of Health Crisis: Lessons Learned from Future Preparedness," brings to light the critical issue of data privacy in the context of health crises, such as the COVID-19 pandemic. The pandemic has underscored the importance of digital technology in managing public health, with contact tracing apps, telemedicine, and digital health records playing pivotal roles in containing the spread of the virus.

However, the authors raise important ethical questions about the collection, storage, and use of personal health data. While digital tools have proven invaluable in managing the pandemic, they have also exposed vulnerabilities in data protection. The mass collection of personal data, often without informed consent, has sparked concerns about surveillance, data breaches, and the potential misuse of sensitive information. Sakka and Zuhuda argue that as we prepare for future health crises, it is imperative to strike a balance between public health needs and the protection of individual privacy. This requires not only robust data protection laws but also a commitment to ethical principles that prioritize the rights and dignity of individuals.





### **Building Trust through Cybersecurity in Marketing**

In "The Importance of Cybersecurity in Building Consumer Faith in Marketing Strategy," Jyoti Jyoti explores the implications of cybersecurity in the digital marketplace. As businesses increasingly rely on digital platforms to reach consumers, cybersecurity has become a critical component of marketing strategy. Consumers are more aware than ever of the risks associated with sharing their personal information online, and their trust in a brand is closely linked to the company's ability to protect their data.

The author highlights the responsibility of businesses to safeguard consumer data and the potential consequences of failing to do so. Data breaches not only harm individuals but also erode public trust in digital commerce, undermining the very foundation of the digital economy. Jyoti argues that cybersecurity should be seen not merely as a technical issue but as a social imperative that is central to building and maintaining consumer trust. By prioritizing cybersecurity, businesses can foster a safer digital environment and contribute to the long-term sustainability of the digital marketplace.

### **The Ethical Quandaries of Transhumanism**

The opinion piece "Transhümanizmin Ahlaki Açmazı" by Bilal Sambur delves into the ethical dilemmas posed by transhumanism, a movement that advocates for the use of technology to enhance human capabilities and transcend biological limitations. Transhumanism raises profound ethical questions about the nature of humanity, the limits of technological intervention, and the potential for unintended consequences.

Sambur argues that while the pursuit of human enhancement offers exciting possibilities, it also poses significant moral challenges. The potential to radically alter human nature through genetic engineering, cybernetic enhancements, and artificial intelligence raises questions about identity, equality, and the ethical use of technology. There is a risk that such advancements could exacerbate social inequalities, creating a divide between those who have access to enhancement technologies and those who do not. Furthermore, the quest for perfection and immortality, central to transhumanist ideals, challenges traditional ethical frameworks and forces us to reconsider what it means to live a good life.



## Free Speech and Social Media: Navigating Ethical Boundaries

In "Sosyal Medya Ekseninde İfade Özgürlüğü," Fatma Tuba Soydoğan addresses the ethical challenges of free speech in the age of social media. Social media platforms have become the primary venues for public discourse, allowing individuals to express their opinions and engage with others on a global scale. However, the rise of social media has also led to the proliferation of hate speech, misinformation, and cyberbullying, raising concerns about the ethical limits of free expression.

Soydoğan explores the tension between protecting free speech and ensuring that social media platforms do not become breeding grounds for harmful content. The author argues that while free speech is a fundamental right, it is not absolute and must be balanced with the responsibility to prevent harm. This requires not only the enforcement of legal restrictions on harmful content but also the development of ethical guidelines that promote respectful and constructive online discourse. The challenge lies in finding a balance that protects individual freedoms while safeguarding the collective well-being of society.

## Digital Diplomacy and Space Exploration

The final section of this issue features article and book reviews that reflect on the dimensions of digital diplomacy and space exploration. In her review of "Diplomacy in Digital Age," Gül Nazik Ünver examines how digital technologies are reshaping diplomatic practices that arise from this transformation. Digital diplomacy offers new opportunities for international engagement and collaboration, but it also raises questions about transparency, accountability, and the potential for digital divides to exacerbate global inequalities.

Similarly, Neslihan Topçu's review of "Space Travel: Ten Short Lessons" explores the implications of space exploration in the digital age. As humanity ventures beyond Earth, of space travel—such as the exploitation of extraterrestrial resources, the militarization of space, and the impact of space exploration on our understanding of humanity—become increasingly important.

## Conclusion: Charting an Ethical Path Forward

As we reflect on the diverse contributions to this issue of *Cyberpolitik Journal*, it is clear that the ethical challenges of the digital domain are as complex as they are urgent. The digital era



offers unprecedented opportunities for innovation, collaboration, and progress, but it also demands a renewed commitment to ethical principles that prioritize the well-being of individuals and societies. As scholars, practitioners, and citizens, we must work together to navigate the ethical complexities of the digital age, ensuring that the technologies we create and use serve the greater good and respect the dignity of all.

This issue invites readers to engage with the ethical questions raised by digital transformation and to consider how we can build a more just and equitable digital future. The articles, opinions, and reviews presented here offer valuable insights into the ethical dilemmas of our time and provide a foundation for ongoing discussion and action in the ever-evolving digital domain.

Nezir AKYEŞİLMEN, Ph.D

Editor-in-Chief

x



**RESEARCH ARTICLES / ARAŐTIRMA MAKALELERİ**

1



## REVISITING ACADEMIC WRITING IN DIGITAL ERA: OPPORTUNITIES AND ETHICAL CONSIDERATIONS

**Nezir AKYEŞİLMEN\***  
ORCID ID: 0000-0001-8184-5280

**Małgorzata KAMOLA-CIEŚLIK\*\***  
ORCID ID: 0003-2956-3969

**Ali Salih Hamdan HAMID\*\*\***  
ORCID ID: 0003-4373-8171

### *Abstract*

Digital transformation has led to significant changes in research, publishing, teaching, and learning processes in academia. Although it provides numerous benefits, it has also brought about serious threats in many aspects, especially in academic ethics. This article focuses on the answer to the question of how academic ethics are affected in the transformation process of academic writing? For this purpose, the research will primarily benefit from literature review, content analysis, data analysis, and document analysis as the research methodology. All academia stakeholders need to actively participate in discussions about ethical considerations and implement practices that support integrity in the rapidly evolving digitally enriched environment. Some findings of the research are one, digitalization in academic writing has brought about new ethical considerations and dilemmas and second, the perception of ethical usage of AI tools among scholars is quite weak.

**Key words:** digital transformation, ethics, academic writing, transparency, cooperation, Artificial Intelligence(AI).

### **Introduction**

---

\* Prof. Dr., Department of International Relations, Selçuk University- Konya – Türkiye ; Research Fellow at the University of Szczecin – Szczecin, Poland. E-mail: [nezmen@yahoo.com](mailto:nezmen@yahoo.com).

\*\* Assist. Prof. Dr., Institute of Security and Political Sciences -the University of Szczecin – Szczecin, Poland. E-mail: [malgorzata.kamola-cieslik@usz.edu.pl](mailto:malgorzata.kamola-cieslik@usz.edu.pl)

\*\*\* Dr., Faculty of Humanities -the University of Zakho -Kurdistan Region - Iraq. E-mail: [ali.hamdan@uoz.edu.krd](mailto:ali.hamdan@uoz.edu.krd)



The process of digital transformation has had a profound impact on all aspects of life during the past two decades. Digitalization has forced business, society, and education, along with other sectors, to change, particularly with the COVID-19 pandemic of 2020. Different concepts such as digitalization, digitization, or digital transformation, despite some concerns, are interchangeably used in literature (Farias-Gaytani, 2023:1; Mikalef and Parmiggiani, 2022:1). The proliferation of internet access and the growing number of individuals utilizing mobile phones, social media, and other information and communication technology (ICT) services have fundamentally transformed the manner in which people engage, communicate, acquire knowledge, and engage in professional activities across nearly all nations (Sauseni, 2020:4).

Digital transformation encompasses the utilization of digital technologies to revolutionize different elements of our lives, such as our habits, professional approaches, manufacturing techniques, written correspondence, social connections, entertainment, and engagement with the surrounding environment. Mikalef and Parmiggiani define digital transformation “as a process that encompasses significant changes through the introduction of information and communications technologies (ICTs)(2022:2). Digitalization facilitates the mechanization of processes and procedures, enables rapid and cheap communication, offers data and tools for analysis, enhances the user experience through customized and interactive digital interfaces, generates novel business models, and revolutionizes emerging technologies such as artificial intelligence, IoT, blockchain, and cloud computing. In short, digitalization is profoundly altering all facets of human existence. The transformation is also evident in academia and academic publications.

Not only writing technology, but also educational technologies, and in particular online learning, have created new contexts for learning that offer various opportunities for writers to exchange papers, give feedback to each other, construct knowledge, and acknowledge the writings of others. Writing and learning technologies have melded into a large field that includes learning, writing, communication, publication, presentation, and research. Perhaps one of the most exciting developments of recent years has been the potential for collaboration afforded by more and more technologies within the writing landscape. Not only can tools within the digital writing ecosystem be used to capture valuable dimensions of the academic writing (and writing-to-learn) process, but other multi-modal digital technologies also now offer valid alternative options to achieve a successful academic writing process without



producing written text. In particular, the proliferation of digital image, audio, and video capture and editing tools in recent years has put the production of multimodal artifacts of learning well within reach of learners of all ages across a range of contexts. While access to these tools may still be more restricted than those required for writing, with the ubiquity of the smartphone, this may become more widely distributed across populations. With the exponential growth in the ability to create, edit, and share multimodal content, the long-dominant position of the written word may well be in jeopardy (Devitt, Benetos, and Kruse, 423–431).

Academic digital transformation involves incorporating digital technologies into educational institutions to enhance teaching, training, learning, and administrative processes. This transformation has numerous impacts in academia in its entirety. The listed features encompass online education, variety of interactive learning tools, participation, accountability, inclusiveness, accessibility, efficiency, online libraries, digital database, digital libraries, cooperation etc. It also promote cooperation among education stakeholders and researchers while minimizing education cost. Digital transformation in education struggle to equip learners and educators with the required tools, skills and competences, promotes a more inclusive, innovative setting, cooperation among all education stakeholders and promotes digital citizenship education(Council of Europe, 2019:10–11).

The benefits of digital transformation in academia are evident, but it also carries substantial adverse repercussions. The considerations in question encompass challenges arising from unstable internet, cybersecurity, online communication, excessive dependence on technology, limited social interaction, troubles with focus, difficulties in controlling and supervising instructors, the digital gap, disparities in digital literacy (Kulish, 2023:94–95), the quality of written content, and ethical dilemmas.

The article aims to provide insights into the changing character of academic research and writing in the digital age by analyzing both the positive and negative outcomes. Having a wholistic approach would help researchers in understanding the challenges and successfully benefitting the opportunities brought about by digital change. There has been an abundant academic research on the effects of digitalization on academia, but very little on the specific topic of academic writing. Therefore, this work aims to provide a detailed analysis and contribute to filling the existing gap in the literature. As a method of research it fundamentally



benefits from literature review, data analysis, content analysis, and document analysis. Furthermore, this essay seeks to offer an understanding of the evolving nature of academic research and writing in the digital era by examining the positive and negative consequences that have emerged due to technological advancements.

### **Does Digitalization Transforms Academic Writing?**

Before the development of computers and the internet, researchers would send their papers by traditional mail, facing difficulties in formatting and editing. In the 1990s, researchers began integrating digitization into their professional lives with the development of specialist software and web-based services. These services are based on aspects such as human exertion, perceived significance, usefulness, utilization, and behavioral inclination (Brunetti et al., 2022:1137). The process of digitalization has both positive and negative impacts on academic writing. One of the numerous beneficial impacts it offers is the facilitation and enhancement of information accessibility. Electronic journals, digital libraries, online databases, freely accessible resources, and generative AI. Enhancing writing resources, applications, and tools; optimizing plagiarism detection programs; expediting research and publication procedures; and improving their efficiency through online platforms. These are the conveniences and opportunities offered by cybertechnology in academic writing. Good writing is culturally valued and highly esteemed, especially in certain academic subjects; therefore, it bears extra weight. Word processors, grammar and style checkers, connectivity, and now generational AI tools are all parts of the digitization process that are having a significant impact on writing. However, these changes are more subtle and less obvious than they once were, making them difficult to identify (Zhao, Cox, and Cai, 2024:2). It is important to see the educational effects of generative AI technologies like ChatGPT and Gemini through the lens of the eventual digitization of written language. The digitization of writing represents a significant change in writing as an essential means of communication and education.

Furthermore, the adverse consequences of digitalization on academic writing are significantly more substantial and have catastrophic implications. The primary concern in this context revolves around the discussions regarding the decline in quality. In the past, significant amounts of time were dedicated to researching articles in libraries with the aim of obtaining useful information and utilizing it to its fullest potential. Today, we have the privilege of rapidly accessing numerous resources on the computer. Although this can be utilized as a benefit, regrettably, it frequently fulfills the opposite purpose. Because it facilitates the





convenient consumption of readily available knowledge. Information is readily consumed. In other words, information is squandered without careful consideration, excessive scrutiny, and adequate deliberation. Typically, many researchers prioritize expediting the completion of their study over ensuring its quality. Since technology means speed and has brought speed into our lives, Academic writing has also gained significant speed in recent years. Although this accelerates and enhances production, it concurrently diminishes quality. Brunetti et al. provide a comprehensive explanation of this mechanism, stating (2022:1138):

*Although expertise in scientific article writing and academic publishing comes with practice, online digital services and software could enable authors to dramatically increase their efficiency and ease of research. Specifically, they could help the researcher improve the research and its outputs, relieving the author of repetitive and, to some extent, non-value-added (but crucial for a successful publication) activities such as corrections, finding sources, reviewing and comparing literature, finding the right journal, collecting data, and performing calculations. On the other hand, all these advanced services could introduce issues that could affect the entire scientific endeavor. For instance, a dramatic increase in research productivity could result in the mass production of similar papers, only to maximize the metrics used to measure the impact of a research product.*

Another significant challenge in this context is the difficulty of selecting the appropriate and trustworthy source from the multitude of sources encountered. Due to a lack of knowledge of source differentiation, particularly among early-career researchers, they tend to choose less reputable sources, thereby making the process more convenient. Instead of relying on scientific articles, journals, and books, people sometimes turn to more accessible sources that are prominently shown in search engines. However, these sources may raise issues about their scientific validity and dependability. Another relevant concern in this matter is the rising prevalence of substandard articles due to the proliferation of predatory journals (Talari and Ravindran, 2023:232). These journals prioritize financial gain over quality and neglect the necessary processes of peer review and editing. There are also several reasons that led researchers to prefer predatory journals. Among them are weak or lack of training in academic research techniques, pressure on researchers to publish, high cost of publishing in an open-access, quality journal, and lastly, for neophyte researchers, the rigorous and occasionally protracted peer-review process with low acceptance rates in high-quality journals is a source of frustration. In an effort to expedite the publication process, they turn to predatory journals that promise a rapid turnaround time and guaranteed acceptance (Talari and Ravindran, 2023:232).



One of the primary problems associated with digitalization in academic writing is the presence of ethical dilemmas. Various issues arise in the realm of digital research, encompassing plagiarism, the safeguarding of data privacy and security, the utilization of non-reliable resources, and infringement of copyrights, which “may violate intellectual property rights by using copyright material in its training without permission; training data sources are not openly declared.” (Zhao, Cox, and Cai, 2024:3), the digital divide and excessive use of generative AI tools and applications, and the employment of artificial intelligence to conceal instances of plagiarism (Flaih and Jasim, 2023:51–54). The launch of ChatGPT-like tools has been a significant and potentially game-changing intervention, changing not only the way writing, a crucial part of learning, is done but also how AI is perceived in the field of education more generally. Within two months of its launch, it reportedly had 100 million users, indicating an extraordinary explosion of use. Concurrently, it has sparked heated debates, especially in the realm of education, and has been entangled in numerous discussions concerning the ethics of AI, including those pertaining to privacy, bias, and society's overall impact. While tools like Grammarly, paraphrasing applications, and Google Translate have been widely used in writing with little to no controversy, ChatGPT and similar tools have sparked a huge debate about the digitization of writing (Zhao, Cox, and Cai, 2024:2). ChatGPT and similar tools and applications have brought about a debate in the academic environment. The most well-known application in this domain is ChatGPT. “Regarded by many as a groundbreaking advancement in AI, ChatGPT represents a new milestone in the field. However, as with any technological evolution, the emergence of ChatGPT brings not only benefits but also inevitable security risks and ethical issues.” (Hua, Jin, and Jiang, 2023:1).

One of the most debated ethical concerns in this context is whether to utilize generative AI applications and tools or not. Two competing approaches emerged with regard to utilizing generative AI: “The first is characterized by the utilitarian approach, which states that an action is ethical if the benefit is probably greater than the damage. The deontological viewpoint emphasizes the importance of moral behavior. From this standpoint, information suppression or user manipulation can never be viewed as ethical (Coltri, 2024:122). There are indeed numerous issues arising in the former situation. Is it advisable for the researchers to leverage artificial intelligence? If that is the case, in what manner and to what degree can it be employed? Is it necessary to provide a comprehensive explanation of these difficulties within



the research? Numerous similar inquiries are indeed posed, although these difficulties serve as the foundation.

The proponents of incorporating artificial intelligence into literature put forth the following arguments: First, it is asserted that this technology will be advantageous for all researchers, hence encouraging widespread adoption. Moreover, it is argued that leveraging advanced technologies, such as artificial intelligence, can enhance the overall quality of academic work. Researchers and academicians that possess greater expertise and can articulate the subject matter and obtain accurate solutions will emerge as the frontrunners in this competition. They argue that utilizing this approach is not morally objectionable, thus asserting that there is no concern of being disadvantaged since everyone will be on an equal footing. Furthermore, some argue that AI can assist in generating ideas, such as outlining research content or designing a specific framework. Furthermore, artificial intelligence can be employed in scientific study as long as researchers are aware of ethical issues arising therefrom. Yet, the experimental research by Zhao, Cox, and Cai proves that students and most probably researchers do employ generative AI, but they have little information and/or concern about ethical considerations (2024:1). However, the primary issue here is that there are no rules and norms set up for proper usage of AI in academic writing.

The opponents of the use of AI, on the other hand, assert that it should be completely avoided due to the contention that the information utilized by AI is essentially a form of plagiarism. They argue that this information is a compilation of data available on the market, and its ownership is anonymous. Consequently, utilizing information generated by AI is deemed ethically problematic. We are utilizing pre-existing information that is owned by others. Furthermore, even in the case that AI generates a novel creation, it is argued that the resulting information does not pertain to us and is not our possession. In this regard, the opponents of using generative AI have legitimate concerns. “Chomsky, Roberts, and Watumull's concern is that AI software lacks the ability to understand and apply ethical principles in the same way that humans do, which could lead to unintended consequences and ethical dilemmas.” (Coltri, 2024:119). In this regard, one possible ethical concern is about hallucinated text.<sup>2</sup> “On the one

---

<sup>2</sup> The phenomenon of ChatGPT generating text that seems semantically or grammatically reasonable but actually incorrect or meaningless is called “hallucination”, which is a common problem in all LLM (large language models). Hallucination can be divided into two types [18]: Intrinsic Hallucinations, which refer to situations where output text contradicts input text, and Extrinsic Hallucinations, which refer to situations where output content includes knowledge that does not exist in or derive from input.



hand, the dissemination and circulation of hallucinated texts will damage the communication ecosystem, especially in academic circles, and also hinder further development and application of ChatGPT in some industries with low fault tolerance. On the other hand, the hallucination was found to be able to reproduce private information in training data, which poses the risk of privacy violations. In addition, the hallucination of ChatGPT may be abused for illegal purposes, affecting social security and order.” (Hua, Jin, and Jiang, 2023:1). Indeed, technically, there is no mechanism to check the accuracy of information generated by generative AI, at least for now. The primary concern pertains to the imprecision of certain data generated by generative AI. This prevalent occurrence of erroneous information can result in incomplete knowledge, rendering individuals non-proficient in matters they lack mastery over or command over. Utilizing the provided information will present significant challenges.

One significant detrimental concern of employing generative AI is the suppression of individuals' creativity, as they are now wholly relinquishing their autonomy to technology. Since AI may appear to offer adequate information on certain matters, particularly those issues with which we lack familiarity. However, it can often deliver overly simplistic, insufficient, or even erroneous information on topics in which we possess expertise. Given our historical track record, it is prudent to exercise caution when placing excessive reliance on AI. As we rely more on AI to complete tasks and draw conclusions, we may observe a decline in our own intelligence and creativity over time. There is a potential danger of impeding the progress of critical thinking, diminishing the cognitive abilities of adults, or, more specifically, eradicating their capacity for creative thinking. This phenomenon is particularly noticeable in schoolchildren. Therefore, “Chomsky has argued that OpenAI ChatGPT, Google’s Bard, and Microsoft’s Sydney use of AI in education and other areas of society should be approached with caution, as it can lead to the commodification of knowledge and the devaluation of critical thinking skills.” (Coltri, 2024:127). Thus, it is imperative to exercise the utmost caution, restraint, and regulation in the utilization of AI.

Another significant ethical issue arising from the digitization of academic writing is the disparity in internet access and information availability among individuals in different places, sometimes referred to as the digital divide. The term "digital divide" refers to “the gap between individuals, households, businesses, and geographic areas at different socio-economic levels with regard to their opportunities to access information and communication



technologies (ICTs) and to their use of the internet for a wide variety of activities” (OECD, 2001:4). Researchers residing in underdeveloped areas with limited internet access and in authoritarian regimes like China, Iran, and North Korea, which impose restrictions or block global internet access for political and security reasons, face a disadvantage compared to their counterparts in the era of digitalization. While the internet is often praised for its ability to provide easy and affordable access to information, it has also had a detrimental impact on researchers in certain areas due to the digital divide.

An additional significant detrimental impact of digitalization on academic writing is the excessive reliance on technology, resulting in a near inability to think independently of it. This not only hampers creativity but also leads to the emergence of a techno-human being that is heavily reliant on technology, to the extent that it has altered our biology. Human beings are inherently distinct from our natural surroundings, as they possess autonomous structure and individual existence. Relying excessively on technology may give rise to more significant challenges for humanity in the future. Technology, inherently, is not a sustainable and consistently dependable framework. Assuming a significant likelihood, it is possible that the internet connection may be severed, the supply of electricity may be disrupted, or the information stored in the database may be erroneous, imprecise, or tampered with. Consequently, any issues related to technology will have a direct impact on the human ‘individual. Relying excessively on technology will result in numerous issues and present a substantial challenge for both the future of humanity and academic literature. Overall, some of the negative impacts of generative AI on learning are, but are not limited to: "less critical thinking and creativity—itsself seen as part of a wider malaise and the crisis of creativity; less writing skills; less authenticity; less agency because of dependence on such tools; less commitment to authenticity in communication, such as valuing authorial voice and sincerity in communications.”.

Generative AI and other tools used in academic writings are seen as “a threat to longstanding practices in education, especially to some genres of academic writing such as essays. They can also be seen as productively bringing to the fore the controversial nature of AI writing technologies, which were already creeping unacknowledged into common use.” (Zhao, Cox, and Cai, 2024:4). We, indeed, do believe that AI could be utilized to a restricted degree. However, it is important to explicitly highlight the extent and specific areas in which artificial intelligence is employed in the research introduction. Despite potential uncertainties,



plagiarism detection software may not yield very precise outcomes. Tools and applications of plagiarism software are uncertain when encountering difficulties. The use of AI products in academic literature is a subject of ongoing debate due to the lack of consensus. However, it is important to acknowledge that their utilization is unavoidable. Whether it is a student working on an assignment or a seasoned researcher, individuals at all levels benefit from these resources in some capacity. Provided that these resources are not abused, therefore, it is justifiable to extract information from them and utilize it to a restricted degree, as long as there is no unethical utilization.

To sum up, while digitization offers certain advantages for academic writing, it also presents significant challenges and ethical dilemmas. Although digitalization enhances us in one aspect, it can impede us in academic writing in another. Although it facilitates the advancement of writing through improved information accessibility and faster composition, the associated issues it presents are too significant to overlook.

### **Evolution in Scholarly Publishing**

The digital transformation has had a tremendous impact on academic publishing. “The use of digital technologies has transformed the processes of writing for academic journals and the dissemination and preservation of academic work. It has also made the measurement of the impact of publications in academic journals easier and this information more accessible to authors.” (Patridge,2020:147). The advent of digital transformation has indeed significantly revolutionized the field of academic publishing, resulting in a profound influence on open access as well as the editing and review procedures associated with books and online journals. Nevertheless, it also entails challenges such as transparency and certain expenses. As a result of digital transformation, a range of essential services are available to support scholars in their research work and publishing. These services span from literature reviews to data sets, from surveys to statistical analysis. Regarding writing services offered, they provide authors with corrections and other technical support to make the manuscript more consistent and readable. In the phase of submission and review, digital tools assist the authors both to submit their manuscript to a convenient journal and to improve their manuscript according to reviewers’ recommendations (Brunetti et al., 2022:1142-s1143). Electronic books and online magazines offer significant advantages, including reduced costs, easy accessibility to resources, faster and more convenient research, affordability, and the ability to search for specific information.



By utilizing search engines, one can efficiently and expeditiously locate the pertinent source by searching for a specific topic, thought, or idea.

Another advantage digitalization gave birth to for the publishing industry is introducing various open-access platforms, including journals, books, and other sources. Open access facilitates the democratization of information as it enables easy and widespread access to information, thereby reducing costs and promoting transparency. Offline journals are known to incur significant expenses for their development and publication, frequently requiring substantial financial resources. The open access policy offers substantial advantages for both institutions and researchers, making it a significant and transformative development. Another advantage pertains to the ecology, as the production of papers and other printing processes have a detrimental impact on the environment.

Digitalization has also significantly impacted the review process of academic papers, introducing fundamental alterations and transformations. Initially, the review process of academic publications can be significantly enhanced in terms of efficiency, simplicity, and transparency. Editors may conveniently locate individuals, and their accessibility is enhanced. However, this also gives birth to certain issues, as the proliferation of publications has reached such a magnitude that reviewers are unable to conduct thorough evaluations when faced with an overwhelming number of submissions. An additional significant issue at hand is the unequal accessibility to the internet among individuals residing in various countries, particularly in different geographical areas. This disparity is commonly referred to as the digital divide. Their internet infrastructures vary, preventing them from accessing the internet due to other amenities on the yacht, thus depriving them of the advantages of this procedure. This results in the formation of a significantly marginalized demographic. Ensuring the long-term security of online data can be prohibitively expensive and frequently unattainable. The potential destruction of all this data is a significant issue. Another big concern arising from online publications is copyright infringement. The internet enables effortless reproduction, distribution, and dissemination of someone else's products, articles, and research without obtaining permission, substantially violating their copyright.

The impact of digital transformation on academic writing extends beyond the consequences discussed above. The technique of digitization has become widespread in scientific research publications since it may be utilized at every level of this process. This study affirms that





digitization enables writers to overcome several challenges associated with publishing a scientific article and simultaneously benefits the authors throughout every stage of the publication process (Brunetti, 2022:1148). As technology advances, novel approaches and tools arise. Research by Brunetti and his colleges has found that the researchers are optimistic about the development of new digital tools and services in the future (Brunetti, 2022:1145). The ongoing development of AI presents both opportunities and risks. Currently, it is challenging to anticipate the potential extent to which generative AI can advance in the future, including the possibility of surpassing human brain capabilities. In addition, he will acquire a fresh set of skills, including the ability to express his thoughts more effectively and articulate them in written form. Undoubtedly, it is premature to pass judgment on whether this is advantageous or detrimental to human beings. However, as previously discussed, it is also deliberated on some of the perils that would ensue from developing a reliance on technology.

As generative AI advances, so do plagiarism-checking programs. The simultaneous development of these two factors would also enhance the overall quality. This new context raises the question of digitalized academic writing, presenting new ethical challenges and thus acquiring new ethical norms. Upon examining the current state of conventional ethical principles and standards, it becomes evident that technology has made significant advancements. In the realm of cybertechnology, established procedures that were once effective may now be rendered inefficient or obsolete due to the emergence of new opportunities and risks.

### **Findings and Conclusion**

The impact of the digitalization on academic literature has been multidimensional and transformative. As a result of the game-changing effect of artificial intelligence tools from the invention of the computer, major changes have occurred in the research, writing and publishing processes. This change and transformation has brought about a number of opportunities and ethical challenges that all education stakeholders need to think deeply about.

The process has facilitated access to information through online resources, academic databases and e-libraries, while boosting collaboration between researchers and effectively speeding up both writing and publishing processes and increasing academic efficiency. However, due to the speed and consumption habits developed in every field in this age,





ethical problems such as superficial research and the quality problems it causes due to the rapid consumption of information. Plagiarism, which can be easily masked with different methods, widespread intellectual property violations and the proliferation of predatory journals have emerged together with some other ethical problems.

Among these ethical problems, the most controversial and academic solution still not developed are utilization of productive AI tools such as ChatGPT and Gemini. While these services increase production and sometimes even quality on one hand, on the other hand, they not only increase the concern about plagiarism (in fact, according to some, the entire production of AI tools already constitutes plagiarism, since it creates a combination of information in the database rather than producing original information itself), but also weaken the ability of people who have become dependent on technology to produce original ideas and think critically. One of the other most important ethical problems here is the existence of technology access barriers that prevent equal access to information. In other words, due to this reality called digital divide, people in different regions have different access opportunities to the internet, and this removes equal opportunities among researchers. In short, digital transformation, as in every field, has brought about great changes and transformations in academic literature, while on the one hand it offers great opportunities, on the other hand it has brought about serious ethical problems and dilemmas. While academic research, publication and dissemination processes, access to information, inclusiveness, use and collaboration processes have gained speed and efficiency, serious ethical problems such as plagiarism, quality problems, intellectual property rights and digital difference have emerged. In this context, the most discussed issue of writing with AI tools seems to be one of the most challenging and worrying developments for researchers now and in the future. In order to solve all these problems and to benefit from the blessings of digitalization with peace of mind, a comprehensive effort is required to solve the ethical issues that arise. This effort should produce a comprehensive and principle-based result that will cover both all educational stakeholders and all regions of the world.

## References

Brunetti, et.al.(2022). Digitalization and academic research: knowing of and using digital services and software to develop scientific papers. *The TQM Journal*, Vol. 35, No. 5, pp. 1135–1155. <https://www.emerald.com/insight/content/doi/10.1108/TQM-02-2022->



[0050/full/pdf?title=digitalization-and-academic-research-knowing-of-and-using-digital-services-and-software-to-develop-scientific-papers](#) [Accessed on August 3, 2024].

Coltri, M.A.(2024). The Ethical Dilemma with Open AI ChatGPT: Is It Right or Wrong to Prohibit It? *Athens Journal of Law*, vol. 10, no. 1, pp. 119–130. <https://www.athensjournals.gr/law/2024-10-1-6-Coltri.pdf> [Accessed on August 3, 2024].

Council of Europe (2019). *Digital Citizenship Education Handbook*. Strasbourg:COE. <https://rm.coe.int/16809382f9> [Accessed on August 5, 2024].

Devitt, A. Benetos, K., and Kruse, O. (2023), Writing and Learning: What Changed with Digitalization? pp. 423–433 in (eds) Otto Kruse, Christian Rapp, Chris M. Anson, Kalliopi Benetos, Elena Cotos, Ann Devitt, and Antonette Shibani. *Digital Writing Technologies in Higher Education: Theory, Research, and Practice*. Cham:Springer.

Farias-Gaytan, S., Aguaded, I., and Ramirez-Montoya, MS (2023). Digital transformation and digital literacy in the context of complexity within higher education institutions: a systematic literature review. *Humanit Soc Sci Commun.*, Vol. 10, No. 386, pp. 1–11. <https://www.nature.com/articles/s41599-023-01875-9> [Accessed on August 5, 2024].

Flaih, T., and Jasim, Y.A. (2023). The Ethical Implications of ChatGPT AI Chatbots: A Review. *Journal of Modern Computing and Engineering Research*, vol. 2023, pp. 49–57. <https://jmcer.org/wp-content/uploads/2023/08/The-Ethical-Implications-of-ChatGPT-AI-Chatbot-A-Review-1.pdf> [Accessed on August 5, 2024].

Hua, S. Jin, S., and Jiang, S. (2023). The Limitations and Ethical Considerations of ChatGPT. *Data Intelligence*, Vol. 6, No. 1, pp. 1–18. <https://direct.mit.edu/dint/article/6/1/201/118839/The-Limitations-and-Ethical-Considerations-of> [accessed on August 5, 2024].

Kulish, I. (2023). Problems of digitalization in institutions of higher education. *Modern Management Systems*, Vol. 18, No. 3, pp. 85–98. <https://nsz.wat.edu.pl/Problems-of-digitalization-in-institutions-of-higher-education,183869,0,2.html> [Accessed on August 5, 2024].

Mikalef, P., and Parmiggiani, E. (2022). An Introduction to Digital Transformation. In: Mikalef, P., and Parmiggiani, E. (eds.), *Digital Transformation in Norwegian Enterprises*. Cham:Springer, [https://doi.org/10.1007/978-3-031-05276-7\\_1](https://doi.org/10.1007/978-3-031-05276-7_1) [accessed on August 3, 2024].

OECD.(2001). *Understanding the Digital Divide*. Paris:OECD Publication. <https://www.oecd-ilibrary.org/docserver/236405667766.pdf?expires=1722868694&id=id&accname=guest&checksum=C37FE83468C082037C86E2F9DCB3B1E4> [Accessed on August 5, 2024].

Patridge, B.(2020). Writing for Academic Journals in the Digital Era.*RELC Journal*, vol. 51, No. 1, pp. 147–157.



<https://journals.sagepub.com/doi/abs/10.1177/0033688219890359> [Accessed on August 5, 2024].

Rosha, Angelina. (2021). Exploring the Role of Ethical Issues in the Context of Digital Transformation. Trends in *Economics and Management*, Vol. 15, No. 38, pp. 23–33. <https://trends.fbm.vutbr.cz/index.php/trends/article/view/591> [Accessed on August 5, 2024].

Sausen, H.(2020). *What is Digitalization: Opportunities and Challenges in East Africa?* Kigali: Friedrich-Ebert-Stiftung Rwanda. <https://library.fes.de/pdf-files/bueros/ruanda/16158.pdf> [Accessed on August 3, 2024].

Talari, K., and Ravindran, V. (2023) Predatory journals: how to recognize and keep them clear!. *The Journal of the Royal College of Physicians of Edinburgh*, Vol. 53, No. 4, pp. 232-236.

Zhao, X., Cox, A., & Cai, L. (2024). ChatGPT and the digitization of writing. *Humanities and Social Sciences Communications*, 11(482). pp. 1–9. <https://www.nature.com/articles/s41599-024-02904-x.pdf> [accessed on August 4, 2024].

---

[11] The phenomenon of ChatGPT generating text that seems semantically or grammatically reasonable but actually incorrect or meaningless is called “hallucination”, which is a common problem in all LLM (large language models). Hallucination can be divided into two types [18]: Intrinsic Hallucinations, which refer to situations where output text contradicts input text, and Extrinsic Hallucinations, which refer to situations where output content includes knowledge that does not exist in or derive from input.



## CONTACT TRACING IN TIMES OF HEALTH CRISIS: PRIVACY AND DATA PROTECTION LESSONS FOR FUTURE PREPAREDNESS

**Alaa SAKKA \***

Orcid: 0009-0006-1683-7958

**Sonny ZULHUDA \*\***

Orcid: 0000-0003-0192-1971

### *Abstract*

This paper examines the connection between the use of tracing applications such as those in the COVID-19 pandemic and the legal issues pertaining to privacy and data protection. It explores how various contact tracing app designs might either mitigate or increase the risks of privacy infringement and personal data breaches. It finds that the COVID-19 applications had faced a variety of difficulties, including security dangers, privacy concerns, political, ethical, and legal uncertainties, as well as issues with standards. The rise of contact tracing techniques and monitoring technologies allows countries to opt for a centralised or decentralised approach. The paper argues that contact tracing apps should operate on a decentralised approach and should collect as limited personal data as feasible. This paper can help us to take lessons from COVID-19 tracing apps to ensure privacy and data protection are adequately addressed for our future crisis preparedness.

**Keywords:** COVID-19, Contact Tracing, Privacy, Data Protection, Apps.

### **Introduction**

During the COVID-19 pandemic, governments introduced nationwide contact tracing programmes using contact tracing apps and mobile devices. Such a programme was created to aid governments to control the spread of coronavirus by recording the movement and the travel of people. With this contact tracing programme, one can discover whether he has come into contact with someone who has tested positive for the virus. This programme

---

\* Ph.D. Candidate, Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia. E-mail: [alaasakka1995@gmail.com](mailto:alaasakka1995@gmail.com)

\*\* Assoc. Prof. Dr. Ahmad Ibrahim Kulliyah of Laws, International Islamic University Malaysia. E-mail: [sonny@iium.edu.my](mailto:sonny@iium.edu.my)



unquestionably helps to stop the disease from spreading, but it also poses tricky and questionable data protection concerns.

The amount of personal information that COVID-19 tracing applications gathered is one of the biggest causes of concern. The software gathers information about a person's whereabouts, health, and possibly other private information including their name, address and contact information. This information needs to be well protected not only because they are personal, but also because the data could be sensitive. Other privacy and data protection concerns originated from the app's data processing and storage: those apps must securely process and store data to prevent unauthorised access, usage and alteration or modification. Among others, COVID-19 tracing applications must adhere to the principle of data minimization and purpose limitation. The app should only gather information that is directly relevant to fulfil its stated objectives and should not use this information for any other purposes.

Concerns regarding accountability and transparency are also present. Users should be informed of the data that is being collected; why it is being collected and how it is being handled by the app. There must be clear lines of accountability in the event of a data breach. However, since COVID-19 tracing apps were considered useful tools for limiting virus spread, it is crucial to make sure that privacy and data protection issues are properly addressed. This would therefore call for precise guidelines, strong data protection safeguards, and openness and accountability from those in charge of running these apps.

As we contemplate how to best prepare for any future crisis, we must learn from the COVID-19 pandemic and establish plans that meet privacy and data protection concerns. This article investigates the lessons learnt from the use of tracing apps during the COVID-19 pandemic, as well as best practices for future efforts. We suggest that privacy and data protection should be key to the design and execution of these programmes and that international standards and guidelines should be adopted to ensure that these issues are effectively addressed. By resolving these concerns, we may increase public trust and confidence in the use of digital tracing apps and other digital technologies in the battle against pandemics.

### **Contact Tracing Application**

During the peak of the coronavirus disease rise, it became essential to track down contacts to identify and manage potentially serious cases. In the early stages of COVID-19, patients who



had been diagnosed with the disease began contact tracing manually. However, the situation has changed due to the use of modern and technological techniques to cover and speed up the process of tracing contacts through programmes that allow the collection of personal information and the location of the person using the Global Positioning System (GPS) and the Bluetooth feature in modern devices, by scanning the QR code (WHO, 2020). Using manual tracing, which is frequently erroneous, (Sowmiya, Abhijith, Sudersan, Sundar, Thangavel, and Varalakshmi, 2020) it would take a lot of time, money, and effort to find a case of the coronavirus. In that scenario, medical personnel would need to speak with the patient and advise ways to stop the disease from spreading further. Currently, the contact tracing tool will be used to get in touch with the infected person when a coronavirus infection is discovered. This will allow for the implementation of measures like self-quarantine, social isolation, and virus testing on sick individuals. Health personnel, for instance, in Malaysia can identify people who have been in close proximity to an infected person according to the data that has been gathered for pandemic control purposes. Digital proximity tracing tools are one component of a larger system of laws, programmes, and investments, even though contact tracing for COVID-19 may benefit from their use. Governments and healthcare organisations should inform the public about how this set of policies, interventions, and technologies will work together as part of a bigger strategy (WHO, 2020).

Contact tracing is divided according to the World Health Organization into three main steps; firstly, identifying the contact by identifying those who have been in direct contact with a person infected with COVID-19, secondly, informing the person so identified of the steps he must take, and thirdly, following up on contacts by watching for symptoms and testing for signs of infection (WHO, 2017). The WHO has further shown that in response to the coronavirus pandemic, new software has emerged to control contact tracing, including human contact tracing and digital contact tracing (WHO, 2017). In Malaysia, for example, both systems have been adopted, but residents have expressed worries about their privacy; this article will explore each of them to shed light on the privacy issues highlighted by contact tracing in light of the COVID-19 pandemic. The COVID-19 tracing applications are used in two methods, centralized and decentralized. Some of them follow Bluetooth technology, including the Global Positioning System (GPS), for instance, the government of India developed the Aarogya Setu app as a coronavirus surveillance tool to monitor the number of cases in a region and stop the infection's spread (Sowmiya, et al., 2020). The Aarogya Setu software for cell phones uses Bluetooth and GPS technology to follow the movements of an



infected individual, inform the public about places they have been, and mark those places as vulnerable zones (Clarance, 2020). The user follows several conditions for use and registration on the server, when the user registers on the server, devices via Bluetooth exchange their temporary identifier when the person is close to a person infected with the Coronavirus (Sowmiya et al., 2020). When a person is infected with the COVID-19 virus, healthcare workers are compelled to send encounter notifications to the central server, or the user can willingly send all their information to the server. To identify vulnerable contacts, the central server provides temporary identification in messages to users (Chowdhury, Ferdous, Biswas, Chowdhury, And Muthukkumarasamy, 2020).

In a decentralized system, the server is only involved in the contact tracing phase because consumer devices have limited capabilities. This technique promotes user privacy by establishing anonymous identities on user devices and processing exposure notifications on personal devices rather than a central server (Sowmiya et al., 2020). Once infected with the COVID-19 virus, the affected person can upload their encrypted key to a central server. In contrast, the centralized architecture uploads the entire user profile.

### **Human Contact Tracing and Its Impact On Privacy**

At the beginning of the COVID-19 crisis around the world, all governments took precautionary and health measures to combat the virus, their concern for the lives of their citizens, and their attempt to contain the Coronavirus. Therefore, governments around the world implemented mass contact tracing programs to monitor the location of an infected or suspected person to know their whereabouts and to help control the spread of COVID-19 (VoxEU, 2021).

At the start of the global pandemic, human contact tracing began with manual data entry. During this time, governments adopted and implemented automated contact tracing programmes. In an effort to reduce and halt the spread of the SARS-Cov-2 virus, these contact tracing techniques benefit the person infected with the virus and impose mandatory quarantine on them for a period determined by the Ministry of Health for the affected citizen, and the ministry determines the severity of their infection. Improved digital data flux, proximity tracing, and geolocation monitoring sped up contact tracking and reporting operations (Vokinger, Nittas, Witt, Fabrikant, and Wyl, 2020). If an infected case is suspected, the person must examine the Coronavirus; if the result is negative, the person can





depart; if the result is positive, the person must be quarantined. These programmes track people by scanning a QR code when they enter any building, whether residential, commercial, or industrial.

When a person with COVID-19 is discovered, their data in the contact tracing programme is updated if they feel sick, cough, fever, or other symptoms. The responsible authority that operates the application can use this information to notify whoever was in the vicinity of the same infected person and determine whether the infected person was in direct or indirect communication with the other person via Bluetooth or GPS (Li, 2021). For instance, in the contact tracing programme used in the state of Massachusetts in the United States of America, the contact tracer can directly contact the infected person and ask them for a list of those who have been in contact with them over the past two weeks. Those who have been in contact with them are then contacted three times in a row to make sure they understand the significance of this call, and when they respond, the contact tracer will inform them of their potential exposure to the virus and advise them to follow certain guidelines (Barry, 2020). While in South Korea, for instance, contact tracers follow up with contacts and either request or impose on a data subject that they promptly report their data and symptoms to a government database if it is determined that they have been infected (Kim, 2020). In Malaysia, the MySejahtera app debuted a new function called MySJ Trace that utilised Bluetooth to find the immediate or passing acquaintances of COVID-19 instances (Su-Lyn, 2021). In order to identify close contacts, the Ministry of Health (MOH) method involves looking at who checked into a specific place at the same time as a confirmed COVID-19 case (Su-Lyn, 2021).

Follow-up of people by health care or health workers before it is too late leads to a reduction in infections with the Coronavirus, imposing social separation and conducting a COVID-19 examination and imposing a quarantine on those who prove that they have been infected will reduce infection among citizens and not direct contact with the injured, Thus, if infections are mitigated and the virus is controlled, this will help to return life to normal as it was before the pandemic.

The impact of tracing human contacts on an individual's privacy is one of the critical aspects that we can discuss in the application of contact tracing. This is due to some concerns on the excessiveness of data being collected and processed vis a vis its usefulness. Human rights and basic freedoms may be violated if vast amounts of sensitive personal and non-personal data





are gathered and used for reasons that are not directly or particularly relevant to the COVID-19 response (WHO, 2020). This concern becomes much more critical if some of the emergency measures put in place to combat the pandemic, including computerised contact tracing, become commonplace (WHO, 2020). Infected individuals may divulge names and contact details of prospective contacts as well as other details, such as the affected person's whereabouts and activities in the days before the beginning of symptoms, during identification talks with contact tracers (Li, 2021). Human contact tracing program carries some security and privacy issues; the more persons who have access to any data such as health data, the greater the danger of data exposure. This has a detrimental effect on privacy (Li, 2021).

Contact tracing needs to be done for specific, legal reasons, or it needs to be disclosed to the data subject beforehand. The Organization for Economic Cooperation and Development's (OECD) Privacy Framework states that "the principle of collection restriction is that there must be restrictions on the collection of personal data and any of this data must be obtained by legal means and fair and, where appropriate, with the knowledge or consent of the data subject" (OECD, 2013). "In terms of the principle of data quality, personal data must be relevant to the purposes for which it will be used, and must be accurate, complete and up to date to the extent necessary for those purposes" (OECD, 2013). There are limitations on the cross-border movement of personal information in Malaysia even though it is not a member of the Organization for Economic Cooperation and Development. According to the OECD, the security guarantee principle requires that all precautions be used to protect personal data from risks such as data loss, use, modification, unauthorised access, destruction, or disclosure.

When it is known that a person has been infected with the Coronavirus, it may be contacted by the health care or others to find out the people who have been in contact with them during the past two weeks and through this communication may be by phone and therefore when sharing the people with whom they came into contact, the infected person may share their information Such as names, phone numbers, address, health information, age and other information. Thus, the information will be shared by phone, and it is not possible to guess whether this data was leaked or violated when shared by hackers. Contact tracing is a vital public health strategy and a vital part of all-encompassing COVID-19 control measures (WHO, 2020). According to WHO, Proximity tracing methods can assist in identifying contacts by determining when people were in close physical contact and were in ongoing



touch with a case whether using Location data or Bluetooth signals; The GPS position of users is the foundation of location-based tools, they could be used to help with contact identification by locating individuals who have visited the same area as cases; Users may receive direct alerts of contact events involving cases reported, testing locations, or other useful information, like as where to find masks, through links to other information systems; While keeping the capacity to supply location-based data for contact tracing, additional location-based applications have been created that protect anonymous by not linking to other databases; Users can determine whether they were close to a case without giving a location by using Bluetooth communication between devices. Contact tracers can use data to find possible contacts for cases (WHO, 2020).

According to Malaysia's Prevention and Control of Infectious Diseases Act of 1988, the regulations established by the Minister may provide for the collection and transmission of epidemiological and health information as well as the required reporting of infectious diseases that occur in Malaysia (Prevention and Control of Infectious Diseases Act 1988 (Act 342) (PCIDA 1988), p.31). One type of data gathered through human contact tracing is health information. According to this statute, the Malaysian Ministry of Health has the authority to handle the collection and processing of data in the COVID-19 crisis for the contagious mutant coronavirus. As a result, the Personal Data Protection Act of 2010 and the Prevention and Control of Infectious Diseases Act of 1988 must be followed in order to comply with the set laws while transferring health data and information, all institutions must comply with the stipulated laws whether in receiving or transferring data. Malaysian PDPA 2010 however does not apply to governments, leaving it only narrowly applied to non-governmental institutions who are involved in the pandemic responses.

When using human contact tracing apps, there are some risks to data privacy and security, especially when the number of people who can access personal data and health information increases, the risk of data exposure and leakage may increase. It can be hard to keep track of whether they practice good cybersecurity safeguards and procedures when it comes to securing data, since so many contact tracing tools run remotely. It can be hard to know who is accessing this data and who is writing it down during conversations. Human error cannot be avoided, so for the sake of security and privacy, it may be best to use a digital contact tracing program.



Since the beginning of the COVID-19 outbreak, Malaysians have witnessed countless instances of patients' private information being released via social media. A patient going by the name of "Patient 16" became the target of hate and discrimination after his name and profile photo was widely disseminated on social media, and these feelings lasted even after he had been cured of the virus (The Star, 2020). In other cases, the public defence of "Patient 26" and "Patient 136," who were allegedly "super-spreaders," on social media was compelled by the publication of private information (Atan, 2020). But as a result of their conduct, more disparaging remarks were made about them. These three examples demonstrate why it's crucial to protect patients' privacy during a pandemic in order to avoid stigmatization, prejudice, and accusation (Yusof, Muuti, Ariffin, and Tan, 2020).

### **Tracking of Digital Contacts**

Digital contact tracking was one of the contact tracing techniques that appeared to restrict the Coronavirus and limit its transmission during the global COVID-19 crisis (O'Neil, Mosley, and Johnson, 2020). The Global Positioning System (GPS) and other Bluetooth technologies, which are connected through proximity data, are modern technologies that are used in digital contact tracing to quickly detect the necessary data to detect a person, whether they are near an infected person or an infected area (Criddle and Kelion, 2020). When one person is near another who is holding a Bluetooth-enabled phone, this feature activates (Criddle and Kelion, 2020).

Some nations have created contact tracing software, and Malaysia is one of them. Malaysia has created the MySejahtera smartphone app for contact tracing and data monitoring of people in order to contain COVID-19 in the nation, which aids in identifying potential contacts of infected people. Applications for contact tracing typically concentrate on two areas to capture and maintain information on two fundamental approaches: (Kaya, 2020) a centralised approach system, which uses location data from mobile phones, and a second, a decentralised approach system, which uses the short-range Bluetooth standard (Criddle and Kelion, 2020). Contact tracers can inform contacts of their potential virus exposure, the risks they may encounter, and the recommended actions through these two systems.

Despite this, it can be claimed that digital contact tracing and human contact tracing are two harmonious methods that complement one another (Cofone, 2021). Instead of employing contemporary technology and software that can be more easily accessed by hackers, human



contact tracing can reduce dangers and provide residents the confidence to record their data. Additionally, human contact tracing is error-free unlike digital contact tracing. While human contact tracing can assist individuals more quickly by providing adequate knowledge about the hazards and the essential advice in the event of virus infection and how to self-isolate. As a result, in terms of data monitoring, human contact tracing and digital contact tracing are complementary to one another but cannot be used in place of one another.

### ***Centralized Digital Contact Tracing***

There are centralized and decentralized digital contact tracing applications, and each differs from the other in terms of saving data in a central server or relying on a central authority for contact tracing data and processes, the central server uses this database to perform contact matching and notify those who have recently contacted the infected person (Zhang et al, 2020). Applications for centralising digital contact tracing are based on two fundamental types of data, one of which is Bluetooth data and the other is global positioning data (GPS), and each of them has a different level of location precision. For example, Bahrain, Kuwait, and Norway track the central connectivity of users' locations by repeatedly uploading GPS coordinates to a central server (Amnesty International, 2020). While in Singapore, the Trace Together app uses Bluetooth to gather proximity data, which is then safely saved on the user's smartphone. However, in the event of a corona infection, the user will be compelled to give his data to the Ministry of Health (Smart Nation Singapore, 2021). Moving on to Qatar, the Ehteraz programme there carries a Bluetooth link between users' smartphones and records the GPS locations of the conflict (Amnesty International, 2020).

The centralised contact tracing application, as we previously stated, is based on two fundamental forms, namely Bluetooth data and the Global Positioning System (GPS). However, the decentralised contact tracing application based on Bluetooth differs from the centralised application in that it exchanges anonymous keys from one device to another device to infer proximity between users. Whereas a Bluetooth-based central contact tracing programme may determine proximity using keys stored in a central database using information gathered from each device and findings sent back to the devices (Li, 2021).

The use of centralised contact tracing raises privacy concerns because governments will be able to save their users' data with some limitations using this data, which worries users because the government has complete control over all data that is collected, used, stored, and



shared with very few limitations on what governments can do with the data. Although governments enforce contact tracing programmes on users and keep their users' data through those programs, each country's laws provide protection against the misuse of user data.

### ***Decentralized Digital Contact Tracing***

Another method that is employed in many nations, including Malaysia, is decentralised digital contact tracing, which uses short-range Bluetooth technology to identify people's proximity when they are connected to Bluetooth devices at specific times. The user's device is the only place where this information is kept while utilising a decentralised digital contact tracing programme. Malaysians utilise the MySejahtera app, which fits under the decentralised paradigm (Rupert, 2021). Location information will only be obtained, in accordance with the MySejahtera privacy policy, when the user has authorised access to the device's location services (MySejahtera, 2021). It was said that the MySejahtera app on Google Play did not gather user data (MySejahtera, 2024). In light of the fact that the decentralised approach only stores data on the user's device, we contend that the app fits within this category. Additionally, as Apple would not have permitted the MySejahtera upgrade, the Malaysian government does not retain users' personal information from the app (Su-Lyn, 2021). While it was said that the MySejahtera Trace app functions as follows, MySJ Trace really permits cooperating devices to exchange proximity data whenever it detects another device with the same software running. Only employees of the Ministry of Health (MOH) will keep and examine the data gathered. A user will begin a process to upload data from their smartphone to a secure database operated by the MOH once it has been verified that they are COVID-19 positive (MySejahtera Trace, 2024). Through MySejahtera, MySJ Trace uses Bluetooth to communicate proximity data that identifies who has been in close vicinity to a COVID-19 holder (Malay Mail, 2021). By tracing the contact, MySJ Trace enhances the functionality of MySejahtera (Salim, 2021).

When a person is infected with the Coronavirus, they themselves will update their data on the application used in the country that follows the decentralized digital communication, but this task can be carried out by another party, for example, and it can be said that the public health authority is in the event that the person goes to test for COVID-19. Thus, decentralized digital contact tracing applications will use a record of anonymous key codes exchanged between phones to identify individuals who have been in close proximity to an infected person.



Despite the fact that some nations have developed contact tracing applications globally, residents and citizens of some of these nations were unsatisfied with these applications due to their concern that these applications would be compromised or that the data they had collected would be leaked. For example, as of July 2020, only 14.4% of the population in Germany had downloaded the Corona-Warn-App, and only 3% of the population in France had downloaded the similar StopCovid app, while the Italian government's Immuni has dropped to 7.2 per cent of the population (Geiger, 2020). But as of September 2022, the German Warn-App COVID-19 contact tracing app was recently downloaded almost 21 million times from the Apple App Store, while the Google Play Store recorded around 26 million downloads, (Statista Research Department, 2022) and in France the StopCovid app had been downloaded by 16.5 million people as of May 2021, (Reuters, 2021) while the Italian government's Immuni app had been downloaded 2.28 million times by users as the first quarter of 2022 (Ceci, 2022). However, as of December 2020, nearly 70% of Malaysians have downloaded the MySejahtera app and use the app to check-in at the places they enter, (Mok, 2020) while as of March 2022, nearly 38 million users are using the MySejahtera app (Zainuddin, 2021). These data collection and storage tools might not be a panacea for every country's COVID-19 situation, but they could help slow the virus's spread and learn how to handle such crises in the future.

Apple and Google have collaborated on COVID-19 contact tracing technology, and in turn, they were able to use Bluetooth technology to track contacts by proximity to one device to another, to help governments and health track contacts and limit the spread of COVID-19, taking into account the privacy of users and the security of their data (Sainz, 2020). The two companies also released a solution that includes Application Programming Interfaces (APIs) and OS-level technology to help enable contact tracing. The first solution is to launch applications programming interfaces and then the second solution is to use Bluetooth technology to trace contacts with the help of developers, governments and public health providers.

Therefore, the use of decentralized digital contact tracing helps protect privacy and data from the violation or hack that may occur in the case of using centralized digital contact tracing, because centralization depends on saving data in a central database of the government that maintains its servers. Users can save data directly on their phones and not go to a central database, thus, with a decentralized system, there is no huge data that hackers can infiltrate and violate (Starks, 2020).



Recently, MySJ Trace was developed in Malaysia by the government. This development was used under the contact tracing application MySejahtera and the addition of this feature on the same application that helps the Malaysian Ministry of Health to contain COVID-19, MySJ Trace adopts the use of Bluetooth to share proximity data through MySejahtera identifies who has been in close contact with a person with COVID-19 (Malay Mail, 2021). MySJ Trace complements the MySejahtera application by tracing the contact when a device is near another via the Bluetooth feature and proving who was in close contact with another person infected with the virus (Salim, 2021).

MySJ Trace was developed through a strategic collaboration between Malaysia's government agencies, the Ministry of Science, Technology and Innovation (MOSTI), the Malaysian Ministry of Health (MoH), the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) and the Malaysian Institute of Microelectronic Systems (MIMOS) (MySejahtera Trace, 2024). The data collected will be stored by the Ministry of Health, the collected data includes the unique user identifier (UUID) generated by this application, and the data will be collected and used in accordance with government information security standards (MySejahtera Trace, 2024).

If it is confirmed that the person is infected with the virus and the person's condition is positive, the infected person can send the interaction data to the Ministry of Health (MoH) to conduct the contact tracing process, since all interaction data is anonymous according to the Ministry of Health (Malay Mail, 2021). The researcher contends that although contact tracing via Bluetooth may be efficient, sometimes it may be inaccurate in terms of data collection. This raises concern because a person may pass by another person who was not particularly close to the infected person but who may be detected as infected, the researcher claims. Therefore, the users of the app might not be interested in Bluetooth's efficacy.

### **Legal Issues in Contact Tracing Programs and Lessons From Malaysia**

The deployment of contact tracing applications in all nations, at both the global and national levels, entails privacy problems and is insufficient to completely get rid of the virus. However, the proliferation of contact tracing software slows the spread of COVID-19 in various nations by facilitating contact tracing. Technical specialists must explain the uses of





centralised and decentralised contact tracing to authorities and policymakers for them to distinguish between and comprehend these uses.

It is noted that in light of the COVID-19 crisis, these recently developed applications cannot be effective correctly and precisely without any errors in the applications. Among these errors may be, for instance, the use of Bluetooth technology on users' devices, which may be advantageous for the speed of its interaction to find the case of an infected or semi-infected person an injured person had met the person or had passed by him. It's possible, though, that the individual was not carrying his gadget and that a proven instance was recorded using Bluetooth technology, or that individuals were seated in their homes and their neighbouring Bluetooth-enabled devices were connected (Anderson, 2020). Thus, these applications are not completely accurate.

Decentralized applications may be preferable to centralised ones because they provide confidence to the data subject utilising them and maintain technological privacy on the user's device (Auxier, Rainie, Anderson, Perrin, Kumar, And Turner, 2019). To cope with the COVID-19 crisis that nations are experiencing, governments that utilise these programmes must enact laws or update their existing ones, given that the laws restrict the use of the data that is gathered through the contact tracing process in order to preserve the privacy of users. People who design, install, and maintain contact tracing software must specify and abide by predetermined criteria, much as researchers are defining interoperability standards for decentralised contact tracing apps.

Therefore, it is against Malaysia's Prevention and Control of Infectious Diseases Act 1988 (PCIDA) to fail to give the necessary data for the control of infectious diseases. Pursuant to Section 22 of this Act or any regulations made thereunder, (PCIDA 1988, p.22) Regulation 6 of the Prevention and Control of Infectious Diseases (Measures Within Local Infected Areas) Regulations 2020, (Federal Government Gazette, 2020) provides for compliance with an authorized official's request for any information relating to the prevention and control of infectious disease. Therefore, when health authorities or officials ask for personal information about a worker or visitor for an investigation or contact tracing, employers are required under legal obligations under PCIDA. Employers are now permitted to gather information and then release it without permission to health authorities and officials in order to comply with legal obligations under PCIDA and PCIDR.





The Prevention and Control of Infectious Diseases Act of 1988 can be useful. The Prevention and Control of Infectious Diseases will be governed by this law. An infectious sickness is any illness that falls under Part II of the First Schedule to the Act. Clearly not mentioned there is COVID-19. This new ailment, however, can be categorised as another microbial infection that poses a serious risk to life according to the given schedule. Section 10 of the Act mandates that every adult resident of a home who becomes aware of the existence of any infectious diseases on any premises must immediately notify the appropriate authorities through notice (PCIDA 1988, p.10).

In accordance with Section 11 (1) of the Act, the Minister of Health may proclaim a district to be an infectious local area by gazette if the Minister is confident that an infectious disease outbreak or pandemic danger exists in any region of Malaysia (PCIDA 1988, p.11). The section also gives the Minister the authority to specify by regulation the steps that must be taken to contain or prevent the spread of infectious illnesses within or from a locally afflicted area. These include requiring any person, group, or class of person to get medical care or immunizations, to be segregated or under close supervision or surveillance, or to undergo any other measures considered necessary (PCIDA 1988). Anyone who disobeys any legitimate orders, directives, or limits issued by an authorised authority or who breaches any rules or regulations established under the Prevention and Control of Infectious Diseases Act of 1988 is guilty of an offence under the Act (PCIDA 1998).

In Malaysia, the experience of dealing with the COVID-19 pandemic gives us massive lessons. Statutes and administrative laws are very crucial in ensuring all necessary responses are taken to control the pandemic while preventing its further spread. Along with their implementation, we face the challenge that individuals' privacy concerns are important and indispensable. The fact that the main data protection law in the country is inapplicable to the government should not undermine the need to respect individuals' privacy. Therefore, defining certain guidelines on data protection best practices during the pandemic response should be a future agenda in Malaysia.

## **Conclusion**

Four years after COVID-19 was first declared a pandemic, the study shows that the privacy and data protection concerns of COVID-19 tracking applications are serious matters that



require due attention. While there is no denying that the software helps stop the virus from spreading, it is crucial to make sure that sensitive personal data is only collected, processed, and stored for the purposes for which it was intended. Strong data protection mechanisms, openness, and responsibility from people in charge of the app's operation are necessary for this. Users also need to be aware of the information being gathered about them, how it will be used, and how they can access and delete it. Ultimately, it is critical to find a balance between defending the public's health and preserving people's right to privacy, and doing so will call for continued work and cooperation amongst many parties.

The worldwide COVID-19 pandemic has drastically altered civilization, to truly appreciate its impacts, the world will need to have a long-term historical perspective. It is apparent that current advancements, whether in privacy or technology, will have an impact on how society develops in the future. Data-driven initiatives launched in response to COVID-19 have already altered how society interacts with technology and privacy concepts, ranging from widespread public health testing to personal communication tools. Expectations of privacy are altering, and the pandemic will certainly have long-term consequences, including unexpected consequences for society's future and how it interacts with technology. Moving forward, it is critical to build socially beneficial privacy concepts, as well as laws and regulations that protect both public health and civil freedoms.

## References

- Aimi Nadia Mohd Yusof, Muhamad Zaid Muuti, Lydia Aiseah Ariffin, & Mark Kiak Min Tan. (2020). Sharing information on COVID-19: the ethical challenges in the Malaysian setting. *Asian Bioethics Review* 12 (3), 349–361.
- Alifah Zainuddin. (2022, March 30). MySejahtera check-ins fall 26% amid app ownership doubt. CodeBlue.
- Andrew Clarence. (2020, May 15). Aarogya Setu: Why India's Covid-19 contact tracing app is controversial. BBC News.
- Auxier, Brooke., Rainie, Lee., Anderson, Monica., Perrin, Andrew., Kumar, Madhu., and Turner, Erica. (2019, November 15). Americans and privacy: Concerned, confused and feeling a lack of control over their personal information. Pew Research Center. Retrieved from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Bernama. (2021, December 26). Health Minister: 'MySJ trace' using Bluetooth tech new feature in MySejahtera to trace close contacts. Malay Mail.
- Boo Su-Lyn. (2021, December 28). How MySejahtera trace's Bluetooth contact tracing works. CodeBlue. Retrieved from <https://codeblue.galencentre.org/2021/12/28/how-mysejahtera-traces-bluetooth-contact-tracing-works/>



- Claudio Guarnieri. (2020, June 16<sup>th</sup>). Bahrain, Kuwait and Norway contact tracing apps are among most dangerous for privacy. Amnesty International.
- Cofone, I. (2021). Immunity passports and contact tracing surveillance. *Stanford Technology Law Review*, 24 (2), 176-236.
- Cristina Criddle, and Leo Kelion. (2020, May 7). Coronavirus contact-tracing: World split between two types of app. BBC News.
- Ellen Barry. (2020, April 16). An army of virus tracers takes shape in Massachusetts. The New York Times.
- Fred Sainz. (2020). Apple and Google Partner on COVID-19 Contact Tracing Technology. Apple Newsroom, Retrieved from, <https://nr.apple.com/d2s6h070n0>
- Gabriel Geiger. (2020, July 21). Europeans aren't really using COVID-19 contact tracing apps. Vice.
- Guidelines governing the protection of privacy and transborder flows of personal data. (2013). The OECD Privacy Framework, 2013. *Organisation for Economic Co-operation and Development*.
- Kaya, E. K. (2020). Safety and privacy in the time of Covid-19: contact tracing applications. *Centre for Economics and Foreign Policy Studies*, 1-11.
- L. Ceci. (2022, April 8). Downloads of official COVID-19 Green Pass apps in Italy 2022. Statista. Retrieved from <https://www.statista.com/statistics/1288072/coronavirus-apps-io-immuni-downloads-italy/>
- Li, T. C. (2021). Privacy in pandemic: law, technology, and public health in the Covid-19 crisis. *Loyola University Chicago Law Journal* 52 (3), 767-866.
- M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury and V. Muthukkumarasamy. (2020). COVID-19 contact tracing: Challenges and future directions. *IEEE Access*, vol. 8, pp. 225703-225729, doi: 10.1109/ACCESS.2020.3036718.
- Max S. Kim. (2020, March 6). South Korea is watching quarantined citizens with a smartphone app. MIT Technology Review.
- Melissa Rupert. (2021, January 22). 1 year on MySejahtera: Effectiveness examined. Snappy Mob Blog. Retrieved from <https://blog.snappymob.com/contact-tracing-apps-1-year-on-effectiveness-examined>
- MySejahtera Privacy Policy. Malaysia. [https://mysejahtera.malaysia.gov.my/privasi\\_en/](https://mysejahtera.malaysia.gov.my/privasi_en/)
- Opalyn Mok. (2020, December 4). Health Ministry source: MySejahtera covers 24.5 million users with up to 30,000 daily downloads despite misconceptions. Malay Mail.
- Prevention And Control of Infectious Diseases Act 1988, <https://www.ummc.edu.my/files/ethic/MCHRS/7%20Human%20Biological%20Materials/PREVEN~1.PDF>.
- Reuters Staff. (2021, May 23). French COVID tracing app downloaded by 25% of the population - Minister. Reuters.
- Ross Anderson. (2020, April 12). Contact tracing in the real world. Light Blue Touchpaper. Retrieved from <https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/>
- Sowmiya, B., Abhijith, V., Sudersan, S. et al. (2021). A survey on security and privacy issues in contact tracing application of Covid-19. *SN Computer Science* 2, (136), 1-11.
- Surviving Covid-19: M'sian man shares his Coronavirus experience. The Star. (2020, March 12).
- Syafiqah Salim. (2021, December 26). Govt introduces MySJ trace feature for Covid-19 close contacts tracing. The Edge Markets.
- Tim Starks. (2020, June 7). Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better. Politico. Retrieved from <https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601>



- TraceTogether Token. (2021, March 11). TraceTogether privacy safeguards. *A Singapore Government Agency Website*.  
<https://www.tracetgether.gov.sg/common/privacystatement/>
- Vokinger, K. N., Nittas, V., Witt, C. M., Fabrikant, S. I., & von Wyl, V. (2020). Digital health and the Covid-19 epidemic: an assessment framework for apps from an epidemiological and legal perspective. *Swiss Medical Weekly* 150, w20282.
- VoxEU. (2021). A cross-country comparison of contact-tracing apps during COVID-19. CEPR. Retrieved from <https://cepr.org/voxeu/columns/cross-country-comparison-contact-tracing-apps-during-covid-19>
- World Health Organization (WHO). (2017, May 1). Infection prevention and control: Contact tracing. Retrieved from <https://www.who.int/news-room/q-a-detail/contact-tracing>
- World Health Organization (WHO). (2020). Digital tools for COVID-19 contact tracing. Annex: Contact tracing in the context of COVID-19. [https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact\\_Tracing-Tools\\_Annex-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1)
- World Health Organization (WHO). (2020, June 2). Digital tools for COVID-19 contact tracing. Annex: Contact Tracing in the Context of COVID-19. Retrieved from [https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact\\_Tracing-Tools\\_Annex-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1)
- World Health Organization (WHO). (2020, May 28). Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim Guidance. Retrieved from [https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics\\_Contact\\_tracing\\_apps-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1)
- Zhang, B., Kreps, S., McMurry, N., & McCain, R. M. (2020). Americans' perceptions of privacy and surveillance in the Covid-19 pandemic. *Plos one* 15 (12), 1-16.



# THE IMPORTANCE OF CYBERSECURITY IN BUILDING CONSUMER FAITH IN MARKETING STRATEGY

Jyoti Jyoti\*

ORCID ID - 0009-0004-7103-7713

## *Abstract*

The protection of computer systems, networks, and data from harm, attacks, and unauthorized access is known as cybersecurity. It employs a range of devices, protocols, and techniques to safeguard data and fend off threats encountered online. Important objectives include protecting against online crimes like malware, phishing, and hacking as well as maintaining data availability, confidentiality, and integrity. As technology advances, cybersecurity becomes increasingly crucial to ensuring the dependability and safety of digital systems in a variety of sectors. Building and maintaining customer trust is essential as more and more people transact business online and reveal sensitive information. Businesses that prioritize effective cybersecurity practices with their data have a higher chance of earning the trust of consumers.

Open communication about cybersecurity precautions, adherence to data protection regulations, and timely handling of security-related incidents all contribute to the establishment and maintenance of consumer confidence. Customers may choose a company over competitors based on its reputation for protecting their personal information. A secure and trustworthy business-consumer relationship is built on the foundation of customer trust and cybersecurity in the digital realm. This study aims to evaluate the impact of cybersecurity measures on consumer trust in marketing strategies and explore the efficacy of current cybersecurity measures in fostering consumer trust in marketing campaigns. By addressing these objectives, the study hopes to provide insights that will help businesses manage the constantly evolving field of digital marketing with enhanced security, ensuring the loyalty of their customers.

**Keywords:** Cybersecurity, Consumer confidence, Marketing strategy, Digital trust, Brand integrity.

## **Introduction**

---

\* Research Scholar, Banaras Hindu University. E-mail- [Jyotibhu708@gmail.com](mailto:Jyotibhu708@gmail.com)



The internet has widened the world and created new challenges, but it has also made it more diverse and challenging. As cyber security has grown, so has the hacking world. Companies providing cloud computing are protected by cutting-edge encryption technology and safeguarding hardware, software, and data connected to the internet against cyberattacks. Both Businesses use both physical and cyber security to prevent unauthorized access to computer systems and data centers. Safety, which maintains Data availability, confidentiality, and integrity is a subset in terms of cyber security. Cybersecurity is a critical component of any business's or organization's infrastructure. To put it briefly, a business or organization that prioritizes cyber security can rise to great heights and enjoy a great deal of success, all thanks to its ability to defend client and private information from rivals.

Customers' and individuals' competitors' organizations are abusive. A business or organization must first and foremost offer this security in the most effective manner possible to grow and succeed (Rodríguez-deArriba et al., 2021). The concept of cybersecurity is the action of protecting data, systems, and computer networks from internet threats, loss, and harm. To safeguard information and ensure the privacy, availability, also integrity of digital resources, it includes various tools, rules, and controls. Cybersecurity is a generally used and complex topic with variable definitions that are often subjective and lackluster. The inability to define cybersecurity in a clear, widely accepted way that takes into account its complexity could hinder advancements in science and technology by supporting a primarily technical view and distinguishing between disciplines that should work together to tackle difficult challenges.

Technical solutions support cybersecurity, but they by themselves do not resolve the problem. Several instances and scholarly work demonstrate organizational, financial, interpersonal, governmental, and human-related issues which are closely linked to initiatives in cybersecurity. Fredrick Chang, former Director of Research at the National Security Agency, explains how cybersecurity is an interdisciplinary field (Craig et al., 2014). Security in the digital sphere comprises methods and technologies intended to safeguard networks, software, computers, and attack-related information, harm, or unapproved entry. Recently The field of cybersecurity has had significant technological change, driving data science this modification. Machine learning (ML), a core part of Artificial Intelligence (AI), has a crucial function in gaining knowledge from data. This technology possesses the capacity to greatly change the cybersecurity environment and is driving a novel paradigm in science.



Related technologies are growing in popularity. with the popularity among these domains increasing from 2014 saw fewer than thirty to over 70 in 2019, which is more than twice as popular as before (Sarker et al., 2020). The integration of technology and trust in marketing is known as cybersecurity, and it necessitates that companies safeguard client information, guarantee safe transactions, and guard against online attacks. In addition to protecting operations, this fosters trust, which is essential for customer loyalty and confidence in a data-driven market. Proactive steps taken to safeguard networks, data, and information from both internal and external threats are referred to as cybersecurity. Cybersecurity professionals protect servers, networks, intranets, and computer systems. Information is only accessible to those who are authorized thanks to cybersecurity (Ahmed Jamal et al., 2021). In an era where sophisticated marketing strategies and digital environments are dominating, the connection between cybersecurity and customer trust becomes critical.

Data security must be ensured as businesses rely more and more on technology to interact with their clients. The importance of cybersecurity in enhancing consumer trust in marketing tactics is examined in this study. In addition to safeguarding personal privacy, it examines how safeguarding sensitive data promotes trust, which is essential for effective brand engagement and longevity. Cybersecurity is the safeguarding of systems and information against different types of attacks, such as cyberterrorism, cyberwarfare, and cyberespionage. These threats can target military, political, and confidential assets. They are especially creative and challenging to counter in government and enterprise networks (P.S. et al., 2018).

## **Literature Review**

Given that networks are being used for vital transactions and that everything in the world is becoming more interconnected, computer security is an important concern. Cybercrime and information security are evolving, with new technologies and threats posing challenges for organizations. To secure their infrastructure and maintain intelligence, organizations must adopt new platforms and intelligence. While there is no perfect solution to cybercrimes, minimizing them is necessary for a secure future in cyberspace (Gade & Reddy, 2014). The rise of malevolent intelligence and online hazards necessitates advanced cybersecurity techniques. DDoS prevention has shown that smart approaches can protect against significant





threats with little funding. Neural networks with artificial intelligence provide the most relevant discoveries for cybersecurity, with implementations continuing in fields like decision support, situation understanding, and information control.

Expert machine development is particularly interesting in this scenario, as the speed of general artificial intelligence advancements is unknown. However, the potential for perpetrators to exploit new forms of AI remains. The latest technology in computer learning could significantly improve systems' cybersecurity capabilities, particularly in understanding, interpreting, and managing information (Das & Sandhane, 2021). Several studies explained the future of cybersecurity will be complex and limitless as digital skills interact with humans across various aspects of society, family, and the environment. The project aims to predict that cybersecurity will become the "master problem" of the internet era, with major changes to how humans and digital machines interact. The objective is to anticipate the ups and downs that could arise from these changes, as change often occurs faster than expected additionally, it is easier to imagine downside risks than advantages.

This will prompt extensive thinking and policy proposals, allowing for more detailed and targeted solutions (Sheth et al., 2021). the assessment of cybersecurity-related behaviour, focusing on RQ3. The research consists of three parts: analysis, measurement scale, and data collection. Subjective data is collected more than objective data, with online self-assessment questionnaires (SAQ) being the greatest prominent technique. Researchers frequently modify measurement scales by drawing on previously published literature. The most commonly used questionnaire is HAISQ. In some articles, PLS analysis is the most commonly used technique. However, the self-assessment approach may yield skewed results highlighting the requirement for future research to address this issue. The following inquiry for research if there are distinctions between an employee's and a manager's behaviour, was not satisfactorily addressed.

Some articles provide insights but not conclusive answers, highlighting the significance of improving cybersecurity culture in organizations. Future studies ought to incorporate workers and administration from the same company, requiring greater organization and preparation than simply posting a survey online. Anonymization of personal data is crucial, and it's





necessary to reduce the chance of biased answers. Hybrid methods, such as surveys for self-evaluation and phishing attempts, can become accustomed to collecting objective and subjective data. Comprehensive data collection within a national market or section is also recommended since context-based research on compliance is dependent (Kannelønning & Katsikas, 2023). A comprehensive framework for implementing Cyber Threat Intelligence (CTI) through a literature review. Key components, like information collection, handling, evaluating, and sharing are identified.

The structure can guide organizations in improving their CTI capabilities and act as a template for additional research. The importance of collaboration between stakeholders, such as government representatives, law enforcement organizations, and cybersecurity specialists in thwarting cyber threats. By assembling specialists, organizations can quickly identify emerging threats. Subsequent research could examine How businesses can customize their CTI implementation method based on its specific Resources and requirements and how to navigate legal and regulatory constraints while fostering stakeholder collaboration (Saeed et al., 2023). The rapid advancement of technology has resulted in digital global information and data being kept online, impacting various aspects of life. The idea behind cyber security is crucial for the development of Internet services and information technology.

Internet attacks are expected to rise in 2021-22, not only from individual hackers however, from nation-state actors as well attempting to obtain information from establishments and authorities. As there are no boundaries in cyberspace maintaining it has become increasingly difficult. As attacks become more innovative, it is essential to define and define what makes up good security on the internet. A technology called cyber security is used to safeguard data and information networks stored on digital devices. This work provides a thorough evaluation of the background of cyber security and different kinds of internet threats. It investigates the numerous types of cyber threats and goes over the classification of cyber attackers. The condition or procedure of protecting and restoring networks, gadgets, and programs anywhere type Cybersecurity is the defense against cyberattacks (Perwej et al., 2021). Cybersecurity involves protecting networks, hardware, software, and information from harm, theft, or illegal access.



Infrastructure and the digital economy have led to a notable rise in cyberattacks, with grave repercussions. The evolution of linked nation-state adversaries additionally the sophistication of cyberattacks are driving a rise in the quantity, intensity, and effect of cyberattacks. cybersecurity powered by intelligence is needed to offer dynamic defence combating ever evolving cyberattacks and handling large data. advisory groups like the National Institute of Standards and Technologies (NIST) encourage proactive and flexible methods, like data-driven analysis and real-time assessments, to prevent future security incidents. Kaur et al., 2023 study analyzed 236 original research projects from 2395 comparable publications from the Scopus database for more than 13 years (2010-2022). It discussed the various AI methods used in cybersecurity as well as the cybersecurity actions that profited from artificial intelligence technology.

The study analyzed the taxonomy of AI in cybersecurity, regularity of release by year, location, kind of cybersecurity contribution, and kind of AI technique employed. The examination showed that while the number of Publications is growing, so it's important to focus more on gathering and presenting historical data about various cybersecurity functions. His study's main contribution is how primary studies are categorized., integrating the condition of writing and understanding the importance of AI in the defense of cybersecurity. It also suggests directions for future studies to tackle new problems for effective AI adoption (Kaur et al., 2023). The risks of cyber threats, including common threats and the effects of cyberattacks on customer data and financial fraud, are growing for the US banking industry.

Safeguarding consumer information, stopping financial fraud, and upholding confidence in the digital financial ecosystem all depend on effective cybersecurity procedures. The regulatory framework, which consists of regulations from agencies like the FDIC and OCC as well as statutes like the Gramm-Leach-Bliley Act, is primarily responsible for enforcing these measures. A successful cybersecurity strategy must include risk assessments, security control implementation, incident response and recovery procedures, and staff training. To protect consumer data, it is essential to prioritize data privacy, implement data handling and classification protocols, ensure that data is transferred and stored securely, and make use of encryption and tokenization techniques. Financial fraud must be avoided by having a thorough understanding of common fraud schemes, implementing fraud detection and



prevention techniques, keeping an eye on transactions, and employing anti-money laundering measures.

Two examples of new cyber-security trends and technologies that offer fresh approaches to fortify defenses and keep ahead of evolving threats are artificial intelligence and machine learning. Industry best practices and collaborative approaches boost the efficacy and resilience of cyber-security strategies (Efijemue et al., 2023). Wahab et al., 2023 investigated Thai customers' inclination to purchase through e-commerce platforms using the Theory of Planned Behavioral (TPB). An online survey was used to test the model, which takes into account perceptions of cybercrime, internet medium, trust in online vendors, and TPB. The Findings indicated that trust in online vendors, internet mediums, cybercrime perception and subjective standards did not considerably impact the purchasing intentions of consumers. As of yet, cybercrime has no direct effect on behaviour attitudes.

However, customer attitudes regarding actions and perceptions of behavioral controls are useful markers of what they plan to purchase when using e-commerce technology. The study suggests that e-commerce businesses should include security measures to lessen weak points and increase users' faith in the system. However, the study's predictive power is only about 50% due to the limited number of respondents and the lack of focus on respondents' characteristics and cultural impact (Wahab et al., 2023). Utilizing digital media is part of digital marketing technology to achieve marketing objectives, but it requires a specific skill set to operate safely in cyberspace. The advancement of technology offers both opportunities and difficulties facing marketers. Towards achieve success in the online marketplace, marketers must understand the advantages and restrictions concerning digital marketing strategies, additionally to the risks associated with them.

Hackers are knowledgeable and familiar with the terrain, so they constantly develop sophisticated software to steal information. To ensure security, social media websites, payment gateways, and online platforms should all have necessary protections in place, and observing sites for trespassing or suspect behaviour is crucial. Integrating security measures for digital marketing campaigns is necessary for a successful digital marketing strategy (Konyeha, 2020). Several research on cybersecurity databases and cyber risk reveal that the majority of datasets are employed within the detection of intrusions as well as machine learning, with less representation of cyber risks. The ever-changing landscape of cyberspace



risk makes stakeholders in cyber insurance challenged to assess and understand it. To assist researchers studying cyber risk and cyber insurers in risk management, a higher density of cyber data is required.

Enforcing mandatory reporting of cyber incidents could enhance insurers' and businesses' comprehension, awareness, and loss prevention of cyber incidents. Because of the data's accessibility, cyber risks can be comprehended more fully, allowing researchers to investigate these risks more thoroughly. Businesses can apply this actual understanding to their corporate ethos to lower the risks of cyberattacks, supporting long-term risk-based pricing. From fresh data, common definitions of cyber risks could be developed, and the databases related to cybersecurity summarized and categorized in this study could offer an alternative viewpoint regarding cyber threats, enabling the creation of uniform terminology for use in cyber policies. It also helps raise corporate behaviour and risk awareness, providing the scientific community with a thorough overview of peer-reviewed datasets and additional datasets in the field of cybersecurity and cyber risk.

Future work should focus on improving the cybersecurity and cyber risk datasets' adaptability and integrability, identifying machine-readable cybersecurity datasets, and ensuring that concrete benchmarks can be applied because of the absence of publicly available datasets (Cremer et al., 2022). The increasing reliance on Information and Communication Technology (ICT) in our day-to-day existence has made cybersecurity a crucial area of concern. However, the ethereal quality of cybersecurity, its social-technical dependencies, and the unclear effects of conflict make it a difficult field for decision-makers. Message framing is a tactic used to communicate difficult problems effectively, but simple frames are not effective. It's essential to frame messages using evidence. for cybersecurity, as it helps to comprehend the main arguments and avoids easy challenges.

Six strategies for framing cybersecurity include not exacerbating it, revealing villains, putting heroes in the spotlight, relating values to cybersecurity beyond security, identifying the message personally for simple recognition, and connecting to more concrete problems. Framing a message is important not just in cybersecurity, but also in numerous areas of government data, such as personal files, privacy use, data, public-private systems, Internet



governance, and identity management opening. Cybersecurity specialists, scholars and decision-makers need to encapsulate their messages well to prevent confusion and ambiguity. enhancing capability through the government as well as additional study on empirically supported framing techniques and their effectiveness is required (de Bruijn & Janssen, 2017).

### **Research Objectives**

1. To explore how cybersecurity measures affect consumers' trust in marketing tactics.
2. To examine how well the cybersecurity procedures in place are doing to build consumer trust in marketing initiatives.

### **Research Question**

1. In what ways do cybersecurity measures either strengthen or weaken consumer trust in marketing tactics?
2. How closely do modern cybersecurity procedures match marketing expectations from consumers?

### **Methodology**

This research study uses a descriptive approach and is qualitative to examine the role of cybersecurity in enhancing consumer confidence in marketing strategies. Descriptive research focuses on describing an observation and its features, often using survey and observational instruments. Although data can be gathered qualitatively, statistical analyses are frequently used to analyze data quantitatively. With a richer collection of data from multiple sources, qualitative research takes a more comprehensive approach to understanding individual participants, including their opinions, perspectives, and attitudes. Understanding and evaluating the relationships between variables requires the use of both kinds of research (Nassaji, 2015). In order to give a thorough grasp of the relationship between cybersecurity measures and customer trust, the study makes use of content analysis and secondary data. Secondary data are derived from research papers and review articles. An overview of cybersecurity's growing importance in the digital realm and how it influences marketing strategies is given in the study's first section. After that, the study offers a comprehensive literature review that details the deliberate process for selecting and obtaining secondary data.

### **Finding**



According to the study, there is a strong correlation between consumer confidence and companies' adoption of cybersecurity best practices. Consumers who see a company's commitment to protecting their data and ensuring secure transactions are more likely to believe in it. Customers' perceptions of strong cybersecurity policies are more consistent and trustworthy, which has a significant influence on their purchasing decisions. Customers lose faith in the affected brands as a result of cyberattacks and data breaches, which damages their reputations. Developing consumer confidence requires openness and communication. When brands are open about their security protocols and respond promptly to security incidents, customers are more likely to view them favorably. Additionally, the study highlights the need for ongoing consumer education and awareness campaigns regarding cybersecurity risks and best practices.

Trust seals and certifications demonstrating conformity to industry standards have a positive effect on consumer trust. The public views companies with these credentials prominently in their marketing materials as more dependable and trustworthy. The study found a clear correlation between strong cybersecurity procedures and increased consumer trust in marketing strategies. Customers now place a higher value on the security of their personal data, as evidenced by the significant increase in consumer confidence in businesses that implemented comprehensive cybersecurity measures. Nonetheless, the study did demonstrate how different cybersecurity practices are amongst businesses, with some having excellent practices and others not having any. This highlights the need for a uniform and stringent approach to cybersecurity across industries in order to ensure ongoing trust-building in marketing initiatives.

## **Conclusion**

In order to foster consumer trust in marketing strategies, the study emphasizes the significance of cybersecurity protocols. It suggests that businesses can gain a competitive edge by cultivating client loyalty and trust, prioritizing cybersecurity, and being transparent about their efforts. However, the consequences of data breaches highlight the need for continued cybersecurity investment to maintain customer confidence and reduce potential reputational harm.. Additionally, the study highlights the positive relationship that exists between customer trust and cybersecurity protocols, providing valuable insights that businesses can utilize to enhance their marketing outreach. Despite the implementation of



various cybersecurity protocols, there is still a significant lack of success in converting these efforts into tangible advantages.

Consumers' concerns about the security and integrity of their data are still being expressed during marketing interactions, suggesting that there is a mismatch between the actual confidence that customers have been given and the perceived level of security that companies are communicating. The study emphasizes how important it is for businesses to prioritize communication plans that demonstrate their dedication to safeguarding client data and to making investments in robust cybersecurity infrastructure. The study highlights how important consumers' trust in marketing strategies is influenced by the internet. Businesses that prioritize cybersecurity and succeed in doing so will find it easier to gain and maintain the trust of their clients. In order to foster long-lasting relationships between businesses and their clients, increase consumer trust, and create a safe environment for marketing campaigns, it is imperative that stakeholders collaborate to enhance cybersecurity protocols.

## Reference

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4, 13–21. <https://doi.org/10.22215/timreview/835>

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. <https://doi.org/10.1016/j.giq.2017.02.007>

Das, R., & Sandhane, R. (2021, July 1). Artificial Intelligence in Cyber Security. *Journal of Physics: Conference Series*, 1964(4), 042072. <https://doi.org/10.1088/17426596/1964/4/042072>

Efijemue, O., Obunadike, C., Olisah, S., Taiwo, E., Kizor, S., Odooh, C., & Ejimofor, I. (2023). Cybersecurity Strategies For Safeguarding Customers Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal of Soft Computing*, Vol. 14, No.3. <https://doi.org/10.5121/ijsc.2023.14301>

Gade, N. R., & Reddy, U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies.





Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behaviour has been assessed. *Information & Computer Security*, 31(4), 463–477. <https://doi.org/10.1108/ICS-08-2022-0139>

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>

Konyeha, S. (2020). Exploring Cybersecurity Threats in Digital Marketing. *NIPES Journal of Science and Technology Research*, 2, 12. <https://doi.org/10.37933/nipes/2.3.2020.2>

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egy.2021.08.126>

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research*, 19, 129–132. <https://doi.org/10.1177/1362168815572747>

Perwej, Dr. Y., Abbas, Q., Dixit, J., Akhtar, N., & Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, Volume 9, Pages 669-710. <https://doi.org/10.18535/ijstrm/v9i12.ec04>

P.S, S., Sundaresan, N., & M, S. (2018). Overview of Cyber Security. *IJARCCCE*, 7, 125–128. <https://doi.org/10.17148/IJARCCCE.2018.71127>

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, 23(16), 7273. <https://doi.org/10.3390/s23167273>

Sarker, I., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from a machine learning perspective. *Journal of Big Data*, 7. <https://doi.org/10.1186/s40537-020-00318-5>

Sheth, M., Bhosale, S., Kurupkar, M., & Prof, A. (2021). Research Paper on Cyber Security. 2021.

Wahab, F., Khan, I., Kamontip, Hussain, T., & Amir, A. (2023). An investigation of cyber attack impact on consumer's intention to purchase online. *Decision Analytics Journal*, 8, 100297. <https://doi.org/10.1016/j.dajour.2023.100297>

White, M., & Marsh, E. (2006). Content Analysis: A Flexible Methodology. *Library Trends*, 55. <https://doi.org/10.1353/lib.2006.0053>





**OPINIONS / YORUMLAR**



# TRANSHÜMANİZMİN AHLAK AÇMAZI

**Bilal SAMBUR\***

## **Giriş**

Transhümanizm, günümüzde etkili bir felsefi ve kültürel yaklaşım konumundadır. Julian Huxley'in transhümanizm kavramını ortaya attığından beri, bu felsefi ve kültürel fikir ve yaklaşım tartışılmaktadır. Transhümanizm, yirmi birinci yüzyılın en baskın ve çekici düşünsel ve kültürel yaklaşımlarından biri olmaya adaydır. Transhümanizm kavramı, hiçbir şekilde posthümanizm kavramıyla özdeşleştirilmemeli veya karıştırılmamalıdır. Transhümanizm, hümanizmi aşan, ancak hümanizm sonrası olan bir yaklaşımı ifade etmemektedir. Transhümanizmde, insan sonrası bir durum yoktur. İnsanın mevcut biyolojik ve zihinsel yapısının teknolojiyle güçlendirilip daha güçlü bir insani varlığın meydana getirilmesi amacı vardır. Teknolojiyi ve bilimi savunan transhümanizm, insanın güçlendirilmesini, insan ve makine birleşimiyle yeni bir hayat formunu öngörmektedir. Gelecekte makine ve insandan oluşan yeni insanın, fiziksel ve psikolojik açılardan daha sağlıklı, zeki ve güçlü olacağı tahmin edilmektedir. Transhümanizmde aşılacak istenen insan değil, insanın biyolojik ve zihinsel sınırlılıklarıdır. Transhümanizm sürekli olarak değişimin ve yeniliğin peşindedir. İnsana ve doğaya dair bütün bilginin sürekli olarak değerlendirilmesi, eleştirilmesi ve yeni bilgilere ulaşılması, transhümanizmin olmazsa olmazıdır. Transhümanizm, insanlığa, doğaya ve topluma dair bilginin sürekli olarak değiştiği ve geliştiği kabulünü esas almaktadır. Transhümanizm, hümanizme ve bilimsel bilgiye değer veren, ancak bu anlayışların sürekli olarak yenilenmesini esas alan felsefi, kültürel ve teknolojik bir yaklaşımdır.

## **Teknoloji ve Transhümanizm**

Transhümanizm, insanın biyolojik ve zihinsel yaşam biçimlerini çok sınırlı ve zayıf görmektedir. Mevcut sınırlı yaşam formlarının bilim ve teknoloji yardımıyla güçlendirilmesi ve yenilenmesi, transhümanizmin en temel amacıdır. İnsanın biyoteknolojik olarak güçlendirilmesi, transhümanizmin temel iddiasıdır. İnsanın biyolojik ve zihinsel hayatının maksimum düzeyde devamlılığının sağlanması, transhümanizmin en asli arzusudur. Transhümanizm, hayatı esas alan bir felsefedir. Akli, bilimi ve teknolojiyi kullanarak insani durumun daha iyi hale getirilmesini, yaşlılık ve hastalık gibi kısıtlayıcı ve zor süreçlerin

\* Prof.Dr., Department of Psychology, Yıldırım Beyazıt Üniversitesi. E-mail: samburbilal@gmail.com



neden olduğu kısıtlamalar ve çaresizlikler karşısında insanın entelektüel, fiziksel ve psikolojik kapasitesinin arttırılmasının, güçlendirilmesinin ve dayanıklılığının arttırılmasını arzulayan transhümanizm, hayatı esas alan, hayatı amaçlayan ve hayata yatırım yapan entelektüel ve kültürel bir perspektiftir. Dinler, ölüm sonrası esas alırken, transhümanizm hayatı esas almaktadır. Bir hayat felsefesi olarak transhümanizm, anlamlı ve ahlaklı bir hayatın akıl, bilim ve ilerleme ışığında gerçekleştirilebileceğini öngörmektedir. Transhümanizmde ahlaklı ve anlamlı bir hayat yaşamak için, kimseye tapmaya, inanmaya ve doğaüstü kurgular uydurmaya gerek yoktur. Birey, boş inançlarla, dualarla, yalvarmalarla ve beklentilerle daha iyi bir hayata sahip olamaz. Birey akli, teknolojiyi, bilimi ve yaratıcılığını kullanarak kendisi için arzuladığı gelişmiş, sağlıklı ve güçlü bir hayatı mümkün hale getirebilir. Transhümanizmin gelişen bir yaşam kültürüne insanlığın ihtiyaç duyduğu saptaması, çok yerinde ve önemlidir. Hayat kültürünün zayıfladığı, ölüm kültürünün yüceltildiği bir çağda yaşama kültürünün geliştirilmesinin öne alınması, insanlık bilincini uyandırmada önemli bir ahlaki uyarıcı işlevi görebilir.

Bilimi, akli, teknolojiyi kullanarak hastalık, yaşlılık ve ölüm karşısında daha iyi ve gelişmiş bir hayatın ve varoluşun mümkün olduğunu öngören transhümanizm, insan hayatında ahlakın olması gerektiği gerçeğinin, bilim ve teknolojinin ahlak dışı yollar için kullanılması gibi önemli tehlikelerinde farkındadır. Yarar sağlamak ve faydalı olmak, her zaman zarar vermekten daha zordur. Bilimsel ve teknolojik imkanları kullanarak çok küçük bir grup, geniş insan gruplarına çok büyük zararlar verebilirler. Kitlesele imha silahlarına sahip olan fanatik, ırkçı veya cinsiyetçi bir haydutlar grubu, insanlığa karşı suçlar ve soykırımlar gerçekleştirebilir. İleri teknolojik ve bilimsel araçlar, insanın yıkım kapasitesini dehşet düzeye çıkaran araçlar olarak kullanılabilir. Biyolojik silahlar, nükleer ve kimyasal silahlardan daha tehlikeli hale gelmiş durumdadır. Geliştirilecek ölümcül bir virüs ile milyonlarca insanın ölümü sağlanabilir. Biyolojik saldırı, kimyasal ve nükleer saldırıdan daha kolay ve etkili bir araç haline gelmiş durumdadır. Transhümanizm, bilimin ve teknolojinin insanlığa karşı bir yok etme aracı olarak kullanılmasına karşıdır. Bilim ve teknoloji istismarı, insanlığın önünde ciddi bir ahlaki sorun ve meydan okuma olarak durmaktadır.

### **Ahlaki Kaygılar**

Bilimin ve teknolojinin istismar edilmesine karşı çıkmakla birlikte transhümanizmin merkezinde ciddi bir ahlaki sorun bulunmaktadır. Transhümanizm, hayatı canlı olmayan teknolojik aletlerle korumayı, sürdürmeyi ve devam ettirmeyi amaçlamaktadır. İnsan



vücudundaki canlı parçaların cansız metal parçalarıyla değiştirilmesi aslında insanın biyolojik ve psikolojik açılardan hayattan arındırılması anlamına gelmektedir. İnsanın biyolojik ve zihinsel sınırlılıklarını ve eksikliklerini giderme adına daha güçlü teknolojik araçların insan vücuduna yerleştirilmesi, hayatın zayıflamasına veya yok olmasına neden olabilir. Hayatı güçlendirmek, korumak ve geliştirmek, transhümanizmin en asli ahlak prensibidir. İnsanın biyolojik ve zihinsel varlığına teknolojik olarak yapılacak olan müdahaleler yoluyla canlı olanın yerine cansız şeylerin konması sonucu hayatı ortadan kaldıracak başedilemez bir tehlikenin ortaya çıkma ihtimali, transhümanizmin içinde derin bir ahlaki açmazın oluşmasına neden olmaktadır.

Transhümanizmin en büyük ahlaki açmazı, insan olmanın bizzat kendisine, insan türünün bir mensubu olmaya ahlaki bir değer atfetmemesidir, çünkü transhümanizme göre türçülüğün hiçbir ahlaki değeri yoktur. Bir insan ile robot arasında hiçbir fark yoktur. İnsan olmanın bizzat kendisini ahlaki olarak değerli görmeyen transhümanizm, insanın biyolojik, psikolojik ve rasyonel kapasitelerinde değerli görmemekte, onlara müdahale etmeyi ahlaki açıdan meşru görmektedir. Acıyı, mutluluğu, sevgiyi, nefreti, umudu, umutsuzluğu, neşeyi, coşkuyu kendisiyle tecrübe ettiğimiz biyolojik varlığımıza müdahale edilebilmekte, değiştirilebilmekte veya ortadan kaldırılabilir. 49

İnsan olmanın bizzat kendisini değerli kabul etmeyen transhümanizm, bireyin insan haklarına müdahale etmekte ahlaki açıdan bir sorun görmemektedir. Biyolojik, psikolojik ve zihinsel varlığımıza teknolojik yollarla yapılan müdahaleler, aslında insanın yaşam hakkına, insan onuruna ve bireysel özgürlüklere müdahale anlamı taşımaktadır. Transhümanizm, insanın insan haklarına müdahale yolunu açtığı için ahlaki açıdan ciddi sorunlar barındırmaktadır. İnsanın insan olarak değerinin ve geleceğinin olmasının bir zorunluluk ve gereklilik olmadığına bizi inandırmaya ve ikna etmeye çalışan transhümanizm, ahlaki açıdan çok zayıf bir felsefi ve kültürel yaklaşımdır.

## **Sonuç**

İnsanın gelişimi, sadece rasyonel ve fiziksel olarak güçlendirilmesinden ibaret değildir. Güçlü ve gelişmiş bir insan olmak için, zihinsel yeteneklerimiz kadar duygularımızda önemli rol oynamaktadır. Transhümanizm, gelişmiş bir hayat için gerekli olan duygulara yeterince vurgu yapmamaktadır. Beynimizi mantıklı bir makine olarak hayal etmek veya bedenimizi teknolojik aletlerle güçlendirmek, bizi yeterince gelişmiş, sağlıklı veya mutlu yapmayabilir.



İnsan, düşünceli olduđu kadar, duygulu ve duyarlı bir varlıktır. İnsanın bizzat insani varlığını bedeniyle ve psikolojisiyle birlikte tamamen medikalize etmek, insanı üzerinde çalışılacak bir et yığımına indirgemek, ahlaki açıdan kaygı verici bir durumdur.



# SOSYAL MEDYA EKSENİNDE İFADE ÖZGÜRLÜĞÜ

Fatma Tuba SOYDOĞAN

ORCID-ID: 0009-0001-7796-5930

## Öz

Bu çalışmanın temel amacı sosyal medya ekseninde ifade özgürlüğü konusunun tüm yönleri ile ele alınarak, detaylı bir şekilde incelenip değerlendirilmesidir. Bu bağlamda bireylerin özgür bir şekilde paylaşım yapıp yapmadığı, paylaşım yaparken sonrasında başına bir şey gelmesinden korkup korkmaması ve paylaşımlarını kısıtlamalar altında mı yaptığı hususu çalışmamızın ana sorunu oluşturmaktadır. Bununla birlikte sosyal medya söylendiği kadar özgür bir platform mu, ifade özgürlüğü dediğimiz kavram sadece bir kavramdan mı ibaret, sosyal medya ekseninde yaşanan suçlar ve çözüm yolları nelerdir? Sorularının cevaplarını aradığımız ve nitel araştırma yöntemlerinden yararlanarak ortaya koyduğumuz incelemeler ve örnekler ışığında çalışma kapsamı ortaya konulmuştur. Bu kapsamı ortaya koyarken öncelikle geleneksel medya ve yeni medya arasındaki farkları ele alacağız. Ardından sosyal medya konusunu detaylı şekilde inceleyeceğiz. Sonra ifade özgürlüğü ve sosyal medya ekseninde ifade özgürlüğünü ele alacağız. Son olarak ise sosyal medya yasası ve Türkiye’de sosyal medya yasası başlıkları altında bahsi geçen yasaları inceleyerek çalışmamızı nihayete erdireceğiz.

**Anahtar Sözcükler:** Sosyal medya, ifade özgürlüğü, sosyal medya yasası

## ABSTRACT

The main purpose of this study is to examine and evaluate in detail the issue of freedom of expression in all its aspects in the context of social media. In this context, the main problem of our study is whether individuals can share freely, whether they are afraid of something happening to them afterwards, and whether they share their shares under restrictions. However, is social media as free a platform as it is said to be, is the concept of freedom of expression just a concept, what are the crimes occurring in the axis of social media and their solutions? The scope of the study has been revealed in the light of the studies and examples that we have searched for answers to the questions and put forward by using qualitative research methods. While presenting this scope, we will first discuss the differences between traditional media and new media. Then we will examine the issue of social media in detail. Then we will discuss freedom of expression in the context of freedom of expression and



social media. Finally, we will conclude our study by examining the topics of social media law and social media law in Turkey.

**Keywords:** Social media, freedom of expression, social media law

## Giriş

Türkiye Cumhuriyeti anayasasının 2. bölümünde yer alan kişinin hakları ve ödevlerini kapsayan 25. ve 26. maddelerinde görüldüğü üzere herkes, düşünce ve kanaat hürriyetine sahiptir.<sup>3</sup>

*“Madde 25 – Herkes, düşünce ve kanaat hürriyetine sahiptir. Her ne sebeple ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce kanaatleri sebebiyle kınanamaz ve suçlanamaz.”*

*Madde 26 – Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.”<sup>4</sup>*

Bu çalışma kapsamında 25. maddeyi ifade özgürlüğü başlığı altında incelemeye tabi tutulacaktır. Bununla birlikte 26. maddeyi ise hem medya hem de sosyal medya üzerinden fikir beyanı yapmakta özgürlüğü kapsayan temel bir madde olarak ele alacağız.

İfade özgürlüğü demokratik toplumun yapı taşlarından birisidir. Birbiri ile ilişkili bu iki kavramın sosyal medya ekseninde herhangi bir değişim söz konusu değildir. Lakin ne yazık ki günümüzde sosyal medya ve ifade özgürlüğü konuları oldukça tartışmaları süreçlerden geçmektedir. Zira oluşturulan yasalar ile de ifade özgürlüğü oldukça kısıtlanmış ve neredeyse ifade özgürlüğü diye bir kavram ortada kalmamıştır. Bunun sonucunda ise şunu belirtmek gerekir ki demokratik bir ortam da yoktur.<sup>5</sup>

<sup>3</sup>T.C. 82 Anayasası,

<https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/illeridaresi/Mevzuat/Kanunlar/Anayasa.pdf>

<sup>4</sup>T.C. 82 Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>5</sup>Faik Uyanık, “Sosyal Medya Kurgusalılık Ve Mahremiyet”, 7 Mayıs 2013 tarihli Kocaeli Üniversitesi Yeni Medya Kongresinde sunulmuş bildiridir. s.8.





Çalışma kapsamında ele alınan sosyal medya ekseninde ifade özgürlüğü konusunu anlamak için öncelikle sosyal medyayı içerisine alan yeni medya kavramını ele alınacaktır. Bununla beraber yeni medya ile geleneksel medya arasındaki farkları ele alarak bu çalışmanın önemini ortaya konulacak. Bu bağlamda kısaca bu iki medya türünün tanımı ele almakta fayda olacaktır. Geleneksel medya; televizyon, radyo, gazete ve dergiler gibi kitle iletişim araçlarını içerisine alan medya türüdür. Yeni Medya ise 20. yüzyılın ikinci yarısında sürekli gelişmekte olan dijital teknolojinin getirmiş olduğu yeniliklerle ortaya çıkan bir kavramdır ve internet üzerinden erişimin sağlandığı bir yapıdadır. Bu medya türü sosyal medya platformlarını, blogları, video paylaşım sitelerini kapsamaktadır.

İki medya türü arasındaki farkları ele aldıktan sonra *Sosyal Medya* nedir, bizim için neden önemlidir detaylı bir şekilde ele alınacak. Kısaca sosyal medya, insanların birbirleriyle etkileşimde buldukları, istedikleri zaman istedikleri yerden katılım sağlayabilecekleri, çoğu zaman ücretsiz kullanıma sahip, her yaşta bireylerin özgürce ulaşım sağlayabildiği çevrimiçi platformlardır.

Sosyal medyayı detaylı olarak ele aldıktan sonra ise *İfade Özgürlüğü* başlığı ile bu konuyu detaylandırılacak. Kısaca ifade özgürlüğü, bireylerin düşüncelerini özgürce yazılı ya da görsel fark etmeksizin ortaya koyabilmesi durumudur.

Tek tek başlıklar altında detaylandırılan konular ise *Sosyal Medya Ekseninde İfade Özgürlüğü* başlığı ile toparlayıp çalışmanın ana teması ortaya konulacaktır. Son olarak ise *Sosyal Medya Yasası Ve Türkiye’de Sosyal Medya Yasası* başlıkları altında bu yasaların içeriği ele alınarak incelemeye tabi tutulacaktır. Bahse konu olan yasalardan kaynaklı olarak çalışmamız kapsamında üzerinde durmuş olduğumuz sosyal medyada ifade özgürlüğünün olmaması konusunda çalışmanın örneklik boyutunu ele alıp sonuç kısmı ile çalışma nihayete erdirilecektir.

Çalışma araştırma yöntemi bakımından nitel araştırmaya tabidir. Nitel araştırma bağlamında gözlem yöntemi ile çalışma kapsamında ele alınan örneklerin durumu ve sürecinin takibi yapılmıştır. Yazılı doküman analizi ile literatürde konuya ilişkin yer alan makaleler incelenmiştir. Odak grupları ile çalışma konusunun tartışıldığı programlardan faydalanılmıştır. Örnek olay araştırması ile konya ilişkin örnekler değerlendirmeye tabi tutulmuştur. Televizyon programlarında yapılan konuya ilişkin konuşmalar ve Youtube



kanallarında yer alan programlarda konuya ilişkin yapılan değerlendirmeler ile medya analizi yapılmıştır. Haber sitelerinin metinleri incelenerek ise konuya ilişkin metin analizi yapılmıştır. Tüm bu kullanılan yöntemler neticesinde toplanmış olan veriler incelenerek çalışma konusunun genel itibarıyla sosyal medya ekseninde ifade özgürlüğünün olmadığı yönünde ilerleyecek olduğu çalışma kapsamında görülecektir.

## Geleneksel Medya ve Yeni Medya Arasındaki Farklar

Geleneksel medya ve yeni medya arasındaki farkları ele almadan önce kısaca teknolojinin gelişimine biraz değinmekte fayda vardır. Zira teknolojinin gelişimi ile toplumun iletişim biçimlerinde de değişiklikler yaşanmıştır. Geleneksel medya ve yeni medya kavramları bu değişiklikler kapsamında anlam kazanmıştır.<sup>6</sup> 1946'da bilgisayarın icat edilmesinden,<sup>7</sup> Yapay zekanın ortaya çıkmasına kadar geçen süreçte birbirini takip eden teknolojik gelişmelerle birlikte hayatımıza birçok yeni araçlar ve kavramlar dahil olmuştur. Bu süreç içerisinde hayatımıza internet ve beraberinde internet erişimi kavramı dahil olmuştur.<sup>8</sup> Gelişim serüveni devam eden medyanın, gelenekselden yeniye geçiş noktasında en ayırt edici özellikleri bu iki kavrama bağlıdır. Zira geleneksel medya ve yeni medya arasındaki en belirgin fark iletişimin yönüdür. Geleneksel medya tek yönlü olup sadece vericiyen yeni medya çift yönlüdür ve alışveriş sağlanan bir medya türüdür.<sup>9</sup>

Geleneksel medya televizyon, radyo, gazete ve dergiler gibi kitle iletişim araçlarını içerisine alan medya türüdür. Geleneksel medya türünde iletişim tek yönlüdür ve etkileşim sınırlıdır.<sup>10</sup> Burada tabiki radyo yayınlarına katılım sağlama gibi durumları göz önüne alırsak geleneksel medyada da iletişimin tek yönlü olması konusu tartışılır hale gelecektir. Fakat iletişim tam zamanlı olarak çift yönlü olmadığından ötürü ve herkesin eşit olarak katılım sağlamadığını göz önüne alarak genel anlamda iletişim tek yönlüdür demek mümkün olacaktır. Bunun dışında ise gelecek paragrafta ele alınacak konuda daha detaylı olarak görüleceği üzere

<sup>6</sup>Nezir Akyeşilmen, *Siber Politika ve Güvenlik*, Ankara: Orion Kitabevi, 2018, s. 25.

<sup>7</sup>Mustafa Bostancı, *Sosyal Medya Dün, Bugün, Yarın*, Konya: Palet Yayınları, 2019 s.14.

<sup>8</sup>Bostancı, *Sosyal Medya Dün, Bugün, Yarın*, s.11.

<sup>9</sup>Bostancı, 2019, s.14.

<sup>10</sup>Cihan Çıldan, Mustafa Ertemiz, Evren Küçük, H. Kaan Tumuçin, Duygu Albayrak, "Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü", Akademik Bilişim Konferansı, 2012, s.3.



geleneksel medya Web 1.0 kapsamında değerlendirildiği için tek yönlü iletişim söz konusudur.

Geleneksel medya web 1.0 kapsamında değerlendirilmektedir. Tim Berners-Lee tarafından icat edilen<sup>11</sup> web 1.0 hipermetin'lerden oluşmaktadır ve kullanıcılar genel itibariyle okur konumundadır. Kullanıcı sayısı yeni medya ortaya çıktıktan sonra ona göre daha az bir durumda değerlendirilmektedir. Web 1.0'da internet tek yönlü bir bilgi aktarımı yapan ekosisteme sahiptir. İçeriğin üretiminden dağıtımına kadar olan süreçte tamamen kurumların kontrolünde olan bir yapı hakimdir. Geleneksel medyada içerik, geniş kitlelere ulaşmak üzere tasarlanır fakat iletişim tek yönlü olduğu için etkileşimde sınırlıdır.<sup>12</sup>

Yeni Medya 20. yüzyılın ikinci yarısında sürekli gelişmekte olan dijital teknolojinin getirmiş olduğu yeniliklerle ortaya çıkan bir kavramdır.<sup>13</sup> Yeni Medya çift yönlü bir iletişim kanalı olduğundan ötürü internet üzerinden erişimin sağlandığı bir yapıdadır.<sup>14</sup> Bu medya türü sosyal medya platformlarını, blogları, video paylaşım sitelerini kapsamaktadır.<sup>15</sup> Yeni medyanın en belirgin özellikleri arasında hem çift yönlü ve etkileşimi arttıran yapısı bulunmakta hem de içerik üretim ve dağıtımının kurumların kontrolünde olmayıp daha demokratik bir yapıda olmasıdır. Yeni Medya web 2.0 kapsamında ele alınmaktadır. Web 2.0 ilk olarak Tim O'Reilly tarafından kullanılmıştır.<sup>16</sup> Web 2.0 aynı zamanda bir sosyal ağ karşımıza çıkmaktadır ve bu sayede artık herkes, minimum maliyetle kendi içeriğini üretebilmektedir. Yani içerik üretimini kurumların tekelinden kurtarmıştır diyebiliriz. Ayrıca üretilen içerikler sadece belirli bir kesime değil dünya çapında bir kitleye ulaştırılabilir hale gelmiştir.<sup>17</sup> Yeni Medya ile birlikte internet kullanıcı sayısı yükselişe geçmiştir. Web 2.0'ın çift yönlü olması dolayısıyla katılım ve etkileşim merkezli bir internet anlayışı yaygınlaşmıştır.<sup>18</sup> Yeni medya ile gelişen bir diğer durum ise içerik tüketicilerinin aynı zamanda birer üreticiye dönüşmesidir. Medya açısından üretim dağıtım ve tüketimindeki geniş yelpazeyi kapsayan yeni medya gerek maliyetlerin düşük olması gerekse kolay erişim sağlanması bireyler

<sup>11</sup>Metatime, <https://metatime.com/tr/blog/web-10-nedir-web-20-nedir#!> (10.05.2024)

<sup>12</sup>Nezir Akyeşilmen, Siber Uzak Ders Notları, 2022

<sup>13</sup>Bostancı, 2019., s.19.

<sup>14</sup>Filiz Aydoğan, Ali Murat Kırık, "Alternatif Medya Olarak Yeni Medya", Akdeniz İletişim Dergisi, ..., s.60.

<sup>15</sup>Albayrak, "Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü", s.1.

<sup>16</sup>Metatime, <https://metatime.com/tr/blog/web-10-nedir-web-20-nedir#!> (10.05.2024)

<sup>17</sup>Bostancı, 2019., s.20.

<sup>18</sup>Tom Alby, "Web 2.0", chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/[https://files.hanser.de/Files/Article/ARTK\\_LPR\\_9783446415805\\_0001.pdf](https://files.hanser.de/Files/Article/ARTK_LPR_9783446415805_0001.pdf), (30.07.2024)



açısından çok fazla olanak sağlanması durumunu ortaya koymuştur. Gelişimin devam etmekte olduğu yeni medya sürecinde temele dünya üzerindeki tüm kullanıcılar tarafından hat safhada bir ilgi kaynağı olan sosyal medyayı koymamız mümkün olacaktır.<sup>19</sup>

Günümüzde her iki medya türünün de varlığından söz etmek mümkündür. Dolayısıyla yeni medya çıktığı zaman geleneksel medya tarihe karışmıştır ve kullanılmıyor gibi bir düşünceye sahip olmak çok büyük bir yanılığdan ibarettir. Teknolojik gelişmeler açısından bakıldığı takdirde her iki medya türünün de halen daha gelişmekte olduğunu görebiliriz. Bizatihi içerisinde yaşamış olduğumuz bu gelişmeler bize şunu gösterebilir, geleneksel medya ve yeni medyayı birbirinden bağımsız olarak düşünemeyiz. Zira her ne kadar yeni medya toplumun haber alma, öğrenme biçimleri ve eğlenme gibi birçok konuda gelişmiş bir teknoloji olarak karşımıza çıkıyor olsa da bunlar geleneksel medya zamanında da yok değildi. Sadece yeni medya ile bilgi daha hızlı yayılmaya başladı ve tek bir kişinin tekelinde kontrolden kurtarılmış oldu. Geleneksel medya ve yeni medya birbirini tamamlayıcı iki kavram olarak değerlendirilebilir. Ancak şunu belirtmek gerekir ki gelişmekte olan teknoloji ve toplum bazında değişiklik gösteren iletişim alışkanlıkları sebebiyle yeni medya önemini ve etkisini gittikçe daha da arttırmaktadır.

## Sosyal Medya

*“Sosyal medya su gibidir. Su kendi başına sadece serinletir, ancak diğer bileşenlerle birleştiğinde tüm yaşam bilimlerinin gelişimini sağlamıştır.” M. VOLPE<sup>20</sup>*

Sosyal medya, yeni medya içerisinde bir çatı kavramı oluşturmaktadır.<sup>21</sup> Zira sosyal ağ demiş olduğumuz bir kavram daha var ki bunun bileşenleri sosyal medya kavramının alt başlıkları olarak karşımıza çıkmaktadır. Nitekim sosyal medya kavramı birçok kaynakta sosyal ağ veyahutta sosyal ağ siteleri gibi tanımlarla da karşılaşmaktadır.<sup>22</sup> Farklı farklı tanımlarla karşımıza çıkıyor olsada genel anlamda sosyal medya insanların birbirleriyle etkileşimde buldukları, istedikleri zaman istedikleri yerden katılım sağlayabilecekleri, çoğu zaman ücretsiz kullanıma sahip, her yaşta bireylerin özgürce ulaşım sağlayabildiği çevrimiçi

<sup>19</sup>Bostancı, 2019, s.21.

<sup>20</sup>Bostancı, 2019, s.22.

<sup>21</sup>Erol Başaran Bural, *Sosyal Medya İstihbaratı*, İstanbul: Yeditepe Yayınları, 2021, s.79.

<sup>22</sup>Bural, 2021., s. 83.



platformlardır.<sup>23</sup> Sosyal medya dediğiniz zaman insanların sadece sosyalleşmek için kullanmış olduğu platformlar gibi algılamamıza sebebiyet veriyor olsada aslında günümüzde iş için kullanımlarına da şahit oluyoruz.<sup>24</sup>

Facebook, Twitter, Instagram, LinkedIn, TikTok, Spotify, Pinterest ve YouTube gibi platformlardan oluşan sosyal medya 21. yüzyılda insanların birbirleriyle etkileşimi ve iletişime geçme biçimlerini tamamen dönüştürmüş bir durumdadır. Bu sosyal medya platformları bireylerin sadece birbirleriyle iletişim kurmaları için değil, aynı zamanda ilgi alanlarını, düşüncelerini paylaşmaları için ve iş fırsatlarından faydalanmaları içinde kullandıkları bir mecraadır.<sup>25</sup>

Sosyal medya platformlarını aşağıdaki şekilde sınıflandırmak mümkün olacaktır;<sup>26</sup>

|  |   |
|--|---|
| <b>1. Sosyal Ağ Siteleri:</b>                    | - Facebook - Instagram - Twitter - LinkedIn   |
| <b>2. Paylaşım Platformları:</b>                 | - YouTube (video paylaşımı)<br>- TikTok (kısa video paylaşımı)<br>- Snapchat (anlık fotoğraf/video paylaşımı) |
| <b>3. Mikroblogging Siteleri:</b>                | - Twitter - Tumblr  |
| <b>4. Fotoğraf Paylaşım Siteleri:</b>            | - Instagram - Flickr - Pinterest  |
| <b>5. İçerik Oluşturma ve Paylaşma Siteleri:</b> | - YouTube (video oluşturma ve paylaşma)<br>- SoundCloud (müzik oluşturma ve paylaşma)                         |
| <b>6. Bloglama Siteleri:</b>                     | - Wordpress - Blogger   |
| <b>7. Mesajlaşma Uygulamaları:</b>               | - WhatsApp - Messenger  |

Tablo: Sosyal Medya Platformları Sınıflandırılması

Bireyler aynı zamanda bu sosyal medya platformları sayesinde kendi küçük dünyalarından çıkıp daha farklı dünyaların olduğunu görme fırsatını elde ediyorlar. Yani kısaca sosyal medya, dünya çapında bir kitle ile bağlantı kurmalarına olanak sağlamaktadır.<sup>27</sup> Aslında bu

<sup>23</sup>Bostancı, 2019., s.23.

<sup>24</sup>Bural, 2021., s. 80.

<sup>25</sup>Bostancı, 2019, s.22.

<sup>26</sup>Mehmet Akpınar, “Sosyal Medya Nedir? Bilmeniz Gerekenler”, <https://mehmetakpinar.com/blog/sosyal-medya-nedir-bilmeniz-gerekenler/> (02.06.2024)

<sup>27</sup>Albayrak, “Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü”, ss. 1-9.



sayede bilgiler ve haberler daha hızlı bir yayılım sağlıyor ve sosyal hareketler daha hızlı bir şekilde büyüyor. Birçok insan aynı ilgi alanlarına (iletişim, ticaret, reklam, üretim, tanıtım, psikoloji, sosyoloji, felsefe, sağlık, eğitim, eğlence, aile) sahip olduğu kişilerle bir araya gelerek topluluklar kurabiliyor.<sup>28</sup> Bu bağlamda şunu dile getirmemiz mümkündür birbirinden farklı birçok konu sosyal medya kapsamı içerisine girmiş durumdadır.<sup>29</sup>

Sosyal medya ile,

- Bireyler artık kendi gibi düşünen insanlar tarafından sesinin duyurulmasına ihtiyaç duymamaktadır.
- Herkes kendi fikirlerini, düşüncelerini ve hazırlamış oldukları herhangi bir içeriği kendi istedikleri şekilde paylaşabilmektedir.<sup>30</sup>
- İçerik üretmenin yanı sıra başkalarının üretmiş olduğu içeriklere katkı sağlayabilme ve yorum yapabilme noktasında etkileşim sağlamıştır.<sup>31</sup>
- Kolay erişim ve hızlı iletişim ağı hayatımıza dahil olmuştur.<sup>32</sup>
- Bireyler tarafından üretilen bu içerikler metinler, görseller, ses dosyaları, videolar ve ilgi alanlarına göre veyahutta düşüncelere göre bir araya gelen topluluklar biçiminde karşımıza çıkabilmektedir.

Bireysel katılım ve etkinin ön planda olduğu sosyal medyayı geleneksel medyadan ayıran bazı karakteristik özellikler vardır. Bu karakteristik özelliklere Göker Ve Keskin'den referansıyla Mayfield'in makalesinde şu şekilde görmemiz mümkün olacaktır;

- *Katılımcılar: Sosyal medya katılımcıları cesaretlendirmekte ve ilgili olan her bir kullanıcıdan geri bildirim sağlamaktadır.*
- *Açıklık: Sosyal medya servisleri diğer medya servislerine oranla en fazla geribildirime ve katılımcıya açık olan servislerdir. Bu servisler oylama, yorum ve bilgi paylaşımı gibi konularda cesaret aşlamaktadır. Bu servislerde ulaşımaya yönelik engelleme durumu oldukça nadir görülmektedir. Bireyse sunulan özgürlük ortamı kullanımı cazip kılmaktadır. Çünkü toplumsal baskı ve kısıtlamalardan sıkılan birey özgürlüğün büyümesine kapılmaktadır.*
- *Konuşma: Geleneksel medya yayına ilişkin iken (içerik aktarımı ya da dinleyiciye bilgi ulaşımı), sosyal medya çift yönlü iletişime olanak tanınması bakımından daha caziptir.*

<sup>28</sup>Bural, 2021., s. 81.

<sup>29</sup>Felemez Güneş, Zeynep Güneş, "İfade Özgürlüğünün Sosyal Medya İçin Taşıdığı Anlam", VII. Hukukun Gençleri Sempozyumu, İstanbul, 22-23 Aralık 2016, ss.1-12.

<sup>30</sup>Bostancı, 2019., s.25.

<sup>31</sup>Bural, 2021., s. 84.

<sup>32</sup>Bostancı, 2019., s.23.



- *Toplum: Sosyal medya topluluklara çabuk ve etkili bir örgütlenme için olanak sunmaktadır. Topluluklar da böylece beğendikleri fotoğraf, politik değerler, favori TV şovları gibi ilgili oldukları şeyleri paylaşmaktadır.*
- *Bağlantılılık: Sosyal medyanın çoğu türü, metinler arası bağlantı sağlamakta; diğer siteler, araştırmalar ve kullanıcıların ilgili oldukları herhangi bir konuda link verilmesine olanak tanımaktadır.* <sup>33</sup>

Sosyal medya birçok olumlu özelliğinin yanı sıra bazı olumsuz yönleri de beraberinde getirmiştir. Bu olumsuz yönlerinden özellikle gizlilik ve veri güvenliği kullanıcılar açısından çok büyük bir endişe kaynağı haline gelmiştir.<sup>34</sup> Bununla birlikte sosyal medya platformları üzerinden yayılan yanlış bilgilerin toplumda büyük yanılgılara sebebiyet vermesiyle toplumsal bölünmelere ve kutuplaşmalara yol açması yine sosyal medyanın olumsuz özelliklerinden bir tanesi olarak karşımıza çıkmaktadır.<sup>35</sup> Bu tür sorunlarla mücadele etmek ise hem platformların hem de bizatihi kullanıcıların sorumluluğundadır. Elbette ki sosyal medyanın getirmiş olduğu bu olumsuz durumlar içerisinde gizlilik ve veri güvenliği konusunda bireylerden daha çok sosyal medya platformlarına ve devletlere sorumluluk düşmektedir.<sup>36</sup>

Sonuç olarak bireylerin internet tabanlı çevrimiçi sosyal ağ sitelerinde bir araya gelerek veyahut kendi başlarına ürettikleri içerikleri (fotoğraf, video, ses dosyası vb.) paylaşmış oldukları platformları sosyal medya olarak tanımlamak mümkündür.<sup>37</sup> Sosyal medya bir çatı kavramdır ve bir alt grubunu oluşturan sosyal ağları ise bireylerin katılım sağlamak için profil oluşturmak durumunda oldukları ve kendileriyle aynı düşünceye sahip diğer bireylerle bir topluluk halinde etkileşimde buldukları Facebook, LinkedIn ,Twitter ve Instagram gibi

<sup>33</sup>Göksel GÖKER, Savaş KESKİN, “Sosyal Medya Türü Olarak Sosyal İçerik Platformları: Betimsel Bir İnceleme” Uluslararası Sosyal Araştırmalar Dergisi, Cilt: 8, Sayı: 39, Ağustos 2015, ss. 1-14.

<sup>34</sup>Metatime, <https://metatime.com/tr/blog/web-10-nedir-web-20-nedir/>! (11.05.2024)

<sup>35</sup>Metatime, <https://metatime.com/tr/blog/web-10-nedir-web-20-nedir/>! (11.05.2024)

<sup>36</sup>Yeşildal, Ali. “Sosyal Medya, Yerel Yönetimler Ve Katılımcı Yönetim: Bilgi Çağında Belediyeler İçin Yeni Stratejiler”. İnsan Ve İnsan 6, sy. 22 (Ekim 2019): 883-902.

<sup>37</sup>Euromsgexpress, [“https://www.euromsgexpress.com/sosyal-medya-nedir/?gad\\_source=1&gclid=Cj0KCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd219Lj0t16zPoONWpSnMzDzTuk8aAr0AEALw\\_wc”](https://www.euromsgexpress.com/sosyal-medya-nedir/?gad_source=1&gclid=Cj0KCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd219Lj0t16zPoONWpSnMzDzTuk8aAr0AEALw_wc) (31.05.2024)





internet toplulukları olarak ifade etmek mümkündür.<sup>38</sup> Kolay erişim imkanı sağlayan bu siteler paylaşılan içeriklerin çok kısa bir zaman dilimi içerisinde tüm dünyaya yayılmasını sağlaması açısından pozitif bir görünüme sahip olsa da gerçek dışı olan profillerin oluşturulması imkanı da taşıdığından dolayı sosyal medya suça bulaşmış bireyler ve suç örgütleri tarafından da aynı kolaylıkla erişim sağlanabilen bir platformdur.<sup>39</sup>

Sosyal medyanın geleceği gelişmekte olan teknolojiye ve bireylerin bu platformları nasıl kullandığına bağlı olarak şekillenecektir. Artırılmış gerçeklik, sanal gerçeklik ve yapay zeka gibi teknolojilerin entegrasyonu, kullanıcıların bu platformdaki deneyimlerini daha da zengin bir hale getirecektir.<sup>40</sup> Pek tabii bu yenilikler ile birlikte kullanıcı gizliliğini ve veri güvenliğini korumanın yollarını bulmakta giderek daha fazla önemli bir hal alacak ve bu hususta daha fazla önlem alınmasını gerekli kılacaktır. Sosyal medya dediğimiz bu medya türünden daha fazla verim alabilmek adına bu tür zorlukların üstesinden gelecek önlemlerin alınması oldukça önemlidir.<sup>41</sup>

## İfade Özgürlüğü

*“Madde 25 – Herkes, düşünce ve kanaat hürriyetine sahiptir. Her ne sebeple ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce kanaatleri sebebiyle kınanamaz ve suçlanamaz.”<sup>42</sup>*

Bu maddeden anlaşılacağı üzere ifade özgürlüğü, bireylere düşüncelerini, görüşlerini ve inançlarını herhangi bir kısıtlama olmaksızın ifade edebilme hakkı vermektedir.<sup>43</sup> Bu cümle ifade özgürlüğü ile çalışmamızın temel konusu olan sosyal medya ekseninde ifade özgürlüğünün arasındaki en önemli farkı anlamamız açısından önem arz etmektedir.

<sup>38</sup> Euromsgexpress, [“https://www.euromsgexpress.com/sosyal-medya-nedir/?gad\\_source=1&gclid=Cj0KCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd219Lj0tI6zPoONWpSnMzDzTuk8aAr0AEALw\\_wc”](https://www.euromsgexpress.com/sosyal-medya-nedir/?gad_source=1&gclid=Cj0KCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd219Lj0tI6zPoONWpSnMzDzTuk8aAr0AEALw_wc) (31.05.2024)

<sup>39</sup>Ali Yeşildal, a.g.m., (11.05.2024)

<sup>40</sup>Bostancı, 2019. s.25.

<sup>41</sup>Bural, 2021, s. 86.

<sup>42</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>43</sup>Mustafa Erdoğan, *İnsan Hakları Teorisi ve Hukuku*, Ankara: Orion Kitabevi, 2016, s.215.



Türkiye Cumhuriyeti 1982 yılında yayımlanan anayasasında yukarıda görüldüğü üzere belirtmiştir ki herkes düşüncelerini özgür bir şekilde ifade etme hakkına sahiptir.<sup>44</sup> Bahsi geçen bu hak demokratik bir toplum olmanın en temel taşıdır. Bireylerin düşüncelerini, görüşlerini ve inançlarını herhangi bir baskı ve kısıtlama olmaksızın ifade edebilmesi en büyük insan haklarından birisi olarak karşımıza çıkmaktadır. İfade özgürlüğü sayesinde bireyler farklı fikirlerini özgürce ifade edip, saygı çerçevesinde oluşturulan fikir tartışmaları oluşturabilir, bilgi ve deneyimlerini rahatlıkla paylaşabilirler.<sup>45</sup> Bu sayede toplumsal gelişim için büyük önem arz eden eleştirel düşünce yapısı teşvik edilebilir. İfade özgürlüğü aynı zamanda toplumsal barışın sağlanması için de önemli bir unsurdur.<sup>46</sup> Anayasal demokrasinin oluşmasında ifade özgürlüğü ne kadar önem arz ediyorsa aynı şekilde ifade özgürlüğünün oluşmasında da demokrasinin varlığı büyük önem arz etmektedir.<sup>47</sup>

İfade özgürlüğü bireylere düşüncelerini özgürce ifade edebilme hakkı tanır. Fakat burada özgürlükten kastettiğimiz bireylerin birbirlerine zarar verecek boyutta bir davranış sergilemesi hakkı değildir. Zira bir başkasına zarar vererek özgür bir ortam oluşturmamız asla mümkün değildir. Düşüncelerimizi inançlarımızı görüşlerimizi elbette ki özgürce paylaşabilmeyiz fakat bunu yaparken başkalarının haklarına da saygı duyup farklılıklara açık olmak zorundayız. Örneğin Türkiye'de yaşıyoruz ve büyük bir çoğunluğu Müslüman bir ülke olduğu için herkesin de müslüman olması gerekiyor gibi bir düşünce ile hareket ederek başka herhangi dini mensup olduğunu ifade eden insanları ötekileştirmememiz ve onlara saygı duymamız gerekmektedir.<sup>48</sup> Başka bir örnekle bir grup içerisinde farklı siyasi görüşlere sahip olan arkadaşların bir konu hakkında fikir beyan ederken sonucunda o ortamda şiddetli bir kavga çıkmasından korkmadan özgür bir şekilde düşüncesini dile getirebilmesi gerekmektedir. günümüzde ne yazık ki fikir özgürlüğü olarak bir özgürlükten pratikte bahsetmek mümkün değil.<sup>49</sup> Zira yerel ve genel seçimlerde ülke genelinde yaşatılan tartışmacı üslup toplumun en küçük yapı taşı olan ailelerde dahi sonucunun kötü bittiği kavgalara sebebiyet vermektedir. Böyle bir toplumda demokrasiden bahsetmek ne yazık ki mümkün değildir. Demokrasinin

<sup>44</sup>Erdoğan, 2016., s.214.

<sup>45</sup> Dominika Bychawska-Siniarska, “Avrupa İnsan Hakları Sözleşmesi Kapsamında İfade Özgürlüğünün Korunması”, Avrupa Konseyi, 2028, ss. 11-21.

<sup>46</sup>Erdoğan, 2016., s.215.

<sup>47</sup>Çiğdem Baloğlu, *İfade Özgürlüğü*, Yayınlanmış Yüksek Lisans Tezi, Kocaeli:Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s.17.

<sup>48</sup>Çiğdem Baloğlu, 2006, s.19.

<sup>49</sup>Çiğdem Baloğlu, 2006, s. 23.



olmadığı bildiğimiz bir toplumda da ifade özgürlüğünden bahsetmek oldukça yanlıştır.<sup>50</sup> Bir başkasının özgürlüğünün kısıtlandığı ve buna benim de sebebiyet verdiğim yerde aslında benim de özgürlüğüm kısıtlanıyor demektir. Bu sebeple bireylerin bu hakları başkalarına zarar vermeyecek bir şekilde ciddi bir sorumluluk bilinciyle kullanmaları gerekmektedir. Bu kapsamda şunu da belirtmek gerekir ki ifade özgürlüğünün korunması, demokrasi işleyişi için olmazsa olmazdır.<sup>51</sup> Zira bahsetmiş olduğumuz bu özgürlük hem hükümetin hem de diğer yetkili organların faaliyetlerini denetleyebilme, yolsuzluklara ve haksızlıklara karşı çıkabilme noktasında imkan tanıyan bir husustur. Fakat şunu belirtmekte fayda var ifade özgürlüğünün sınırları ile ilgili hem uluslararası hem de yerel düzeyde farklı yaklaşımlar mevcuttur.<sup>52</sup> Örnek vermek gerekirse, şiddeti teşvik etme, nefret söylemi ve iftira gibi durumlar, genellikle ifade özgürlüğünün sınırları içerisinde kabul edilmez.<sup>53</sup> Yukarıda bahsetmiş olduğumuz bir başkasının özgürlüğünün kısıtlanmasında bireyin kendisinin de etken olduğu hususu tam bu noktada ele alınması gereken bir durumdur.

Sonuç olarak, ifade özgürlüğü hem bireyler açısından hem de toplumun gelişimi açısından vazgeçilmez bir haktır.<sup>54</sup> Lakin bu özgürlüğün etkili bir şekilde korunması ve sürdürülmesi için hem bireysel hem de toplumsal bazda ciddi bir sorumluluk bilinci ile hareket edilmesi gerekmektedir.<sup>55</sup> İfade özgürlüğünün daha sağlıklı bir toplum için oluşturmuş olduğu zemin, farklılıkların hoşgörü ile karşılanması, eleştirel düşüncenin gelişimi ve demokrasinin güçlenmesi açısından büyük önem arz etmektedir.<sup>56</sup>

## Sosyal Medya Ekseninde İfade Özgürlüğü

*“Madde 26 – Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra*

<sup>50</sup>Kulaçoğlu Hukuk Bürosu, <https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/> (10.05.2024)

<sup>51</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>52</sup>Çiğdem Baloğlu, 2006, s.20.

<sup>53</sup>Jindar Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü”, Hukuk Fakültesi Dergisi, Yıl: 7, Sayı 2, Aralık 2021, ss. 352-353.

<sup>54</sup>Çiğdem Baloğlu, 2006, s.19.

<sup>55</sup>Akyeşilmen, 2019, s.152.

<sup>56</sup>Akyeşilmen, 2019, s.153.



*hükmi, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.*

*Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulince belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.”<sup>57</sup>*

İfade özgürlüğü, bireylerin düşüncelerini, inançlarını, fikirlerini ve duygularını, *sansür ya da korku* olmaksızın ifade edebilme hakkıdır. Bir önceki başlıkta değinmiş olduğumuz üzere bu cümlede ifade özgürlüğü ile sosyal medya ekseninde ifade özgürlüğü arasındaki temel farkı görüyoruz. Bu fark italik olarak belirtmiş olduğumuz “sansür ve korku” kelimeleri ile açıkça görülmektedir.<sup>58</sup> İfade özgürlüğü gündelik hayatımızı da içerisine alan bir husustur ve bu konu ile ilgili örnekleri yukarıda verdik. Fakat sosyal medya ekseninde ifade özgürlüğü dediğimiz zaman sansür kavramı hayatımıza dahil olmaktadır. yani buradan hareketle ifade özgürlüğümüze devlet eliyle bir kısıtlama getirilmektedir.<sup>59</sup> düşüncelerimizi görüşlerimizi duygularımızı ve inançlarımızı özgür bir şekilde ifade edememek anlamı taşımaktadır bu.

Anayasal Demokrasinin temel taşlarından biri olarak kabul edilen ifade özgürlüğü sosyal medyanın yükselişi ile birlikte yeni bir boyut kazanmıştır.<sup>60</sup> Yenilenen bu boyutta sosyal medya platformları hayatımıza dahil olmuştur ve bireyleri düşüncelerini çok geniş bir kitleye hızlı bir şekilde uğraştırma imkanı sağlamıştır.<sup>61</sup> Geleneksel medya döneminde olduğu gibi bir konuda ortaya atılan görüşe farklı bir bakış açısı olduğu zaman insanların bir araya gelip

<sup>57</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>58</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>59</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>60</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>61</sup>Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü”, s.352.



protestolar düzenlemesini beklemek yerine artık sosyal medya platformları sayesinde bireyler seslerini daha önce hiç olmadığı kadar güçlü bir şekilde duyurabilmektedir.<sup>62</sup>

Bireyler bazında olumlu bir anlam taşıyan bu durum devletler açısından bir o kadar olumsuz anlam taşımaktadır. Zira sansür uygulamasının yanı sıra yapmış olduğumuz paylaşımların sonucunda herhangi bir cezaya çarptırılma korkusu ile ifade özgürlüğümüz elimizden alınmıştır.<sup>63</sup> Bu durum halkın içerisinde yaşayan sıradan bir insan için de geçerli Türkiye Büyük Millet Meclisi'nde milletin oylarıyla seçilip gelen milletvekilleri için de aynı şekilde geçerlidir. Şunu da belirtmek gerekirse ana akım medyaya ters düşen paylaşımlar kim tarafından yapıldığına bakılmaksızın cezaya çarptırılmaktadır. Örnek vermek gerekirse 27. dönem Kocaeli milletvekili Ömer Faruk Gergerlioğlu'nun Twitter platformu üzerinde bir haber paylaşımına RT yapması üzerine hakkında soruşturma başlatılmıştır.<sup>64</sup> Bunun sonucunda ise Gergerlioğlu'nun Twitter hesabı askıya alınmış ve Milletvekilliği düşürülmüştür.<sup>65</sup> Bir süre sonra hesabı tekrar aktif hale gelmiş olsa da hukuki süreçler devam etmekteydi. Gergerlioğlunun böyle bir hukuksuzluğa maruz kaldığı olayda paylaşımı yapan Twitter kanalına herhangi bir yaptırım uygulanmamıştır.<sup>66</sup> Bununla birlikte paylaşımı retweet eden diğer kullanıcılara da herhangi bir ceza verilmemiştir. Burada görüyoruz ki tam anlamıyla bir kişi hedef alınmış ve ifade özgürlüğü yok sayılmıştır.<sup>67</sup> Bu hususta anayasa'nın ilgili maddesi bu örnek olaya ile ilgili olumsuzluğu bize şu şekilde göstermektedir:

*“Madde 31 – Kişiler ve siyasi partiler, kamu tüzel kişilerinin elindeki basın dışı kitle haberleşme ve yayım araçlarından yararlanma hakkına sahiptir. Bu yararlanmanın şartları ve usulleri kanunla düzenlenir.*

*(Değişik fıkra: 3/10/2001-4709/11 md.) Kanun, millî güvenlik, kamu düzeni, genel ahlâk ve sağlığın korunması sebepleri dışında, halkın bu araçlarla haber almasını, düşünce*

<sup>62</sup>Av. Begüm Gürel, <https://www.bghukukburosusu.com.tr/9613/> (31.05.2024)

<sup>63</sup>Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü”, ss. 371-376.

<sup>64</sup>T.C. Anayasa Mahkemesi, Genel Kurul Kararı, <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2019/10634> (28.07.2024)

<sup>65</sup> Ömer Faruk Gergerlioğlu, HalkTV Sözümleri Var, <https://www.youtube.com/watch?v=7OBiDLKnf4U> (02.06.2024)

<sup>66</sup> Ömer Faruk Gergerlioğlu, HalkTV Sözümleri Var, <https://www.youtube.com/watch?v=7OBiDLKnf4U> (02.06.2024)

<sup>67</sup>T.C. Anayasa Mahkemesi, Genel Kurul Kararı, <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2019/10634> (28.07.2024)



*ve kanaatlere ulaşmasını ve kamuoyunun serbestçe oluşmasını engelleyici kayıtlar koyamaz.”<sup>68</sup>*

Sosyal medya bireylerin düşüncelerini özgürce ve herhangi bir muhalefet gücüne gerek kalmadan ifade edebildikleri bir ortam olması gerekirken günümüzde ne yazık ki düşünceleri özgürce ifade edebildiğimiz bir konumda değildir. Özellikle hükümet politikalarına karşı bir eleştirel yaklaşımda bulunmanın yanı sıra herhangi bir yorum yapmanın dahi sonucu farklı cezalarla karşılaşmak anlamı taşımaktadır. Bu hususa sosyal medya üzerinde dolaşan, espri olduğu iddia edilen şu cümle ile açıklık getirebiliriz, “Silivri soğuktur!” bir tek cümle ile ifade özgürlüğümüzün ne kadar kısıtlı olduğunu görmek ne yazık ki mümkün bir duruma gelmiştir. Zira espri amaçlı olarak dahi kurulmaması gereken bir cümlenin altında yatan bir gerçek vardır.

Sosyal medya üzerinde düşüncelerini fikirlerini herhangi bir konu hakkındaki görüşlerini ifade edebilme noktasında ülkemizde ne yazık ki tam manasıyla bir özgürlük bulunmamaktadır. Bu bağlamda sosyal medya üzerinde ifade özgürlüğünü değerlendirebilen bir isim olarak Sedat Peker<sup>69</sup> olayını ele alabiliriz. Sedat Peker YouTube üzerinden videolar yayınlamaya bazı konularda düşüncelerini belirtmiştir.<sup>70</sup> Bu olayın olumlu tarafı Sedat Peker'in bu videoları sosyal medya üzerinden yayınlayabilmesiydi fakat olayın olumsuz tarafı ise bunu kendi ülkesi sınırları içerisinde değil aksine ülkesinden kaçarak çıkmış olduğu yurt dışında bir ülkede gerçekleştirmiş olmasıydı. Eğer Türkiye'de kalmış olsaydı Peker'in bu videoları yayınlama olasılığı neredeyse yok denecek bir orana sahiptir. (Videoların içeriğinden bağımsız bir örneklendirmedi.)<sup>71</sup>

Sosyal medya ifade özgürlüğü kapsamında birçok imkan sağlamış olsa da beraberinde bazı zorlukları da getirmiştir. Örneğin nefret söylemi, yalan haber, aşırı kutuplaşma ve özel

<sup>68</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>69</sup>Reha Talha Aygen, “Devlet, Siyaset Ve Organize Suç Örgütleri: Reis Sedat Peker Örneği”, Uluslararası Sosyal Ve Beşeri Bilimler Araştırma Dergisi, Cilt. 8, Sayı 76, 2021, S. 2733.

<sup>70</sup>Youtube, Sedat Peker, <https://www.youtube.com/watch?v=QJx4CABC7oE> (02.06.2024)

<sup>71</sup>Fulya Şen Y. Furkan Şen, “Sosyal Medya, İletişim Hakkı Ve İfade Özgürlüğü Üzerine Bir Değerlendirme”, Gazi Üniversitesi, İibf Dergisi, Cilt. 17, Sayı 2, 2015, S. 131.



hayatın gizliliğinin ihlali gibi sorunlar ortaya çıkmıştır.<sup>72</sup> Bu tür sorunlar sebebiyle sosyal medya bağlamında ifade özgürlüğü tek başına bir hak olarak değerlendirilmemelidir. Zira başka temel haklar arasında da denge kurma ihtiyacı bu noktada hasıl olmaktadır. Özellikle, bireylerin ya da toplulukların zarar görmesine neden olabilecek içeriklerin yayılmasını engellemek amacıyla sosyal medya platformları üzerindeki düzenlemeler ve gözetim konusu tartışılmalıdır.<sup>73</sup>

Bu bağlamda sosyal medya ve ifade özgürlüğü arasındaki ilişkiyi anlamak için aynı zamanda yönetebilmek hem bireylerin hakkını korumayı hem de kamusal alanın sağlıklı bir şekilde işlemini sağlayabilmek için çok kritik bir öneme sahiptir. Bilinçli bir dijital vatandaş olmanın önemi her zaman daha da artmaktadır.<sup>74</sup> Bu kapsamda yapılabilecek en iyi işlerden bir tanesi dijital vatandaşlık eğitiminin yaygınlaştırılmasıdır.<sup>75</sup> Bu adımdan sonra devletin ifade özgürlüğünü tam manasıyla yaşayabileceğimiz bir ortam oluşturması gerekmektedir.<sup>76</sup> Zira sadece bireysel manada bir adım atmak kimseyi bir adım ileriye götürmeyecektir. Bu bir denge durumudur ve bu dengeyi sağlamak, özgür ve sağlıklı bir kamuoyu alanının sürdürülmesi için önemlidir.

Sonuç olarak, ifade özgürlüğü ve sosyal medya arasındaki ilişki, devamlı bir denge ve düzenleme gerektiren karmaşık bir husustur. Bir kereye mahsus adımlar atılıp bu konu hakkında yapılacakların bittiğinin düşünülmesi çok büyük bir yanılgıdan ibarettir. Sürekli olarak gelişen ve değişen bir yapı olan sosyal medya özellikle takip edilmesi gereken ve sürekli olarak yeniliklerle ve gelişmelerle ele alınması gereken bir konudur.<sup>77</sup>

## Sosyal Medya Yasası

<sup>72</sup>Eray Taş, Yeni Medyada Nefret Söylemi, Yeni Medya Elektronik Dergisi, Cilt. 1, Sayı 1, 2017, s.64.

<sup>73</sup>Eray Taş, Yeni Medyada Nefret Söylemi, *DergiPark*, 2017, s.65

<sup>74</sup>Ali Murat KIRIK, Kenan BÖLÜKBAŞ, Gönül CENGİZ,, “Sosyal Medya Bağlamında Dijital Vatandaşlık: TRT İstanbul Radyosu Prodüktörleri Üzerinden Bir Değerlendirme”, Mavi Atlas Dergisi, Cilt.7, Sayı 2, 2019, s.5.

<sup>75</sup>KIRIK, BÖLÜKBAŞ, CENGİZ, “Sosyal Medya Bağlamında Dijital Vatandaşlık: TRT İstanbul Radyosu Prodüktörleri Üzerinden Bir Değerlendirme”,s.7.

<sup>76</sup>T.C. 82

Anayasası, <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5> (11.05.2024)

<sup>77</sup>Bostancı, 2019., s.23.





Sosyal medya yasası, dijital platformlarda kullanıcılarının haklarını korumak ve sosyal medya şirketlerinin sorumluluklarını tamamlamak amacıyla oluşturulan bir dizi düzenlemelerdir.<sup>78</sup> Bu yasalar ülkeden ülkeye farklılık göstermektedir.<sup>79</sup> Fakat genellikle sosyal medya platformlarının ve belirli içerikleri hızlıca kaldırmaya veya kullanıcıların kimliklerini açıklamaya zorlayabilen yasalardır.<sup>80</sup>

Sosyal medya yasaları şu konuları ele alır; sosyal medya platformlarını düzenlemek, sosyal medya platformlarında kullanıcı bilgilerini koruma, yanıltıcı içerikleri engelleme, kullanıcıların gizliliğini koruma, nefret söylemi ile mücadele, yanlış bilgilerin yayılmasını önleme, ifade özgürlüğü, güvenlik, gizlilik hakları ve tüm haklar arasında dengeli bir ilişki kurmayı hedefler<sup>81</sup>

Bahse konu olan yasalar, sosyal medya platformlarında yayınlanacak olan içeriklerin önceden denetlenerek kontrol edilmesi gerektiği anlayışı ile hareket etmektedir. Bu anlayış ile hareket ederken kullanıcıların kişisel verilerinin korunmasını hedeflemektedir. Bu hedefinin yanı sıra sahte hesaplar ve yanıltıcı içeriklerin de tespit edilmesini amaçlamaktadır.<sup>82</sup> Sosyal medya yasaları yapmış olduğu bazı düzenlemeler ile yasa dışı içeriklerle mücadele ve zararlı materyalin yayılmasını engelleme amacı taşımaktadır.<sup>83</sup> Fakat bu aynı zamanda sansür ve ifade özgürlüğüne müdahale gibi birçok eleştiriye de maruz kalan bir durumdur.<sup>84</sup> Aslında yukarıda da ele almış olduğumuz üzere hükümet politikalarında yer alan hususlarla ilgili yapılan eleştirel paylaşımın genel itibarıyla sansür uygulanarak veyahut da kısıtlama yapılarak paylaşımın kaldırılması gibi sonuçlar ya da daha ağır bir şekilde cezai işlem sonucunda ifade özgürlüğüne müdahale eleştirisi oldukça haklı bir eleştiri olarak karşımıza çıkmaktadır.<sup>85</sup>

<sup>78</sup>TRT Haber, “Sosyal Medya Yasası Nedir?”, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html>, (02.06.2024)

<sup>79</sup>TRT Haber, “Sosyal Medya Yasası Nedir?”, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html>, (02.06.2024)

<sup>80</sup>Bostancı, 2019., s.25.

<sup>81</sup>Kulaçoğlu Hukuk Bürosu, <https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/> (16.05.2024)

<sup>82</sup>TRT Haber, “Sosyal Medya Yasası Nedir?”, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html>, (02.06.2024)

<sup>83</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>84</sup>Closer Partners, “15 Soruda Sosyal Medya Yasası Nedir?”, <https://www.closer-partners.com/15-soruda-sosyal-medya-yasasi-nedir/> (01.06.2024)

<sup>85</sup>Closer Partners, “15 Soruda Sosyal Medya Yasası Nedir?”, <https://www.closer-partners.com/15-soruda-sosyal-medya-yasasi-nedir/> (01.06.2024)





Sosyal medya yasası, dijital çağda demokrasi ve bireysel haklar için büyük bir meydan okumayı temsil etmektedir.<sup>86</sup> Teknoloji şirketleri, sivil toplum kuruluşları, yasa koyucular ve kullanıcılar arasında devamlı bir diyalog ve işbirliği gerektirmektedir.<sup>87</sup> Yine yukarıda bahsetmiş olduğumuz şekilde sürekli gelişmekte olan bir alandan bahsediyoruz ve bunun için de bu devamlı diyalog ve işbirliği hususun oldukça önemli bir husus olduğunun altını çizmek gerekmektedir. Bu bağlamda sosyal medya yasalarının pozitif bir yönünü görmüş oluyoruz.<sup>88</sup> Bu yasaların amacı ise dijital alanda sağlıklı bir iletişim ortamını teşvik ederken, aynı zamanda bireylerin haklarını korumak ve toplumsal zararları minimize etmektir.<sup>89</sup>

Sonuç itibarıyla sosyal medya yasaları, internet üzerindeki sosyal medya platformlarının denetim altına alınmasını ve daha güvenli bir ortam sağlama hedefi ile geliştirilmiştir yasalardır. Ancak uygulamasının nasıl gerçekleştirileceği ve hangi sınırların belirleneceği konularında tartışmalar devam etmektedir.

### **Türkiye’de Sosyal Medya Yasası**

Türkiye’de sosyal medya yasası, dijital ortamın giderek artan önemi ve sosyal medya platformlarının toplumsal iletişimdeki merkezi rolü nedeniyle hayati bir konu haline gelmiştir.<sup>90</sup> Ülkemizdeki çıkarılan bu yasalar sosyal medya platformlarının işleyişi ve bu platformlar üzerindeki içeriklerin denetlenmesi ile ilgili birtakım kurallar belirlemeyi amaçlamaktadır.<sup>91</sup> Yasal düzenlemeler, kullanıcıların haklarını korumak, kişisel verilerin güvenliğini sağlamak ve zararlı içeriğin yayılmasını önlemek gibi önemli bir takım amaçlar içermektedir.<sup>92</sup>

<sup>86</sup>Kulaçoğlu Hukuk Bürosu, <https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/> (16.05.2024)

<sup>87</sup>KIRIK, BÖLÜKBAŞ, CENGİZ, “Sosyal Medya Bağlamında Dijital Vatandaşlık: TRT İstanbul Radyosu Prodüktörleri Üzerinden Bir Değerlendirme”,s.7.

<sup>88</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>89</sup>Kulaçoğlu Hukuk Bürosu, <https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/> (13.05.2024)

<sup>90</sup>Kulaçoğlu Hukuk Bürosu, <https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/> (13.05.2024)

<sup>91</sup>Hasan Oymak, “7253 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri”, Ankara Hacı Bayram Veli Üniversitesi Yeni Medya Hakemli Uluslararası E-dergi, Sayı: 9, 2020, ss. 130-133.

<sup>92</sup>Oymak, “7253 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri”, ss. 136-138.



Türkiye'de çıkarılan sosyal medya yasası sadece bireysel manada kişileri bağlayan kısıtlamaların yanı sıra platform sahiplerine belli başlı yükümlülükler de getirmektedir.<sup>93</sup> Ayrıca platformlara Türkiye sınırları içerisinde temsilcilik açmaları konusunda zorunluluk getirmiştir.<sup>94</sup> Bu temsilcilikler ise devletin platformların üzerindeki denetimini kolaylaştırmaktadır. Bununla birlikte yasalara uymayan içeriklerle ilgili daha hızlı eylem yapabilmesine olanak tanıyacaktır.<sup>95</sup> Ayrıca, bu yasalar ile kullanıcı verilerinin korunması konusunda da katı kurallar getirilmiştir. Bu kurallar sayesinde kullanıcıların dijital ortamda güvende olmaları gibi hedefler konulmuştur. Fakat bu yasal düzenlemeler bazı tartışmalara da yol açmaktadır.<sup>96</sup> Birtakım eleştirilenler ve siyasiler bu yasanın ifade özgürlüğü üzerindeki kısıtlayıcı etkilerine dikkat çekmektedir. Bu hususta 27. Dönem Kocaeli Milletvekili Ömer Faruk Gergerlioğlu'nun 23 Temmuz 2020 Tarihli basın açıklamasını ele alabiliriz:

*“Sosyal Medya Yasasıyla özgürlükler kısıtlanmaya çalışılıyor. Sulh Ceza Mahkemelerinin tedbir kararlarının vuku bulması çok tehlikeli! Öncesinde erişim yasağı getirilirken artık içerik silinmesine de karar verebilecek. Bu karar uygulanırken içerik sahibinin haberi olmayacak.”<sup>97</sup>*

Özellikle devletin sosyal medya içeriklerine müdahalesinin genişletilmesi ve sansür uygulamaları çok fazla endişe içeren bir konudur.<sup>98</sup> Devletin bireylerin paylaşımlarına müdahalesi ve sansür uygulamaları ile ilgili daha önce de belirttiğimiz gibi ifade özgürlüğünün ortadan kalkmasına neden olan bir durum söz konusu olmaktadır.<sup>99</sup> Bu durum ise anayasal demokrasinin ortadan kalkması demektir.<sup>100</sup>

<sup>93</sup>Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü”, s. 364.

<sup>94</sup>Closer Partners, “15 Soruda Sosyal Medya Yasası Nedir?”, <https://www.closer-partners.com/15-soruda-sosyal-medya-yasasi-nedir/> (01.06.2024)

<sup>95</sup>Closer Partners, “15 Soruda Sosyal Medya Yasası Nedir?”, <https://www.closer-partners.com/15-soruda-sosyal-medya-yasasi-nedir/> (01.06.2024)

<sup>96</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>97</sup>Gergerlioğlu, TBMM Basın Açıklaması, 23 Temmuz 2020, <https://www.youtube.com/watch?v=uHbk8DCTLcc>, (02.06.2024)

<sup>98</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>99</sup>Ibin, (15.05.2024)

<sup>100</sup>Oymak, “7253 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri”, ss. 129-133.



Sonuç olarak sosyal medya yasasından uygulanması ve sosyal medya platformları ile devlet arasındaki ilişkiler, Türkiye'deki dijital özgürlüklerin geleceği açısından ciddi ve kritik bir öneme sahiptir.<sup>101</sup>

### A. Dezenformasyonla Mücadele Yasası

Dezenformasyon Yasası olarak bildiğimiz lakin tam adıyla Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, 13 Ekim 2022'de TBMM'DE kabul edilmiştir. Ardından 18 Ekim 2022 Tarihinde De 31987 Sayılı Ve 7418 Sayılı Kanun T.C. Resmi Gazetesinde yayınlanarak yürürlüğe girmiştir. Yasa 40 maddeden oluşmaktadır.<sup>102</sup> Yanlış veya doğruluğu bulunmayan, kasıtlı olarak yayılan bilgi ya da bilgi çarpıtma anlamına gelen dezenformasyon<sup>103</sup> ile ilgili maddesi ise aşağıda görüldüğü üzere 29. maddesinde yer almaktadır;

*“MADDE 29- 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununa 217 nci maddesinden sonra gelmek üzere aşağıdaki madde eklenmiştir.*

*“Halkı yanıltıcı bilgiyi alenen yayma*

*MADDE 217/A- (1) Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır.*

*(2) Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır.””<sup>104</sup>*

*“Dezenformasyon Yasası ile birlikte; 5187 sayılı "Basın Kanunu", 5237 sayılı "Türk Ceza Kanunu" ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" isimli yasalar ve maddeleri de düzenlenip gözden geçirilmiş, Türk Ceza Kanunu'nun 217/A maddesine ekleme yapılmıştır.”<sup>105</sup>*

<sup>101</sup>Hasan Oymak, “Kamuoyunda Dezenformasyon Yasası Olarak Bilinen, 7418 Sayılı “Basın Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri”, Ankara Hacı Bayram Veli Üniversitesi Yeni Medya Hakemli Uluslararası E-dergi, Sayı: 13, 2022, ss. 504-505.

<sup>102</sup>TRT Haber, sosyal medya yasası, <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html> (15.05.2024)

<sup>103</sup>Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü” ss. 371-376.

<sup>104</sup> Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Resmi Gazete, <https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm#:~:text=MADDE%20217%2FA%2D%20>, (16.06.2024)

<sup>105</sup>Uçar, “İnternet Ortamında İfade ve Basın Özgürlüğü” ss. 371-376.



Yasanın 29. maddesi Türkiye kamuoyunda oldukça tartışmalı bir ortam yaratmıştır.<sup>106</sup> Zira bu madde bazı taraflarca sansür uygulaması anlamı taşımaktadır. Bazı taraflarca ise böyle bir anlam ifade etmemektedir. Maddeyi inceleyecek olursak eğer hükümet tarafından kontrol edilerek ve sınırlamalar getirilerek yapılacak olan bir işlemdir bu durum. Yani kişinin ifade özgürlüğünü sınırlamak ve paylaşım yaparken kısıtlanarak paylaşımında bulunmasına sebebiyet vermek başta ifade özgürlüğüne karşı bir durumdur. Burada insan haklarının ihlal edildiğini belirtmek gerekmektedir. Bir diğer tarafı ise gerçeğe aykırı bilgi paylaşımının iktidar elinde bulunan basın araçları tarafından yapılması durumunda yine aynı cezai işlemin uygulanıp uygulanmayacak olması hususu vardır. Türkiye şartlarında ne yazık ki bunun mümkün olmayacağını yani iktidarın kendi basın organlarına bu kanunu uygulanmayacak olduğunu yaşayarak görüyoruz her durumda. Bahse konu yasa mecliste AKP ve MHP oylarıyla kabul edilmiş olup CHP tarafından yasanın iptal edilmesi talebiyle anayasa mahkemesine başvuru yapılmıştır.<sup>107</sup> Başvuru sonucunda ise Anayasa Mahkemesi (AYM), bu iptal talebini oy çoğunluğu ile reddetmiştir. Burada iptali istenen konu ise “*Halkı Yanıltıcı Bilgiyi Alenen Yayma*” suçuna 1 yıldan 3 yıla kadar ceza verilmesi hususudur.<sup>108</sup>

Sonuç itibarıyla bu yasa bütün iptal istemelerine rağmen şu an yürürlükte olup uygulanmaktadır. Sansür Yasasına karşı olarak yapılan eylemler ise ne yazık ki yine olumlu bir dönüt almamıştır.

## Sonuç

*Sosyal Medya Ekseninde İfade Özgürlüğünü* ele aldığımız çalışmada, konuyu tüm yönleriyle ortaya koyarak geniş bir çerçeveden durum değerlendirilmeye tabi tutuldu. Öncelikle geleneksel medya ile yeni medyanın en önemli farkının etkileşim olduğunu belirttik ki bu şekilde sosyal medyanın amacını ortaya koymuş oluyoruz. Etkileşim almak ya da vermek için oluşturulmuş olan sosyal medya bireylerin, nefret söylemine bulaşmadan fikirlerini özgürce ifade etmesi gereken internet tabanlı bir sosyal alandır. İfade özgürlüğü ise bireylerin en doğal haklarından birisi olarak Anayasamızın 25. Ve 26. Maddeleri ile ortaya koyulmuştur.

<sup>106</sup>Anayasa Mahkemesi 'Dezenformasyon Yasası'nın iptal talebini reddetti, BBC News <https://www.bbc.com/turkce/articles/c9731e066vjo#:~:text=Kamuoyunda%20%22Dezenformasyon%20Yasas%C4%B1%22%20olarak%20bilinen,kadar%20hapis%20cezas%C4%B1yla%20cezaland%C4%B1r%C4%B1lmas%C4%B1%20%C3%B6ng%C3%B6r%C3%BCld%C3%BC> , (16.06.2024)

<sup>107</sup>Ibin, (16.06.2024)

<sup>108</sup>Oymak, “Kamuoyunda Dezenformasyon Yasası Olarak Bilinen, 7418 Sayılı Basın Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun’un Getirdikleri”, s .507.



Çalışmamız kapsamında ele almış olduğumuz örneklerden de anlaşılacak olduğu üzere ne yazık ki sosyal medya eksenin de bir ifade özgürlüğünden bahsetmemiz mümkün değildir. Zira şarkıda geçtiği gibi her şeyin bir bedeli var. Fikirlerinizi özgürce ifade edebilmek için atmış olduğunuz bir tweet'ten dolayı para cezasına ya da hapis cezasına çarptırılılabiliyorsunuz. Yine incelemiş olduğumuz örneklerden gördüğümüz üzere sosyal medyada özgürce fikir beyan etmek için ülkemiz ne yazık ki güvenli bir bölge değildir. Gerek yapılan anayasal düzenlemeler gerekse uygulanan cezai işlemler göstermiştir ki ülkemizde sosyal medya alanında ifade özgürlüğü söz konusu değildir.

Son söz olarak makale içerisinde üzerinde durulan Dijital Vatandaşlık Eğitimi hakkında detaylandırma yapmakta bir beis görmüyorum. Otuz yıldır aşkın bir süredir gerek bireysel gerekse toplumsal bazda hayatımızı derinden etkileyen teknolojik gelişmeler, siber uzay olarak adlandırılmış olduğumuz yeni bir hareket alanını dahilinde karşımıza çıkmaktadır. Çalışma kapsamında işlenen sosyal medya konusu da bu yeni hareket alanı içerisinde önemli bir yere sahiptir. Gerek ekonomikk ve siyasi gerekse sosyal ve kültürel alanlarda varlığını ciddi anlamda idrak ettiğimiz Siber Uzay, bireseyl olarak kendimizi koruyabilmenin önemini her geçen gün ortaya koymaktadır. Zira telgrafını icadından yapay zekaya kadar olan süreç içerisinde bütün şartlar değişikliğe maruz kalmıştır. Fakat bir şey değişmemiştir ki, o da bireylerin kendi güvenliği için kendisinin uğraş vermesi hususudur. Bireylerin ortamlara göre farklı adlandırmalarla karşılaştığımızı biliyoruz. Siber uzayda da bireyler olarak hepimiz birer Dijital Vatandaşız! Ve bu noktada güvenliğimizi sağlayabilmek adına biliçli birer dijital vatandaş olmak durumundayız. Bilinçli bir vatandaş ve bilinçli bir dijital vatandaş görev, sorumluluk ve haklarının bilincindedir ve bu doğrultuda hareket eder. Dijital Vatandaşlık Eğitimi tam olarak bunun için önem arz etmektedir. Bu eğitim ile şu soruların cevaplarını alarak, görev, sorumluluk ve haklarımızın farkına varacağız; Dijitalleşen Dünyanın Vatandaşları Kimlerdir? Dijitalleşen Dünya Ne Demektir? Dijital Vatandaş Kimdir? Bilinçli Dijital Vatandaş Olmak Ne Demektir? Dijital Vatandaşlık Eğitimi Nedir? Neden Dijital Vatandaşlık Eğitimine İhtiyaç Duyarız? Dijital Vatandaşlar Ne Gibi Özellikler Taşımalıdırlar? Paydaşları Ve Sorumlulukları Nelerdir? Ne Gibi Politika Ve Önerilere İhtiyaç Duyulmaktadır? Etik Eğitimi, Barış Eğitimi Ve İnsan Hakları Eğitimi İle İlişkisi Var Mıdır? Dijital Vatandaş Eğitimini Kimler Almalıdır? Dijital Vatandaşlığın Unsurları Nelerdir? Dijital Vatandaşlık Eğitimi Kim Tarafından, Kim İçin Ve Kimlere Verilir? Dijital Vatandaş Eğitimi Nasıl Olmalıdır?



## Kaynakça

- AKPINAR Mehmet, (02.06.2024). "Sosyal Medya Nedir? Bilmeniz Gerekenler". Mehmet Akpınar Blog. Erişim tarihi: [Erişim Tarihi]. <https://mehmetakpinar.com/blog/sosyal-medya-nedir-bilmeniz-gerekenler/>
- AKYEŞİLMEN, Nezir. Siber Politika ve Güvenlik. Ankara: Orion Kitabevi, 2018
- AKYEŞİLMEN Nezir, Siber Uzay Ders Notları, 2022
- ANAYASA MAHKEMESİ, "Dezenformasyon Yasası'nın iptal talebini reddetti", BBC News. Erişim tarihi: 16.06.2024, <https://www.bbc.com/turkce/articles/c9731e066vjo#:~:text=Kamuoyunda%20%22Dezenformasyon%20Yasas%C4%B1%22%20olarak%20bilinen,>
- ALBY Tom, "Web 2.0", chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/[https://files.hanser.de/Files/Article/ARTK\\_LPR\\_9783446415805\\_0001.pdf](https://files.hanser.de/Files/Article/ARTK_LPR_9783446415805_0001.pdf), (30.07.2024)
- AYDOĞAN Filiz, KIRIK Ali Murat, "Alternatif Medya Olarak Yeni Medya", Akdeniz İletişim Dergisi.
- AYGEN Reha Talha, "Devlet, Siyaset Ve Organize Suç Örgütleri: Reis Sedat Peker Örneği", Uluslararası Sosyal Ve Beşeri Bilimler Araştırma Dergisi, Cilt. 8, Sayı 76, 2021.
- BALOĞLU, Çiğdem, (2006). İfade Özgürlüğü [Yayınlanmış Yüksek Lisans Tezi]. Kocaeli: Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü
- RESMÎ GAZETE, Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun,. Erişim tarihi: 16.06.2024, <https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm#:~:text=MADDE%20217%2FA%2D%20>
- BAŞARAN BURAL, E. (2021). Sosyal Medya İstihbaratı. İstanbul: Yeditepe Yayınları.
- BOSTANCI, Mustafa. Sosyal Medya Dün,Bugün,Yarın. Konya: Palet Yayınları, 2019.
- BYCHAWSKA-SINIARSKA Dominika "Avrupa İnsan Hakları Sözleşmesi Kapsamında İfade Özgürlüğünün Korunması", Avrupa Konseyi, 2028.
- CLOSER Partners.(01..06..2024)"15 Soruda Sosyal Medya Yasası Nedir?" Closer Partners web sitesinden erişildi:[Erişim tarihi]<https://www.closer-partners.com/15-soruda-sosyal-medya-yasasi-nedir/>
- ÇİLDAN Cihan, Mustafa Ertemiz, Evren Küçük, H. Kaan Tumuçin, Duygu Albayrak, "Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü", Akademik Bilişim Konferansı, 2012.





GERGERLIOĞLU, TBMM Basın Açıklaması, 23 Temmuz 202. YouTube video. Erişim tarihi: 02.06.2024, <https://www.youtube.com/watch?v=uHbk8DCTLcc>

GERGERLIOĞLU, Ö.F. (02.06.2024). "HalkTV Sözüm Var". Youtube video dosyası, <https://www.youtube.com/watch?v=7OBiDLKnF4U>

GÖKER Göksel, KESKİN Savaş, "Sosyal Medya Türevi Olarak Sosyal İçerik Platformları: Betimsel Bir İnceleme" Uluslararası Sosyal Araştırmalar Dergisi, Cilt: 8, Sayı: 39, Ağustos 2015.

GÜNEŞ Felemez, GÜNEŞ Zeynep, "İfade Özgürlüğünün Sosyal Medya İçin Taşdığı Anlam", VII. Hukukun Gençleri Sempozyumu, İstanbul, 22-23 Aralık 2016.

GÜREL, Begüm Av., "Bağımsız Bir Hakime Göre Anayasa Mahkemesinin Kararlarının Bağlayıcılığı". BGHukukBurosusu.com.tr sitesinden erişildi: [Erişim Tarihi], <https://www.bghukukburosusu.com.tr/9613/>

EUROMSGEXPRESS. (31.05.2024). "Sosyal Medya Nedir?" Euromsgexpress.com sitesinden erişildi: [Erişim Tarihi], [https://www.euromsgexpress.com/sosyal-medya-nedir/?gad\\_source=1&gclid=CjKCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd2l9LjtI6zPoONWpSnMzDzTuk8aArAEALw\\_wc](https://www.euromsgexpress.com/sosyal-medya-nedir/?gad_source=1&gclid=CjKCOjw6uWyBhD1ARIsAIMcADpy1tpJyAntU6enf8rVgyLqpnQjd2l9LjtI6zPoONWpSnMzDzTuk8aArAEALw_wc)

ERDOĞAN, Mustafa. (2016). İnsan Hakları Teorisi ve Hukuku. Ankara: Orion Kitabevi.

KIRIK Ali Murat, Kenan BÖLÜKBAŞ Kenan, CENGİZ Gönül, "Sosyal Medya Bağlamında Dijital Vatandaşlık: TRT İstanbul Radyosu Prodüktörleri Üzerinden Bir Değerlendirme", Mavi Atlas Dergisi, Cilt.7, Sayı 2, 2019

KULAÇOĞLU HUKUK BÜROSU, (16.05.2024) "Yeni Sosyal Medya Kanunu" Kulaçoğlu Hukuk Bürosu web sitesinden erişildi :[Erişim tarihi]<https://kulacoglu.av.tr/yeni-sosyal-medya-kanunu/>

METATIME, <https://metatime.com/tr/blog/web-10-nedir-web-20-nedir#!> (10.05.2024)

OYMAK Hasan, "7253 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun'un Getirdikleri", Ankara Hacı Bayram Veli Üniversitesi Yeni Medya Hakemli Uluslararası E-dergi, Sayı: 9, 2020

OYMAK Hasan, "Kamuoyunda Dezenformasyon Yasası Olarak Bilinen, 7418 Sayılı "Basın Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un Getirdikleri", Ankara Hacı Bayram Veli Üniversitesi Yeni Medya Hakemli Uluslararası E-dergi, Sayı: 13, 2022.

ŞEN Fulya, ŞEN Y. Furkan, "Sosyal Medya, İletişim Hakkı Ve İfade Özgürlüğü Üzerine Bir Değerlendirme", Gazi Üniversitesi, İlibf Dergisi, Cilt. 17, Sayı 2, 2015.



TAŞ Eray, Yeni Medyada Nefret Söylemi, Yeni Medya Elektronik Dergisi, Cilt. 1, Sayı 1, 2017

T.C. 82 ANAYASASI.

<https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/illeridairesi/Mevzuat/Kanunlar/Anayasa.pdf>

T.C. ANAYASA MAHKEMESİ, Genel Kurul Kararı,

<https://kararlarbilgibankasi.anayasa.gov.tr/BB/2019/10634> (28.07.2024)

TRT HABER. (02.06.2024). "Sosyal Medya Yasası Nedir?". TRT Haber web sitesinden erişildi: [Erişim Tarihi], <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html>

TRT HABER. (15.05.2024). "Sosyal Medya Yasası Nedir? Maddeleri Nelerdir?" TRT Haber web sitesinden erişildi: [Erişim Tarihi], <https://www.trthaber.com/haber/guncel/sosyal-medya-yasasi-nedir-maddeleri-nelerdir-713608.html>

UÇAR Jindar, "İnternet Ortamında İfade ve Basın Özgürlüğü", Hukuk Fakültesi Dergisi, Yıl: 7, Sayı 2, Aralık 2021.

UYANIK Faik, "Sosyal Medya Kurgusallık Ve Mahremiyet", 7 Mayıs 2013 tarihli Kocaeli Üniversitesi Yeni Medya Kongresinde sunulmuş bildiridir. s.8.

YEŞİLDAL Ali. "Sosyal Medya, Yerel Yönetimler Ve Katılımcı Yönetim: Bilgi Çağında Belediyeler İçin Yeni Stratejiler". İnsan Ve İnsan 6, sy. 22 (Ekim 2019)

YOUTUBE, (02 Haziran 2024)"Sedat Peker Açıklama Videoları." Youtube video dosyası. <https://www.youtube.com/watch?v=QJx4CABC7oE>





**ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ**

76



## DIPLOMACY IN THE DIGITAL AGE

*Brian Hocking ve Jan Melissen.(2015). Ethics in Digital Era. Clingendael Report. 58 p.*

**Gül Nazik ÜNVER\***

**ORCID-ID: 0009-0005-5003-1555**

Clingendael Institute tarafından yayımlanan bu önemli eser, Brian Hocking ve Jan Melissen tarafından rapor olarak kaleme alınmıştır. Kitap, dijital teknolojilerin diplomasi üzerindeki etkilerini ve diplomasi pratiğinin nasıl evrildiğini incelemektedir. Dijitalleşmenin diplomasiye getirdiği fırsatlar ve zorlukları tartışarak, modern diplomasi uygulamalarına dair kapsamlı bir perspektif sunmaktadır. Dijital teknolojilerin diplomasiye entegrasyonu ve bu sürecin getirdiği yenilikler incelenirken, dijital diplomasinin doğası, yeni diplomatik araçlar ve yöntemler de tartışılmakta ve geleneksel diplomasi ile karşılaştırmalı bir analiz sunulmaktadır.

Hocking ve Melissen, dijital teknolojilerin devletlerarası ilişkileri nasıl dönüştürdüğünü ve diplomatların yeni medya araçlarını nasıl kullandığını örneklerle açıklamaktadır. Özellikle dijital diplomasi ile gelen şeffaflık, hız ve etkileşim imkânları üzerinde durulmuştur. Dijital araçların kriz yönetimi, halkla ilişkiler ve kamu diplomasisi gibi alanlarda nasıl kullanıldığına dair bazı somut örnekler verilmiştir. Sosyal medya, dijital iletişim araçları ve veri analizinin diplomatların iş yapış biçimlerini nasıl değiştirdiği üzerinde durulmuştur. Ayrıca, dijital diplomasinin devletlerarası ilişkiler, uluslararası kuruluşlar ve sivil toplum üzerindeki etkileri de incelenmiştir. Ancak, kitabın teorik çerçevesi zaman zaman yetersiz kalmakta ve pratik örneklerin derinliği tartışmalıdır.

Hocking ve Melissen, farklı ülkelerden ve uluslararası kuruluşlardan örnekler vererek, dijitalleşmenin küresel diplomasi pratiği üzerindeki etkilerini göstermektedir. Özellikle dijital diplomasi uygulamalarında öncü olan ülkeler ve bu ülkelerin diplomatik stratejileri incelenmektedir. Ayrıca, dijitalleşmenin diplomatik hiyerarşi ve karar alma süreçlerini nasıl etkilediği de ele alınmaktadır. Ancak, dijital diplomasinin doğasını ve yeni diplomatik araçları tartışırken, bazı önemli detaylar göz ardı edilmiştir. Örneğin, dijital teknolojilerin getirdiği

---

\* Dr., Lecturer, Batman University, Batman-Türkiye. E-mail: gulunver@outlook.com



etik ve gizlilik sorunları yeterince ele alınmamıştır. Ayrıca, yazarlar dijital diploması ile gelen şeffaflık ve hızın olumsuz yanlarına yeterince değinmemişlerdir. Dijital araçların diplomatik yanlış anlamalara ve bilgi kirliliğine yol açabileceği gerçeği daha fazla vurgulanması gerekmektedir. Ancak, bazı kritik kurumlar ve dijital diplomasının öncüsü olan aktörlerin daha detaylı şekilde incelenmesi, konunun derinlemesine analiz edilmesini sağlayacaktır. Örneğin, Çin ve Rusya'nın dijital diploması stratejilerinin kitabın ana bölümlerinde daha fazla yer alması, konuyu daha anlaşılır kılacaktır. Kitap, beş bölümden oluşmaktadır: Dijital Çağda Diplomasıye Giriş, Dijital Çağı Tanımlamak, Çevrimdışı ve Çevrimiçi Perspektifler, Diplomasının Değişen DNA'sı ve Sonuç. Kitapta her bölüm, bir öncekini tamamlayacak şekilde ilerlemekte ve ana temalar sistematik bir şekilde ele alınmaktadır. Giriş, gelişme ve sonuç bölümleri arasındaki geçişler düzgün ve anlaşılırdır. Her bölümde, dijital diplomasının farklı yönleri detaylı bir şekilde ele alınmakta ve okuyucuya bütüncül bir perspektif sunulmaktadır.

Dijital Çağda Diplomasıye Giriş bölümünde, dijital çağda diplomasının tanımı yapılmakta ve bu yeni dönemin diplomasıye getirdiği sorular ve belirsizlikler tartışılmaktadır. Yazarlar, dijital diplomasının çevrimiçi ile çevrimdışı diploması arasındaki hibrit yapısını incelemektedir.

Dijital Çağı Tanımlamak bölümünde, dijital çağın genel bir tanımı ve tarihsel bağlamı üzerine durulmuştur. Dijitalleşmenin diploması üzerindeki etkileri, büyük veri kullanımı ve hükümetlerin ağ toplumuna adaptasyonu gibi konular tartışılmaktadır. Bu bölümde, dijital çağın getirdiği fırsatlar ve zorluklar ele alınmaktadır.

Çevrimdışı ve Çevrimiçi Perspektifler bölümünde, dijital diplomasıde güven ve iletişimin önemini tartışılmaktadır. Dijital diplomasının farklı kategorileri ve bu kategorilerin nasıl işlediği incelenmektedir. Ayrıca, dijital teknolojilerin diploması üzerindeki yıkıcı etkileri ve diplomatların dijital diploması hakkındaki yorumları ele alınmaktadır.

Diplomasının Değişen DNA'sı bölümünde, dijital teknolojilerin diplomatik süreçleri nasıl dönüştürdüğü ve dış politika üzerindeki etkileri incelenmektedir. Dijital çağda kamu diplomasısının rolü, bilgi yönetimi, politika yönetimi ve müzakere süreçleri tartışılmaktadır.



Son bölümde, kitabın genel bir değerlendirmesi sunulmakta ve dijital diplomasinin geleceği hakkında öngörülerde bulunmaktadır. Dijitalleşmenin diplomasi pratiği üzerindeki uzun vadeli etkileri ve bu alandaki potansiyel gelişmeler ele alınmaktadır.

Hocking ve Melissen, akademik bir üslupla fakat anlaşılır ve akıcı bir dil kullanarak konuyu ele almaktadır. Kitap, okuyucunun dikkatini çekecek şekilde yapılandırılmış ve konular açıklanmıştır. Akademik referanslar ve örneklerle desteklenen anlatım, okuyucunun konuyu anlamasına yardımcı olmaktadır. Kitapta kullanılan dil, hem akademik çevreler hem de diplomasiye ilgi duyan genel okuyucular için uygun ve erişilebilirdir. Ancak, bazı bölümlerde dilin fazla teknik ve kuru olması, genel okuyucu kitlesinin ilgisini kaybetmesine neden olabilecektir. Ayrıca, kitabın bazı bölümlerinde tekrarlar ve gereksiz detaylar, okuyucunun ana konudan uzaklaşmasına yol açabilmektedir.

Kitabın özellikle dijital diplomasinin pratik uygulamaları ve sosyal medyanın diplomasi üzerindeki etkileri hakkındaki bölümleri dikkat çekicidir. Bu bölümler, somut örneklerle zenginleştirilmiş olup okuyucuya dijital diplomasinin gerçek dünyadaki yansımalarını göstermektedir. Özellikle sosyal medya kampanyaları, dijital kriz yönetimi ve çevrimiçi etkileşim stratejileri üzerine yapılan tartışmalar, dijital diplomasi konusunda bilgi sunmaktadır. Ancak, bu bölümlerde verilen örneklerin bir kısmı yüzeysel kalmakta ve daha derinlemesine analizler gerekmektedir. Özellikle, sosyal medya kampanyalarının başarısızlıkları ve bu başarısızlıkların diplomatik ilişkilere etkileri daha ayrıntılı incelenmesi önem arz etmektedir.

“Diplomacy in the Digital Age”, dijitalleşmenin diplomasi üzerindeki etkilerini anlamak isteyenler için değerli bir kaynak olsa da, bazı eksiklikleri ve yüzeyselliği nedeniyle tam anlamıyla tatmin edici değildir. Kitap, dijital teknolojilerin sunduğu fırsatları ve karşılaşılan zorlukları dengeli bir şekilde ele almakta, ancak yetersiz bir şekilde incelenen önemli konular bulunmaktadır. Kitabın teorik ve pratik boyutlarının daha dengeli bir şekilde ele alınması, okuyuculara daha kapsamlı bir bakış açısı sunulmasını sağlayacaktır. Ancak, dijital diplomasinin daha eleştirel ve derinlemesine bir analizini arayanlar için ek kaynaklar araştırmak faydalı olabilir.

Sonuç olarak “Diplomacy in the Digital Age”, dijital teknolojilerin diplomasi dünyasındaki rolünü anlamak için iyi bir başlangıç noktası sunmakta, ancak daha kapsamlı ve eleştirel bir



bakış açısı arayanlar için yeterli derinliği sağlamamaktadır. Dijitalleşmenin diploması üzerindeki etkilerini derinlemesine anlamak ve bu alandaki güncel gelişmeleri takip etmek isteyen herkes için faydalı olacaktır. Ayrıca, dijital stratejiler geliştirmek isteyen diplomatlar ve politika yapıcılar için de önemli bir rehber niteliğindedir. Bu kitap, modern diplomasinin geleceğine dair geniş bir perspektif sunarak, dijital çağın gerekliliklerine uyum sağlamak isteyen herkes için önemli bir kaynaktır. Dijital teknolojilerin diploması üzerindeki etkilerini anlamak isteyen akademisyenler, öğrenciler ve profesyoneller için değerli bir kaynak olabilir. Ancak, bazı eksiklikleri ve eleştiriye açık noktaları olduğu unutulmamalı ve ek kaynaklardan yararlanılması konuyu daha anlaşılır kılacaktır.



## SPACE TRAVEL: TEN SHORT LESSONS

*By Paul Parsons, Maryland: Johns Hopkins University Press, 2020, pp. 192*

**Neslihan TOPCU\***

**ORCID:** [0000-0002-0822-0062](https://orcid.org/0000-0002-0822-0062)

The main point of Paul Parsons' book *Space Travel: Ten Short Lessons* is to inform to the reader the process from the developments that led to the beginning of space travel to the moment when space travel took place. In addition, Parsons also focuses on possible future space-related projects. In other words, the book conveys the past, present and future of space travel to the reader.

One of the most important aspects about the book is that the language of the book is quite simple. Information about a complex field such as space is given in a way that everyone, whether interested in space or not, can understand. Many books about space can be very difficult to understand due to the abundance of technical information. However, in this book, even technical information expresses in a way that readers from all strata can understand.

Another aspect that makes the book easier to understand is that the technical details mentioned in the book are shown with visuals. In this way, a schema is formed in the reader's mind about the subject such as the spacecraft. And what's more, space programs, launched rockets, space flights and similar information are also collected in tables. Thus, analysis of information has become easier. All these details in the book contributed to the understanding of the subject and the fluency of the book.

As understood from the name of the book, it consists of ten main chapters. In the first chapter, "How Far We've Come", the emergence of the rocket, the studies on orbit, the Moon and Mars are discussed. But it is noteworthy that in this chapter the subject is mainly focused on US space studies. Apart from mentioning Russia's actions in a few places, considering that many countries such as China, India and Japan have space travel capabilities, not mentioning such states is an incomplete approach.

---

\* PhD Student at Department of International Relations, Selcuk University-Konya-Turkey. She works on Space Politics in Ir. Can be accessed via e-mail: [neslihan.topcu@outlook.com](mailto:neslihan.topcu@outlook.com)



In the second chapter, “How to Leave the Planet”, discusses the development of rocket technology, from fiery arrows to today’s rockets. Unlike the launch of the rockets in the first chapter, more technical information about the rocket is included in this chapter. The first chapter mostly contained the stories of rocket scientists discovering the rocket.

In the third chapter, “Use the Force”, the dynamics of space are mentioned. In this context, information about the gravitational force, orbit types and Lagrange points is given. It is emphasized that planning space travels by knowing the dynamics of space provides both safer and more convenient movement in space.

In the fourth chapter, “How to Stay Alive in Space”, the dangers of space travel and those who lost their lives during space travel are mentioned. The subject is supported by giving many examples of accidents in space. In this regard, it is referred what should be taken into consideration to make the journeys of astronauts safe.

In the fifth chapter, “When to Let the Machines Take Over”, Parsons, who talked about the difficulties related to the process from going to space to returning from space in the previous chapter, emphasizes in this chapter that it will be easier to overcome such difficult tasks thanks to robots in the coming years. In this way, human losses will decrease, and it will be possible to explore planets that are difficult for humans to go to, through robots. Accordingly, Parsons gave examples of some robotic missions sent to the Moon and Mars. Parsons adopts an approach that in the future, robots will assist humans in challenging tasks rather than replacing them.

In the sixth chapter, “Space Is Big Business”, discusses the commercial use of space. In this context, space tourism is elaborated. It focuses on space companies such as Virgin Galactic and SpaceX and their activities. In addition to space tourism, precious stones and energy resources found in space are also referred as another commercial dimension of space. In this context, Helium-3, a rare substance, stands out.

In the seventh chapter, “The Next Giant Leap Has Already Begun”, he talks about the projects that have been carried out and planned for the future on the Moon, Mars, Jupiter and Saturn. Giving the plans for planets and satellites of various countries such as the USA, European countries, Japan, India and China under this section has been a good attitude in terms of revealing the diversity in space studies.



In the eighth chapter, “It’s a Small Solar System”, the difficulties and alternative solutions brought about by going beyond the sun are touched on. Here, solar sails come to the fore. When some technical information about solar sails is given, it is stated that the realization of this project will pave the way for humanity to reach the stars.

In the ninth chapter, “There’s No Place Like Space”, it is explained through examples how difficult it is to fulfil basic needs such as eating, going to the toilet, and maintaining one’s health on the International Space Station. Because of these difficulties, the idea of establishing space stations on surfaces such as the Moon and Mars is being discussed. In this regard, the concept of terraforming is mentioned. It describes the construction of a structure similar to life on Earth on the surface of another planet.

In the tenth chapter, “How to Reach the Stars”, information is given about the technical infrastructure and equipment required to reach the stars. There is discussion about what kind of technologies can come this dream true or not. And all, within this scope, the claims by various scientists about the nature of space are addressed in this chapter.

In the book, Parsons generally discussed both social (states’ space goals) and technical (how these goals will be achieved) issues related to space. The book creates in people the idea that space is becoming more accessible and that systems on Earth are becoming more and more integrated into space. In the 21<sup>st</sup> century, in the age of information and technology, states staying away from space policy and studies can damage to their own interests in the long term. Therefore, it is important to publish such works in order to increase the awareness of both states and individuals about space. Additionally, Parsons left a reading list at the end of the book. It is a good contribution for readers who want to deepen their reading in this field.





## NOTES FOR AUTHORS / YAZARLAR İÇİN NOTLAR

We would like to thank you for choosing to submit your paper to *Cyberpolitik*. In order to fasten the process of reviewing and publishing please take try to read and follow these notes in depth, as doing so will ensure your work matches the journal's requirements.

All works including research articles, comments and book reviews submitted to *Cyberpolitik* need to be original contributions and should not be under consideration for any other journal before and/or at the same time.

All submissions are to be made online via the Journal's e-mail address: cyberpolitik@gmail.com

The authors of a paper should include their full names, affiliations, postal addresses, telephone numbers and email addresses on the cover page of the manuscript. The email address of the author will be displayed in the article.

Articles should be **1.5-spaced** and with standard margins. All pages should be numbered consecutively. Please avoid breaking words at the end of lines.

The articles need to be between 5000 - 7000 words (including footnotes and references); comments between 2000-4000 words (including footnotes and references); and book - article reviews between 500 - 1500 words.

An abstract of up to 150 words should be added during the submission process, along with an average of five keywords.

Authors should make a final check of their article for content, style, proper names, quotations and references.

All images, pictures, maps, charts and graphs should be referred to as figures and numbered. Sources should be given in full for images, pictures, maps, tables and figures.

### ***Comments in Cyberpolitic***

A comment is a short evaluation of an expert regarding new issues and/or development in cyberpolitics.

Comments require journal's full reference style.

### ***Book / article Reviews in Cyberpolitic***



A book review should provide a fair but critical assessment of a recent (not older than 5 years) contribution to the scholarly literature on the themes and topics relevant to the journal.

***A book review for Cyberpolitik:***

- provides complete bibliographical references of the book(s) and articles to be reviewed.
- summarizes the content and purpose of the book, focusing on its main argument(s) and the theory, methodology and empirical evidence employed to make and support these arguments
- Critically assesses the author(s)' arguments, their persuasiveness and presentation, identifying the book's strengths and weaknesses
- presents a concluding statement that summarizes the review and indicates who might benefit most from reading the book

Book / article reviews should be preceded by full publication information, in the following form:

*Education for Peace: Politics of Adopting and Mainstreaming Peace Education Programs in Post-Conflict Settings* by Vanessa Tinker, Academica Press, 2015, \$81.62 (Hardcover), ISBN 978-1680530070.

The reviewer's name, affiliation and email address should appear, on separate lines, at the top of the review, right after the bibliography of the book/article.

***Journal style***

Authors are responsible for ensuring that their manuscripts conform to *cyberpolitik's* reference style.

Reference style of *Cyberpolitik* is based on APA 6th Edition.

