YENİ MEDYA
DERGİSİ
Hakemli, uluslararası, e-Dergi

Sayı Vol., 18, Bahar Spring, (2025)
https://dergipark.org.tr/tr/pub/yenimedya
DOI » https://doi.org/10.55609/yenimedya.1626763

Data Violence in Networked Environments: A Study on User Experience

Ağ Bağlantılı Ortamlarda Veri Şiddeti: Kullanıcı Deneyimi Üzerine Bir İnceleme

Hasan Hüseyin KAYIŞ

Araştırma Makalesi Research Article Başvuru Received: 25.01.2025 ▪ Kabul Accepted: 19.03.2025

ABSTRACT

In the context of networked environments, communication with other network users can introduce the element of violence into everyday life. In this case, users may encounter data violence in social media applications, which is a form of violence transferred to networked environments. In this study, data violence encountered by users in social media environments is discussed. Identifying the factors that lead to data violence is important in identifying the problem. This study aims to provide a framework for what can be done in the face of these actions that cause serious harm, along with the factors that cause data violence to occur and continue. The complaints of ordinary users about social media environments on an online complaint platform were collected through document analysis and qualitative content analysis was applied to the data. The findings showed that data violence occurs under different categories, from user to user or platform to user. Platforms' solutions to data violence are inadequate. To prevent data violence caused by the technical infrastructure of the platforms, the need for ethical design and ethical operation of the platforms was emphasized and the duties of the authorities were emphasized.

Keywords: Data, Data Violence, Social Media, Users, Ethics.

ÖZ

Ağ bağlantılı ortamlarda gerçekleşen iletişimde ağdaki diğerleri ile temas etmek gündelik hayattaki şiddet unsurunu bu ortamlara taşıyabilmektedir. Bu durumda kullanıcılar sosyal medya uygulamalarında şiddetin ağ bağlantılı ortamlara taşınmış biçimi olan veri şiddeti ile karşılaşabilmektedir. Bu araştırmada kullanıcıların sosyal medya ortamlarında karşılaştıkları veri şiddeti ele alınmıştır. Veri şiddetine yol açan etmenlerin ortaya koyulması sorunun tespitinde önemlidir. Bu çalışmada veri şiddetini ortaya çıkaran ve sürmesine neden olan etmenlerle birlikte ciddi zarar oluşturucu bu eylemler karşısında neler yapılabileceğine dair bir çerçeve sunulması amaçlanmıştır. Bir çevrimiçi şikâyet platformunda yer alan sosyal medya ortamlarıyla ilgili sıradan kullanıcıların şikayetleri doküman incelemesi tekniğiyle toplanmış ve söz konusu verilere nitel içerik analizi uygulanmıştır. Bulgular veri şiddetinin farklı kategoriler altında, kullanıcıdan kullanıcıya ya da platformdan kullanıcıya şeklinde gerçekleştiğini göstermiştir. Platformların veri şiddeti konusundaki çözümleri yetersizdir. Platformların teknik altyapılarından kaynaklı veri şiddetinin önlenebilmesi için yine platformların etik bir biçimde tasarlanması ve etik bir biçimde işletilmesi gereğinin üzerinde durulmuş, otoritelerin görevleri vurgulanmıştır.

Anahtar Kelimeler: Veri, Veri Şiddeti, Sosyal Medya, Kullanıcılar, Etik.

Introduction

Data shared in networked environments causes ordinary people to be subjected to data violence[1]. Essentially, this action is a form of everyday life transferred to networked environments. These acts are frequently encountered when violence in everyday life is transferred to networked environments through data. The victims of this action are usually ordinary people. The victimizers are both the perpetrators and the platforms themselves. Platforms have to prevent victimization. Platforms need to manage data well, protect privacy, and prevent conflicts of interest so that users are not victimized in the same way as in real life. All this is necessary to prevent users from being subjected to different categories of data violence in the networked environment. Data violence occurs when these tasks are not fulfilled.

Despite the long-standing presence of data in our lives, the history of our engagement with its networked form is a recent development. Since its emergence, there has been no consensus on how to approach it, with the initial approaches to networked data being accompanied by instrumental approaches and a technological determinist perspective. However, the possibility of data misuse has also been discussed. The extent to which digital monitoring implemented by different institutional actors can contribute to injustice and inequality has been discussed. However, there have been no positive developments in protecting or informing users against the algorithmic processes of networked technologies, supported at the institutional level. In particular, issues such as digital literacy, public access, privacy, or especially how networked data is shared regarding the internet and digital devices are not experienced equally by all users (Nissenbaum, 2010; Gangadharan, 2017: 597). Luciano Floridi attributes this to the two-faced nature of technology. The optimistic side of such technologies focuses on the users and consists of the interfaces that allow them to use them. However, the part that operates with different protocols, is technically invisible to users, and they begin to perceive the technology with optimism as they did in its first use (Floridi, 2024: 62). This is the reason for both users' frustration and reactions to the data violence they experience in social media environments.

Problems with data usage

Current academic discourse concerning networked technologies oscillates between evoking a sense of moral panic and conceptualizing technology as a comprehensive solution. The inherent inaccuracies in data-driven systems, the inadequacy of algorithmic frameworks, or a combination of both factors, give rise to discrimination predicated on "advanced technology," as evidenced in media narratives and prevailing societal discourses, particularly within the American context. The repercussions of misclassifications, excessive targeting, systemic barriers, and erroneous predictions have a disproportionate impact on particular demographic cohorts, especially those who have been historically marginalized. To mitigate this predicament, a diverse array of scholars advocate for the adoption of equitable, accountable, and transparent machine-learning frameworks to avert the reinforcement of biased, racist, or sexist systems (Leavy, 2018).

However, it is evident that further actions are imperative. With each subsequent scandal involving surveillance, electoral manipulation, and workforce displacement, the significance of ethical practices within technological domains becomes increasingly apparent. Technology corporations themselves also underscore the enduring consequences of digital technologies internally yet offer limited direction on how ethical considerations can be integrated into technical processes beyond the formal structures of the organization. These methodologies further treat

[1] Data violence is a concept closely associated with digital inequalities. For a more detailed discussion of this topic, please refer to the following sources: Kayış, H. H. (2021). Dijital Eşitsizlikleri Yakindan İncelemek: Dijital Uçurum Buzdağinin Görünen Yüzü Müdür? Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli E-Dergisi, (15), 109-124.

ethics as a hierarchical set of directives, formulated by CEOs and subsequently executed by designers. A robust techno-ethics must challenge these hierarchical tendencies (Amrute, 2019: 57). Despite, or perhaps owing to, such sensitivities concerning ethics, numerous high-profile corporations, organizations, and communities are utilizing public discourse to articulate their ethical commitments. Nevertheless, many of these initiatives are deficient in a coherent vision for the ethical or responsible advancement of Artificial Intelligence and Machine Learning systems, wherein "values" are not adequately considered.

It would be more fitting to elucidate this circumstance through a specific illustration. In May 2013, a cohort of 200 esteemed individuals was convened at the Grove Hotel in Hertfordshire, England for Google's annual Zeitgeist Conference. This assembly featured prominent speakers from relevant sectors, alongside numerous governmental representatives. The event commenced with a musical tribute extolling the emancipatory potential of technology, presented by Google CEO Eric Schmidt (Bridle, 2020: 246-247). At this juncture, Schmidt (2013) articulated, "Perhaps due to the nature of our political processes, or possibly because of the operational dynamics of the media... I believe we are overlooking certain aspects. Our level of optimism is insufficient... There exist numerous favorable advancements for humanity, both within Google and on a global scale, and we ought to place our trust in the inherent trajectory of innovation and adopt a more positive outlook concerning our future"(2013). In the subsequent discussion session following this address, he paradoxically responded to a utopian inquiry derived from George Orwell's literary work, 1984, endeavoring to elucidate how technological advancements, particularly the proliferation of mobile devices, have rendered the world a more habitable place (Bridle, 2020: 247). Schmidt (2013) supported this argument by stating that it has become more difficult to commit systematic evil in the digital age. As an example, he gave the horrible events in Rwanda in 1994, even the genocide in his own words. He said that if every individual had a smartphone in 1994, people would not have been massacred with machetes. He argued that people could prevent the events with technology.

James Bridle suggests that information about the possibility of genocide was available to the former colonial powers in the area, such as the United States, France, and Belgium, weeks or even months before the genocide took place. In addition, many non-governmental organizations, ambassadors, and various officials, including representatives of the United Nations, were in the area, but they all decided to leave. Intelligence agents simply listened to radio broadcasts of threats and death announcements. For a long time, the United States denied having any intelligence at the time of the genocide. In 2012, during the trial in the United States of one of the participants in the Rwandan massacre, the prosecution presented high-resolution satellite images showing the full extent of the genocide. These images clearly showed all the details, including mass graves and bodies strewn in the streets (2020: 247-248). Bridle's point implies that the main issue under discussion goes beyond technology. This observation highlights the understanding that having a lot of data does not automatically lead to stopping violence. Furthermore, contrary to Schmidt's assertion, the large amount of data has led to a new kind of violence (Kayış, 2021: 115-116).

The aforementioned developments give rise to a plethora of interrogations. They establish the tenor for discourses surrounding ethics and AI/ML, concurrently engendering novel conflicts and simultaneously eclipsing prevailing tensions. They advocate for AI/ML ethics and proffer recommendations for their discourse and implementation. Conversely, they mitigate the contentious ethical concerns (Greene et al., 2019: 2123). To avoid such pitfalls, a more thorough examination of the ethical issues is essential.

It is evident that ethical sensitivities regarding data are applicable to both technology producers and individuals. An examination of the threat of data and algorithmic decision-making from the perspective of CEOs reveals an increased risk of a deterioration in the distribution of important liberal goods, such as rights, opportunities, and wealth (Persson & Kavathatzopoulos, 2018). As Mimi Onuoha (2018) describes, this threat is alarming not only because it can create new inequalities, but also because it has the power to conceal and magnify existing ones. In the United States, the problem has found its manifestation in rights and anti-discrimination discourses. According to experts in academia, industry, and government, if left unchecked, these tools are highly likely to produce discrimination. However, an uncritical approach to these tools risks perpetuating traditional forms of discrimination.

As computer algorithms play a bigger role in our lives, we worry more about the biases they may have and the real effects of those biases (Davis, 2021). As algorithms become increasingly pervasive in everyday life, concerns regarding their biases and impacts are mounting. Notable incidents include a black developer being misclassified by Google's photo software, Facebook suspending Native American users' accounts for using real names, and facial recognition technology struggling to identify black faces. Additionally, airport body scanners have erroneously flagged transgender individuals as threats, and Google Translate has produced biased translations of gender-neutral pronouns. While the use of the term "violence" in this context may appear exaggerated, it is important to recognize the harmful outcomes stemming from flawed data collection and algorithmic decisions. These outcomes can be considered analogous to the "data violence" described by Dean Spade (Hoffmann, 2022: 324). Consequently, "data violence" emerges as a significant phenomenon. There exists no assurance that these processes will not culminate in both indirect and overtly detrimental, or potentially lethal, repercussions (Hoffmann, 2021: 3541).

Algorithms are the main culprits for data violence.

Nick Seaver's approach to algorithms, AI, and MLs also suggests that data can be misused and turned into violence in algorithmic processes. In 2013, at a conference on algorithms, he drew attention to the main problem through a question asked by a scientist. The scientist said: "For all this talk about algorithms, I've never heard anyone talk about a real algorithm; everyone talks about a filtered ranking function. Seaver also noted that the speakers covered algorithmic topics ranging from Google's autocomplete feature to credit scoring. However, he also agrees with the questioner. Filtered ranking cannot be seen as a simple algorithmic function because additional contextual understanding is required. The filtered sorting implied by the questioner is a real algorithm. Functions like autocomplete serve different purposes (Seaver, 2017: 1-2). While this example is a bit confusing, the confusion gets to the heart of the matter.

It is imperative to acknowledge that when contemplating algorithms, it is essential to refrain from reducing them to technical jargon. The Governing Algorithms conference at New York University was a seminal event in the application of humanities and social science approaches to algorithms in the growing interdisciplinary field of critical algorithm studies (Gillespie & Seaver, 2016). A key tension within this field pertains to the extent of knowledge held by humanities and social scientists regarding the objects of this field, which until recently were the domain of computer scientists (Seaver, 2017: 2). There is a consensus in contemporary discussions about the significance of the technical aspects of discrimination, particularly in relation to algorithmic discrimination. While interpretations of its causes and effects vary, the research emphasizes the potential for algorithmic discrimination to reflect traditional forms of discrimination. Engineers and computer scientists are regarded as having the capacity to promote justice through the implementation of discrimination-sensitive data practices. Conversely, data justice experts concentrate on human-centered governance, acknowledging technology's transformative capacity as a tool for justice. Technology is central to the agendas of both fields (Kleinberg et al., 2018).

The domain of justice, accountability, and transparency studies is concerned with ethical dilemmas associated with automated systems, and it places emphasis on engineering and technical solutions to mitigate risks to vulnerable groups (Novelli et al., 2024: 1872). The examination of equity, responsibility, and openness was initially aligned with the preliminary investigation into the essence of bias in the architecture of computational systems and the safeguarding of privacy in data mining endeavors. (Zhang & Zhao, 2007: 53). Computer science has seen a discourse on the potential for data mining and machine learning algorithms, which underpin automated systems, to exhibit discriminatory tendencies towards individuals (Pessach & Shmueli, 2023: 870). To circumvent the creation of systems that give rise to bias, unfair treatment, and illegal discrimination, researchers in the fields of computer science and engineering have conceptualized and modeled methodologies for the identification and avoidance of such risks in automated decision systems (Dechesne, 2020: 18). Consequently, contemporary researchers have identified numerous criteria for determining the fairness of machine learning systems. However, these advances have semantically shifted from the detection and prevention of harm, bias, or discrimination. Nevertheless, such advances still hold algorithmic decision-making and automated systems to standards of fairness, accountability, and transparency (Birhane et al., 2023).

Moreover, studies of justice, accountability, and transparency fail to fully account for anti-discrimination. In addition, existing literature tends to neglect important debates in the field of political philosophy about the extent to which all instances of inequality are objectionable (Lippert-Rasmussen, 2015: 210). Consequently, the field is left with technical solutions that are overly simplistic and ill-equipped to adapt to the intricacies of social life. Indeed, endeavours focused on justice, accountability, and transparency frequently overestimate the transformative capacity of technology and overlook the barriers to justice in automated computer systems or parametric decision rules, especially when attempting to achieve intended design or engineering objectives. In contrast to scholars who focus on justice, accountability, and transparency, an emerging group of researchers who focus on data justice offer a broader perspective to address the problem of algorithmic discrimination (Rosenbaum & Fichman, 2019: 238-239). These studies elucidate the purpose of equitable data collection, data analytics, and automated data-driven decision-making. That is, while justice, accountability, and transparency studies focus on identifying justice constraints, data justice studies consider the purpose of equity. In essence, while justice, accountability, and transparency emphasise the technical, data justice emphasises the sociotechnical. With its focus on data-driven harms and opportunities, data justice operates on a contentious border between technological and social determinism (Taylor, 2017). Nevertheless, it is of paramount importance to recognize that this issue carries with it a level of social significance that is far too substantial to be limited or restricted by any sort of predefined or established boundaries that may exist.

What does data violence cost?

Data violence is now ubiquitous, pervading all aspects of data and automated systems that accompany our lives. Our tracking and shopping habits, our health and fitness tracking, our financial information – all of it is produced about us by third parties, and data-driven systems are at the ready (Hoffmann, 2018). The shift towards automation in contemporary monitoring and surveillance strategies is therefore unsurprising. The imminent dominance of driverless vehicles on roads, and the subsequent potential obsolescence of practices such as speeding and red light violations, are indicative of this trend. While these developments are undoubtedly beneficial, they concomitantly entail a consolidation of centralized forms of information gathering and control. It is acknowledged that this progression is a continuous process, and that, in part due to the emergence of "smart" technologies, there is an imminent shift towards a scenario in which corporate and government agencies will possess exhaustive profiles of every element of our professional, personal, and social lives. The future is not merely a concept relevant to our telephones, our vehicles, our places of work, and our urban environments; it is a reality. The technological capabilities of digital media facilitate comprehensive data collection, and the enhanced control that this enables makes it a desirable outcome. Consequently, data today possesses the potential to eradicate uncertainty and lack of control (Andrejevic, 2019: 9).

The severity of unintended consequences associated with the use of technology can be high. For example, there are striking parallels between plutonium, a material with limited non-military applications, and artificial intelligence and facial recognition systems. Plutonium is a by-product of nuclear energy and a major component of nuclear waste. In very small quantities it is used as a power source for specialized scientific instruments such as space probes. Plutonium has a limited number of highly specialized and strictly regulated applications. If allowed to proliferate, it could have harmful effects in the hands of various organizations. As a result, plutonium can be seen as a material metaphor for digital facial recognition technologies. It is harmful to public health and will therefore be subject to strict restrictions. Its use would have extremely harmful consequences for public health, outweighing potential benefits (Stark, 2019: 1-5). This assertion is further supported by Hartzog and Selinger (2018), who states that "the future of human development depends on banning facial recognition technologies before they become too ingrained in our lives". "Otherwise, people will not know what it is like to be in a society without being automatically identified, profiled, and potentially exploited" (Hartzog & Selinger, 2018: 1-5). To avoid social toxicity and racial discrimination, it is crucial to understand facial recognition technologies for what they are. In other words, they should be seen as a threat that needs to be handled with extreme caution (Bacchini & Lorusso, 2019: 321-322).

Digital technologies should therefore be approached as legitimate objects of ethical concern, with human values embedded in them. This argument may seem obvious to researchers who recognize the importance of human value in technological production, but this is not the case. Technological neutrality is just a discourse in Silicon Valley and elsewhere (Russo, 2018: 656). There is currently no consensus on the moral responsibility of computer engineers and data scientists for their inventions. Consequently, an emerging movement known as 'ethical design' has emerged with the aim of either establishing such a consensus or at the very least, formalizing the terms of debate, in the fields of AI and machine learning (Stahl & Wright, 2018: 27-29).

Is a new ethical approach necessary?

The dichotomy of technical and ethical perspectives on the issue does not allow for a clear position on the data. However, as mentioned above, there are some developments and ethical steps that can be taken. For example, egalitarianism is the idea that people should be treated equally and (sometimes) certain things of value should be distributed equally. Egalitarianism makes discrimination wrong. Surprisingly, this connection has been resisted by many of the previously mentioned theorists of discrimination, as can be seen from the gap between the technical and ethical views. Some have even argued that the link between anti-discrimination laws and equality is negligible (Holmes, 2005: 175). Others argue the opposite. There are those who believe that only a direct appeal to egalitarian norms can satisfactorily explain everything that is wrong with discrimination (Segall, 2012: 82). For present purposes, this debate can be safely avoided. This is not because the debate is uninteresting or unimportant, as a philosophical project. Rather, the aim here is to examine how egalitarian norms might develop an account of why, and when algorithmic systems might be considered unjust (Binns, 2018: 5-6). Therefore, common sense is needed to develop new concepts for data injustice and data violence based on inequality. The new data ethics also need an umbrella definition of such discussions.

In this context, it becomes important to understand the power of algorithms and to make sense of the epistemologies on which they are based. The absence of such knowledge allows the perpetuation of algorithm-driven and big data-driven violence. It is, therefore, better to seek critical analyses of algorithmic processes, the social world they inhabit, and the alternative futures they can bring us, rather than focusing solely on the algorithm itself. Therefore, technologists and academics have a significant role in tackling the epistemological ignorance embedded in algorithms, i.e., the "ethical significance of algorithmic mediation". They also have a significant role in how algorithmic processes can promote justice and humanitarian considerations (Mittelstadt et al., 2016: 12). It needs to be recognized that algorithmic processes, including those in financial and urban planning sectors, can perpetuate systemic biases. However, the way data is generated is also called into question. Questions about the politics of data creation and the definition of valid data are sparking new concerns and debates. The issues at stake in these debates include data production, management, ownership, transparency, and access. Digital divides the consequences of 'smart' technologies, and the ethics and politics of public sector collaboration with private data owners and managers can also be investigated. The accountability, transparency, bias, and justice of algorithmic design, and the extreme racial bias of the technologies themselves, also require an ethical approach. These debates are not only about technological design but more importantly about addressing how data-driven assessments and predictive modeling have the power to bring futures into being (Introna, 2016: 25; Leszczynski, 2016: 1695; Shelton, 2017: 3).

In sum, by drawing attention to these limits, we are not suggesting that they are absolute or impossible to overcome. In fact, in asserting and examining the intertwined insidiousness of data and discrimination, it is necessary to point to productive points that can overcome them, not to offer fatal diagnoses. However, the problems resist any easy solutions. Nor can we simply discuss a fix that can be applied at the coding level. We need to focus our iterative critical attention on them, looking for these problems not only in system failures, but also in the kinds of worlds constructed through the design, development, and implementation of data-intensive, algorithmically mediated systems (Hoffmann, 2019: 910).

In short, given that data violence is born, there are symbolic ethical concerns at the institutional level, but this is not likely to be overcome. It has always been difficult to speak and understand the language used by engineers. Therefore, it is imperative to adopt a critical social theory approach in the new data ethics. In this way, a protective shield can be created for the individual against algorithmic processes.

Aim and methodology

This study will examine data on violence experienced by ordinary people in social media environments. The challenges faced by ordinary people in networked environments have diversified with the widespread use of social media applications. The fact that ordinary people can encounter people, groups, and masses that they would not be able to meet in daily life without networked environments has led to different types of data violence. Data violence in networked environments can cause serious harm to users. The psychological, financial, and social effects of data violence can extend beyond the online realm, impacting real-life circumstances and manifesting in physical forms of violence. Anna Lauren Hoffmann's research on data violence, as it relates to data-intensive systems and platforms, examines the concept of data violence in the international literature. The concept of data violence is also examined in the context of intersectionality in the works of Hoffmann et al., specifically *in Imagining Intersectional Futures: Feminist Approaches in CSCW (2017)* and *Data, Technology, And Gender: Thinking About (And From) Trans Lives (2017).* To date, there have been no scientific studies in Türkiye that directly address the concept of data violence. However, the findings of studies such as the Social Information and Communication

Association's (Toplumsal Bilgi ve İletişim Derneği -TBİD) Digital Violence Research in Türkiye (Türkiye'de Dijital Şiddet Araştırması -2021) are relevant to the concept of data violence.

It is imperative to ascertain the specific dimensions and causes of data violence that social media users in Türkiye may encounter. The form of violence in networked environments is analogous to violence in real life; therefore, solutions to such problems can be developed. The objective of this study is to comprehend the problem from the perspective of platforms and users by elucidating the data violence that users encounter as a result of their use of social media and the factors that cause this data violence. The research study was designed to address the following four research questions:

RQ1: Can violence in everyday life be transferred to the networked environment?

RQ2: Do social media applications cause data violence?

RQ3: What types of data violence do ordinary people experience in networked environments and who is responsible?

RQ4: What is the cost of data violence in networked environments?

The issue will be approached from an ethical perspective, recognizing that the new types of data emerging from networked technologies and the problems arising from their processing are the main concerns of data violence. A theoretical framework will be used to examine the data of social media users in order to explore new ethical issues between the producers and users of technology. In order to trace the problems related to data violence faced by social media users, a selected online complaint platform partially resolves and adjudicates complaints against brands and companies in Türkiye. The reason for selecting the designated complaint platform is its independence from social media applications. Users try to resolve problems with social media applications through the designated units of these applications. However, if they do not find a solution to the problems, they lose confidence in the application and the processes and turn to alternative methods. Therefore, the fact that the designated platform is independent and the most prominent complaints platform in the country was a decisive factor in the selection of the sample. On this platform, there are many complaints created by users of YouTube, TikTok, X (Twitter), Facebook, and Instagram. Of these complaints, 25 from Facebook, 36 from Instagram, 35 from TikTok, 6 from X, and 28 from YouTube were included in the research sample to be analyzed. The complaints included in the sample are cases of data violence experienced by users. Users attempt to resolve data violence victimization on social media applications primarily through the in-app complaint system. The fact that users who cannot find an in-app solution to their complaints turn to a neutral complaint platform shows trust in the platform. The sample is limited to this complaint platform because the complaints reveal real victimization.

The research used the technique of document analysis to collect complaints about data violence. Document analysis is the detailed study of documents produced in a wide range of social practices, including written and visual images. Such research is important for uncovering the meanings associated with the historical conditions of documents (Wharton, 2006: 79). Following the compilation of all complaints submitted from the first complaint to 30 November 2024, qualitative content analysis was applied to the data obtained. Qualitative content analysis aims to find concepts and relationships that can explain the data collected. In this process, different themes and concepts can be discovered. In addition, efforts are also made to reveal the facts hidden in the data (Yıldırım & Şimşek, 2018: 242). Qualitative content analysis was conducted within the framework of eight themes. These are biased in representation, harassment and cyberbullying, misinformation and manipulation, privacy violation and data security, discrimination, digital labor exploitation, polarization, and data exploitation.

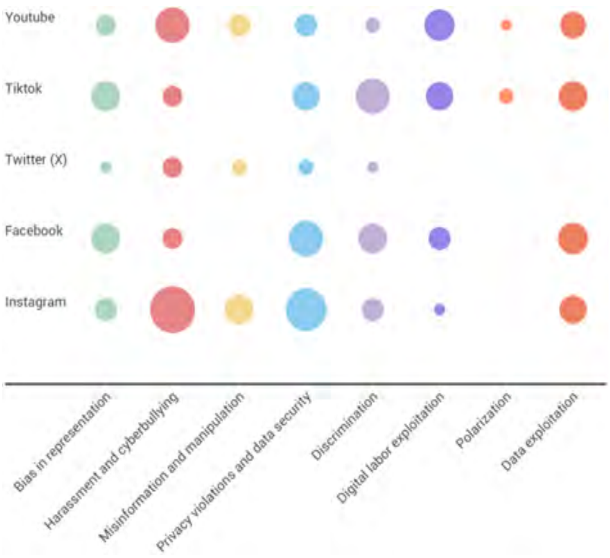
The identification of these themes was informed by a preliminary analysis of the most recurrent forms of data violence reported on the complaints platform. The principles of research ethics were taken into account when analyzing and presenting the findings within each of the themes. Since the complaints in question contain data about an individual and an institution, the posts in question were categorized and evaluated, and the name of the platform on which the complaint was made was masked. In this way, ordinary people were not harmed by the unauthorized use of their data, which they did not wish to share as an example for scientific research.

Findings

This research, conducted to uncover the data violence that occurs as a result of communication in networked environments, has identified several forms of new data violence. The findings, which provide a detailed perspective on the position of platforms in the new data ethics, show that data violence can occur under multiple headings.

Figure 1

Social media applications and types of data violence

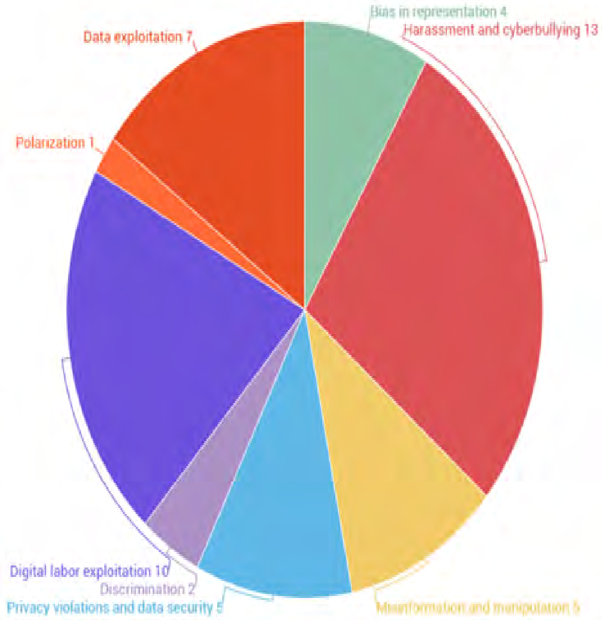


The results in Figure 1 show the distribution of ordinary social media users' complaints by category. Here, the social media applications in question generally cause data violence in categories such as bias in representation, harassment and cyberbullying, privacy and data security violations, discrimination, and data exploitation. Complaints about polarisation, misinformation and manipulation, digital labor exploitation, and data exploitation were found to be less common than other categories in the sample. Each category seems to differ depending on the social media application. This shows that the applications may contain unique forms of violence. Therefore, evaluating each social media application separately in terms of the data violence it generates may explain this situation. Common issues can then be identified through a general overview.

First, the results of YouTube, an online video-sharing and social media application, are presented.

Figure 2

Data Severity Findings for YouTube

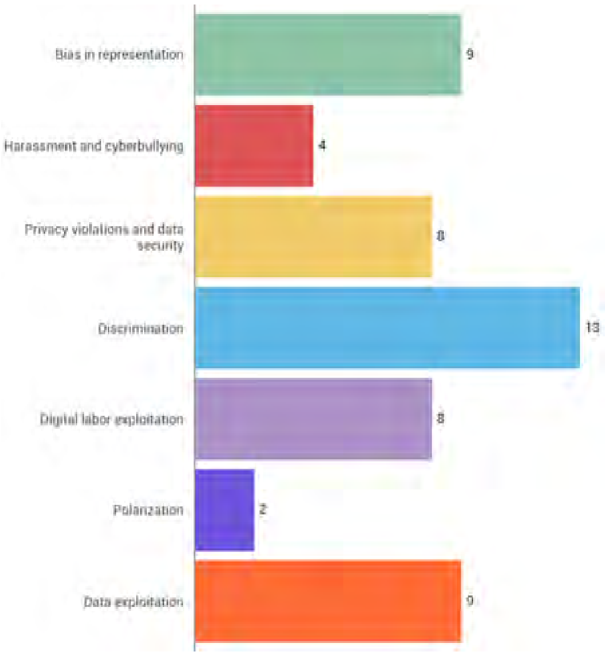


The most common forms of data violence on YouTube are harassment and cyberbullying. These are examples of harassment and cyberbullying where users' personal information is at the center, and where users are often the perpetrators. Examples include mutual bad-mouthing in video comments or the constant harassment of a user by people posing as investors they met through their YouTube channel. Victimization in the form of unjustified channel suspensions, problems with distribution revenues, and loss of monetization opportunities can be read as digital labor exploitation through the harm caused by YouTube to users. This type of data violence is the second most common example found on YouTube. Similarly, data exploitation includes examples where users who do not use YouTube for financial gain are subjected to financial harm (usually unauthorized withdrawal of money from their account by YouTube), and examples such as engagement with content that is not typically followed by the purchase of subscriptions are assessed under the category of data exploitation. The fact that similar examples make up the third most common category can be interpreted as YouTube managing personal data in a way that causes data violence against ordinary users. There are also complaints about privacy and security issues on YouTube. It is common for inappropriate and disturbing content to be shared from accounts created using users' photos and numbers. The existence of complaints about misinformation and manipulation also shows that YouTube content can cause data violence by manipulating and misinforming users. For example, complaints allege that users have suffered material and moral harm as a result of misinformation and manipulative content. In addition, complaints have been received where YouTube has been accused of bias in representation and discrimination. Users who felt that YouTube was biased in its presentation also criticized it for discrimination. For example, the user interpreted the fact that the channel in question dropped down the list of recommended channels when content glorifying an ethnic group started to be shared as representation bias and discrimination. In another study, YouTube was accused of being polarising by highlighting videos from one group and not recommending videos from other groups. The involvement of children in data violence in all of these findings shows that data violence is a threat to vulnerable groups.

In the case of TikTok, another social media application, complaints have generally centered on the idea that there are discriminatory elements in the way the application operates. Complaints include allegations that TikTok's management takes sides in value attacks. The allegations of discriminatory data violence shown in Figure 3 are common on TikTok. Similarly, users complain that TikTok is biased in its representation. Users accused TikTok of bias in content moderation, even though posts containing slang and profanity were not removed, while their posts that did not violate any community rules were removed. The number of complaints about TikTok's use of data is also high. As with YouTube, there are complaints about TikTok that can be interpreted as data exploitation, such as irregular deductions from users' bank accounts and the disappearance of TikTok gift money. Similar complaints have also been made by those who earn commercial income from TikTok. These practices, which can be interpreted as digital labor exploitation, include allegations that the videos of accounts with a very high number of followers are unfairly blocked and that the number of views has decreased because they do not pay a fee to TikTok.

There are also complaints from users that privacy and data security issues constitute data violence. Complaints often include victimization caused by users' photos being taken without permission by other users, diverted from their original purpose, and shared inappropriately. These photos include images of users' spouses and children. In addition, some users respond with profanity to those who

Figure 3. Data severity findings for Tiktok



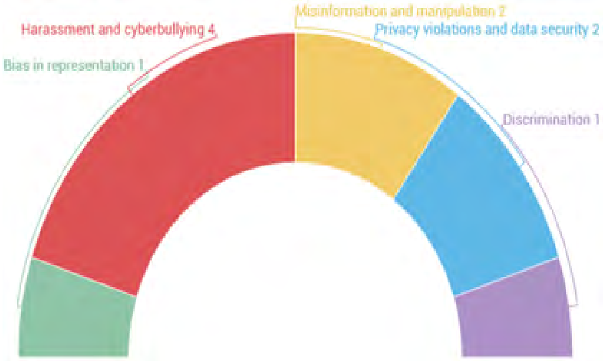
warn others about violating community rules in their posts. They engage in harassment and cyberbullying. These complaints are examples of harassment and cyberbullying leading to data violence. Users claiming that polarisation leads to data violence also stated that TikTok encourages polarisation by positively discriminating against posts that engage in polarising discourse between different segments of society.

There are fewer examples of actions that may constitute data violence coming from application X than from other social media applications. When the posts related to data violence on the relevant complaint platform were scanned, problems related to harassment and cyberbullying were identified. An example of harassment and cyberbullying complaints in Figure 4 is when a video of an ordinary user is taken and shared on another account, and insults and abuse are made under this post. In this case, the video was shared to be abused and insulted by others. Although the user has asked for help from the X authorities to deal with the abuse, he has not received any results.

There have also been complaints about privacy and data security issues. For example, users were identified on the X application who claimed that they had been subjected to data violence due to the publication of sexually explicit videos of ordinary people. The X application also identified complaints from other users whose user information was used in a misinformative and manipulative manner. In addition, the closure of the first account complained about as a result of two users arguing that X was seen by the user as biased and discrimination in representation.

Figure 4

Data severity findings for X

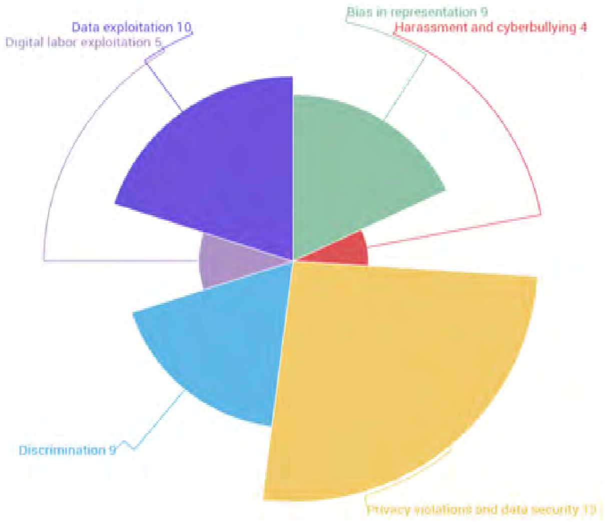


Looking at Facebook's results in Figure 5, it is clear that privacy violations and data security complaints are the primary forms of data violence. There are examples of data violence in different contexts due to Facebook's failure to ensure the privacy and security of users' data. For example, a cascading effect occurred when a user's username and password, which should have been kept confidential and secure, were stolen. The person, who also used his stolen account for commercial activities, received no support from Facebook and was exposed to data violence through data breaches.

Another category of data violence commonly seen on Facebook is data exploitation. Similar to incidents in other social media applications, users' financial information has been exploited and money has been taken from their accounts without their knowledge. It is also noteworthy that there are many cases where practices involving bias and discrimination in representation constitute data violence. Users generally complained about the removal of comments due to Facebook's community rules, the removal of only one side's post in the case of insults and swearing, punishment, discrimination against a particular group, and bias. In addition, individuals and businesses that use Facebook for commercial

Figure 5

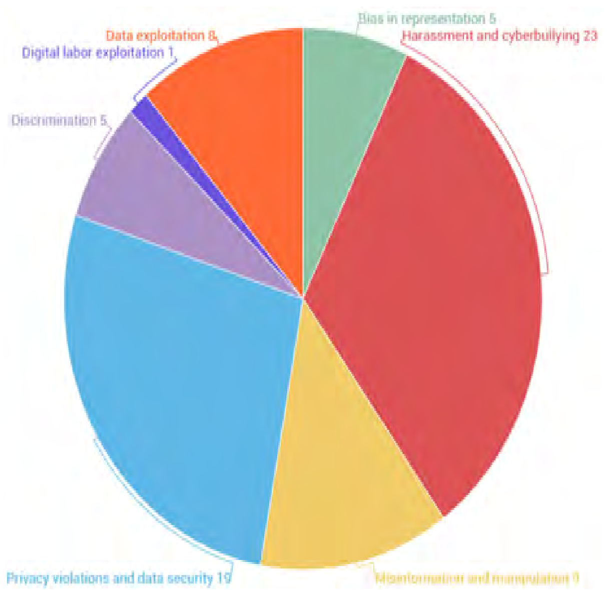
Data Severity Findings for Facebook



purposes suffer losses due to problems arising from the application, which can be considered in the category of digital labor exploitation. For example, a company that wanted to advertise on Facebook was unable to place the ad because it did not receive the code from Facebook. Therefore, the user claimed to have suffered a commercial loss. The existence of individuals who have been harassed and cyberbullied shows that Facebook can also cause data violence in this context. One woman who once posted her phone number was constantly harassed and was unable to remove it, making the data violence permanent.

Figure 6

Data Severity Findings for Instagram



Harassment and cyberbullying, which can be interpreted as data violence, rank lowest in complaints about Facebook, but highest for Instagram, as shown in Figure 6.

Examples include defamation by secret users who put people in difficult situations, the creation of user accounts with images of ordinary users, and the sharing of inappropriate content. Privacy and data security issues also often lead to data violence on Instagram. For example, when one user saw a video shared by an unknown person, another user was disturbed by the situation, complained, and asked for a solution. Many similar complaints, where users feel that their privacy and security have been violated, can be assessed in the context of data violence. One category on Instagram that constitutes data violence, and is not common on other social media applications, is misinformation and manipulation. The complaints indicate that it is common to tag and share other users in any video or photo on Instagram and that these posts are not liked by other users. The complaints also show that this practice, which constitutes data violence, victimizes users. It is also possible to encounter new forms of data exploitation on Instagram. One user stated that he had received coupons from an Instagram account that sold ready-made virtual betting coupons, but they did not work. On the contrary, the victimized user was constantly asked for money; the user was exposed to material and moral losses due to the demands for payment. Although the user asked Instagram for help, people in similar cases have been harmed by the exploitation of their data. Bias and discrimination in representation, common in other social media applications, were also identified against Instagram. Users argued that Instagram practiced ethnic discrimination and representation bias based on the way comments were deleted. These examples are prevalent in the removal of posts that do not comply with community rules. One user reported that his gaming account, in which he had worked and earned commercial income for many years, was stolen and his content deleted. In this way, Instagram failed to protect the security of a user's account, resulting in digital labor exploitation.

Discussion and conclusion

The phenomenon of violence continues to exist in networked environments that resemble the real world. As Nick Seaver (2017: 1) states, artificial intelligence shows that data can be misused in algorithmic processes, which can lead to violence. It is clear that individuals in Türkiye are using social media applications in ways that can affect their daily lives. The violence that results from these uses has similarities to the examples that inspired the concept of data violence. Similar to the suspension of Native Americans' Facebook accounts for using their real names, examples of discrimination and bias in representation have been observed in the use of networked technologies in Türkiye. Therefore, the exposure of social media users in Türkiye to data violence cannot be considered independent of the technical accidents, data collection processes, and algorithmic stages of these technologies. As such, users in Türkiye are exposed to data violence in a manner similar to physical violence in the real world (Hoffmann, 2022: 324).

While data violence occurs in networked environments, this research shows that the act of data violence occurs in different categories depending on the social media application. The YouTube, TikTok, X, Facebook, and Instagram applications examined in the research are known to have different user audiences and purposes. Different audiences and purposes also lead to different types of data violence experienced. Those who use YouTube for commercial purposes often report being subjected to digital labor exploitation, which is linked to financial losses due to the medium's algorithms. TikTok, on the other hand, often inflicts data violence by exposing users to discriminatory practices. This has sometimes occurred when a user has been discriminated against by another user, or when discrimination has been practiced directly by TikTok. The prevalence of harassment and cyberbullying on social media applications such as X and Instagram, which are widely used in Türkiye, shows that the elements of violence that individuals may encounter in their normal lives are also transferred to the online environment. Companies have not taken any initiative to address the data violence that users have suffered as a result of defamation based on an image or idea they have shared; or as a result of defamation by people they do not even know for fraudulent purposes. As a result, users stated that they had tried all possible ways to resolve their victimization and had resorted to the complaints platform as a last resort. On Facebook, it was observed that complaints about privacy and data security violations, which constitute data violence against users, were frequent. Illegal access to users' accounts, photos, and videos caused data violence against users.

A striking aspect of the complaints and grievances raised by users is that, despite their unconditional trust in the platforms, they are being subjected to data violence. Users still expect the platforms to provide redress. Nevertheless, users have experienced every category of data violence in every social media environment. Therefore, it makes sense to categorize platforms as the main actors in data exploitation. The only question to ask of platforms that cannot prevent and manage defamation of ordinary users and common acts such as fraud is what benefit they derive from all this. Therefore, all categories of data violence found indicate that platforms are engaged in data exploitation. Platforms generate value only from exploiting users' data, leaving other complaints unresolved due to administrative patterns such as community rules.

Once the confidentiality and security of personal data are breached, the other categories are likely to occur. There is an open-ended series of scenarios regarding the potential harm that data can cause to individuals. Users who are aware of all this can only contact the platform itself.

After that, the application is inconclusive and the user exposed to data violence desperately applies to the complaint platform. However, from the way the platform works, it can be said that all these complaints are inconclusive. When a problem is solved on the complaints platform, it is marked as "solved". As a result, the reputational damage and the financial and material losses suffered by users become data violence. The platforms' automated complaint and feedback mechanisms, which include algorithms, do not help to overcome this. The findings therefore point to the need for platforms, as perpetrators of data violence, to take action. Platforms have the most important role in overcoming data violence by identifying and addressing it. There is a need for mechanisms that clearly define and prevent data violence. Furthermore, the categories of data violence in the examples analyzed do not overlap with freedom of expression. These acts of data violence directly target individuals.

Therefore, new data ethics can be advocated by examining what causes data violence in social media environments, which are products of technological design, and how it can be overcome. When ethics are not embedded in technological design, as in the social media environments examined in this study, examples of data violence will emerge. Therefore, as Daniel Greene et al. (2019: 2123) state, computer engineers, data scientists, or those responsible for these processes should act in accordance with the principles of 'ethical design'. Otherwise, technologies designed in a discriminatory and inequitable way will create new and more severe examples of data violence. Elisa Holmes (2005: 175) also states that the dichotomy between technical and ethical perspectives does not contribute to solving problems; designers caught between technique and ethics prioritize technique over ethics as the main source of the problem. It is imperative to combine technique and ethics in order to design technological products that are not inequitable, do not cause discrimination, and do not cause data violence. Otherwise, as seen in this research, proposed solutions to the problems identified by users will be met with resistance. Instead, it will remain an accepted and widespread practice for the technology used to constantly involve data violence. The countries where such technologies are used also have an obligation here. In a situation where the technologies used cause data violence to people, states can protect users through legal processes. With appropriate laws and sanctions, technology companies can be forced to take steps in this direction and users can be protected. In this way, it can contribute to understanding the new dimensions of social media platforms in relation to data violence identified in this study and support a better understanding of the responsibilities of platforms.

References

Amrute, S. (2019). Of techno-ethics and techno-affects. *Feminist Review*, 123(1), 56–73. https://doi.org/10.1177/0141778919879744

Andrejevic, M. (2019). Automating surveillance. *Surveillance and society*, 17(1–2), 7–13. https://doi.org/10.24908/ss.v17i1/2.12930

Bacchini, F., & Lorusso, L. (2019). Race, again: how face recognition technology reinforces racial discrimination. *Journal of information, communication and ethics in society*, 17(3), 321-335.

Binns, R. (2018). *Fairness in machine learning: lessons from political philosophy.* 2016, 1–11. http://arxiv.org/abs/1712.03586

Birhane, A., Kasirzadeh, A., Leslie, D., & Wachter, S. (2023). Science in the age of large language models. *Nature reviews physics,* 5(5), 277-280.

Bridle, J. (2020). *Yeni karanlık çağ teknoloji ve geleceğin sonu.* (K. Güleç, Translation) İstanbul: Metis.

Dechesne, F. (2020). Fair enough? on (avoiding) bias in data, algorithms and decisions. Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14, 17-26.

Floridi, L. (2024). *Dördüncü devrim: bilgiküre insan hakikatini nasıl yeniden şekillendiriyor?* (O. Önder, Translation) İstanbul: Albaraka yayınları

Fox, S., Menking, A., Steinhardt, S., Hoffmann, A. L., & Bardzell, S. (2017, February). Imagining intersectional futures: Feminist approaches in CSCW. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 387-393).

Gangadharan, S. P. (2017). The downside of digital inclusion: expectations and experiences of privacy and surveillance among marginal Internet users. *New media and society*, 19(4), 597–615. https://doi.org/10.1177/1461444815614053

Gillespie, T., & Seaver, N. (2016, December 15). *Critical algorithm studies: a reading list*. Retrieved on October 21, 2024, from social media collective: https://socialmediacollective.org/reading-lists/critical-algorithm-studies/

Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, nicer, clearer, fairer: a critical assessment of the movement for ethical artificial intelligence and machine learning. *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 2122–2131. https://doi.org/10.24251/hicss.2019.258

Hartzog, W., & Selinger, E. (2018, August 2). *Facial recognition is the perfect tool for oppression*. Retrieved on October 22, 2024, from Medium: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

Hoffmann, A. L. (2017). Data, technology, and gender: Thinking about (and from) trans lives. In *Spaces for the Future* (pp. 3-13). Routledge.

Hoffmann, A. L. (2018, April 30). *Data violence and how bad engineering choices can damage society*. Retrieved on October 20, 2024, from Medium: https://medium.com/s/story/data-violence-and-how-bad-engineering-choices-can-damage-society-39e44150e1d4

Hoffmann, A. L. (2019). Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse. *Information Communication and Society*, 22(7), 900–915. https://doi.org/10.1080/1369118X.2019.1573912

Hoffmann, A. L. (2021). Terms of inclusion: data, discourse, violence. *New media & society*, 23(12), 3539-3556.

Hoffmann, A. L. (2022). Excerpt from where fairness fails: data, algorithms, and the limits of antidiscrimination discourse. In *Ethics of data and analytics* (pp. 319-328). Auerbach publications.

Holmes, E. (2005). Anti-discrimination rights without equality. *The modern law review limited*, 68(2), 175–194. https://doi.org/10.2307/824017

Introna, L. D. (2016). Algorithms, governance, and governmentality: on governing academic writing. *Science technology and human values*, 41(1), 17–49. https://doi.org/10.1177/0162243915587360

Kayış, H. H. (2021). Dijital eşitsizlikleri yakindan incelemek: dijital uçurum buzdağinin görünen yüzü müdür? *Ege üniversitesi iletişim fakültesi yeni düşünceler hakemli e-dergisi*, (15), 109-124.

Kleinberg, J., Ludwig, J., Mullainathan, S., & Sunstein, C. R. (2018). Discrimination in the age of algorithms. *Journal of legal analysis,* 10, 113-174.

Leavy, S. (2018). Gender bias in artificial intelligence: the need for diversity and gender theory in machine learning. In Proceedings of the 1st International Workshop on Gender Equality in Software Engineering (pp. 14-16). https://doi.org/10.1145/3195570.3195580

Leszczynski, A. (2016). Speculative futures: cities, data, and governance beyond smart urbanism. *Environment and planning* A, 48(9), 1691–1708. https://doi.org/10.1177/0308518X16651445

Lippert-Rasmussen, K. (2015). Discrimination: an intriguing but underexplored issue in ethics and political philosophy. *Moral philosophy and politics*, 2(2), 207-217.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: mapping the debate. *Big data and society*, 3(2), 1–21. https://doi.org/10.1177/2053951716679679

Nissenbaum, H. (2010). Privacy in context: technology, policy, and social life. In Jurimetrics (C. 51). http://search.proquest.com.strauss.

uc3m.es:8080/docview/913137931

Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: what it is and how it works. Ai & Society, 39(4), 1871-1882.

Onuoha, M. (2018, March 22). *GitHub*. Retrieved on October 20, 2024 from https://github.com/MimiOnuoha/On-Algorithmic-Violence

Persson, A., & Kavathatzopoulos, I. (2018). How to make decisions with algorithms: ethical decision-making using algorithms within predictive analytics. *ACM SIGCAS computers and society*, 47(4), 122-133.

Pessach, D., & Shmueli, E. (2023). Algorithmic fairness. In *Machine learning for data science handbook: data mining and knowledge discovery handbook* (pp. 867-886). Cham: Springer International Publishing.

Rosenbaum, H., & Fichman, P. (2019). Algorithmic accountability and digital justice: A critical assessment of technical and sociotechnical approaches. Proceedings of the association for information science and technology, 56(1), 237-244.

Russo, F. (2018). Digital technologies, ethical questions, and the need of an informational framework. Philosophy & Technology, 31(4), 655-667.

Schmidt, E. (2013, May 20). How should we think about the future? *You Tube Video.*

Seaver, N. (2017). Algorithms as culture: Some tactics for the ethnography of algorithmic systems. *Big data and society*, 4(2), 1–12. https://doi.org/10.1177/2053951717738104

Segall, S. (2012). What's so bad about discrimination? *Utilitas,* 24(1), 82–100. https://doi.org/10.1017/S0953820811000379

Shelton, T. (2017). The urban geographical imagination in the age of *Big Data. Big data and society*, 4(1), 1–14. https://doi.org/10.1177/2053951716665129

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: implementing responsible research and innovation. IEEE Security & Privacy, 16(3), 26-33.

Stark, L. (2019). Facial recognition is the plutonium of ai. *XRDS: Crossroads, The ACM magazine for student*s, 50-55.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big data and society*, 4(2), 1–14. https://doi.org/10.1177/2053951717736335

Toplumsal Bilgi ve İletişim Derneği (2021). Türkiye'de dijital şiddet araştırması. Retrieved on February 22, 2025, from https://turkiye.unfpa.org/sites/default/files/pub-pdf/digital_violence_report.pdf

Wharton, C. (2006). Document analysis. In Victor Jupp, *The Sage dictionary of social research methods* (pp. 79-81). London: Sage.

Yıldırım, A. & Şimşek, H. (2018). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin.

Zhang, N., & Zhao, W. (2007). Privacy-preserving data mining systems. Computer, 40(4), 52-58.

Genişletilmiş Özet

Ağ bağlantılı ortamlarda paylaşılan veriler sıradan insanların veri şiddetine uğramasına neden olmaktadır. Esasen bu eylem gündelik hayatın ağ bağlantılı ortamlara taşınmış bir biçimidir. Gündelik hayatta yer alan şiddetin veriler aracılığıyla ağ bağlantılı ortamlara taşınmasıyla bu eylemlerle sıkça karşılaşılmaktadır. Bu eylemin mağdur tarafında olanlar genellikle sıradan insanlardır. Mağdur edenler ise eylemi gerçekleştirenler ve bu eylemin gerçekleştirildiği platformların kendisidir. Mağduriyetin ortaya çıkmaması adına platformların üzerine düşen görevler vardır. Platformlar kullanıcıların gerçek hayattaki gibi şiddete uğramaması için verileri iyi yönetmeli, gizliliği korumalı ve farklı çıkar çatışmalarını önlemelidir. Tüm bunlar kullanıcıların ağ bağlantılı ortamda farklı türden veri şiddeti kategorilerine uğramaması için gereklidir. Bu görevler yerine getirilmediğinde veri şiddeti ortaya çıkar.

Bu araştırmada sosyal medya ortamlarında sıradan insanların uğradıkları veri şiddeti incelenecektir. Ağ bağlantılı ortamlarda karşılaşılan veri şiddetinin kullanıcılara ciddi zararları söz konusu olabilir. Çeşitli psikolojik, finansal ve sosyal etkiler ağ bağlantılı ortamların dışına taşıp gerçek hayatı etkileyerek şiddet olgusunu somutlaştırabilir. Türkiye'deki sosyal medya kullanıcılarının somut olarak karşılaşabileceği veri şiddetinin boyutlarını ve nedenlerini ortaya koymak önemlidir. Çünkü şiddetin ağ bağlantılı ortamlardaki biçiminin gerçek anlamdaki şiddetten herhangi bir farkı yoktur. Bu tür sorunların çözümüne yönelik yol haritalarının bu şekilde çizilebileceği söylenebilir. Bu doğrultuda bu araştırmada kullanıcıların sosyal medya kullanımları sonucu karşılaştıkları veri şiddeti ve bu veri şiddetine neden olan unsurlar ortaya koyularak, soruna platformlar ve kullanıcılar açısından bir bakış açısı kazandırmak amaçlanmıştır.

Ağ bağlantılı teknolojilerin ortaya çıkardığı yeni veri türleri ve bunların işlenmesinden kaynaklı sorunların veri şiddetinde temel uğrak noktaları olduğu kabul edilerek konuya etik bir perspektiften yaklaşılmıştır. Sosyal medya kullanıcılarının karşılaştıkları veri şiddetiyle ilgili sorunların izini sürebilmek için Türkiye'de marka ve firmalar hakkında şikayetlerin kısmen çözüm ve karara bağlandığı bir çevrimiçi şikâyet platformu seçilmiştir. Bu platformda Youtube, Tiktok, X (Twitter) Facebook ve Instagram uygulamalarını kullananların oluşturduğu birçok şikâyet yer almaktadır. Bu şikayetler arasında yer alan ve kullanıcıların veri şiddetine maruz kaldığını belirten Facebook'tan 25, Instagram'dan 36, Tiktok'tan 35, X (Twitter)'ten 6 ve Youtube'dan 28 şikâyet incelenmek üzere araştırma örneklemine dahil edilmiştir. Örnekleme dahil edilen şikayetler kullanıcıların tecrübe ettiği veri şiddeti vakalarıdır. Kullanıcılar sosyal medya uygulamaları kaynaklı uğradıkları veri şiddetiyle ilgili mağduriyetleri öncelikle uygulama içi şikâyet sistemi ile gidermeye çalıştığı bilinmektedir. Şikayetlerine uygulama içi çözüm bulamayan kullanıcıların görece tarafsız bir şikâyet platformuna yönelmeleri ilgili platforma güveni göstermektedir. Bu yüzden örneklemin bu şikâyet platformu ile sınırlandırılması ele alınan örnek şikayetlerin gerçek mağduriyetleri ortaya koyması nedeniyledir.

Bireylerin Türkiye'de sosyal medya uygulamalarında gündelik hayatlarını etkileyebilecek kullanımlar ortaya koyduğu açıktır. Bu kullanımlar sonucu ortaya çıkan şiddetin tıpkı veri şiddeti kavramının tanımlanmasında ilham alınan örneklerle benzeşen yanları vardır. Yerli Amerikalıların gerçek adlarını kullandıklarında Facebook hesaplarının askıya alınmasındakine benzer şekilde ayrımcılık ve temsilde yanlılığa benzer örneklerin Türkiye'deki ağ bağlantılı teknoloji kullanımlarında ortaya çıktığı görülmüştür. Dolasıyla Türkiye'deki sosyal medya kullanıcılarının veri şiddetine maruz kalmalarını bu teknolojilerin mühendislik kazalarından, veri toplama süreçlerinden ve algoritmik aşamalarından bağımsız olarak düşünülemeyeceği görülmüştür. Bu haliyle Türkiye'deki kullanıcılar gerçek dünyadaki fiziksel şiddete benzer bir biçimde (Hoffmann, 2018) veri şiddetine maruz kalmaktadır denebilir.

Araştırmada incelenen Youtube, Tiktok, X, Facebook ve Instagram uygulamalarının her birinin farklı kullanıcı kitleleri ve amaçları olduğu bilinmektedir. Söz konusu farklı kullanıcı kitleleri ve amaçları tecrübe edilen veri şiddeti türünü de farklılaştırmaktadır. Youtube'u ticari amaçlarla kullananlar genellikle ortamın algoritmaları nedeniyle maddi kayıplarla bağlantılı dijital emek sömürüsüne maruz kaldıklarını söylemektedir. Tiktok ise genellikle kullanıcıları ayrımcı uygulamalarla karşı karşıya getirerek veri şiddeti uygulamaktadır. Bu durum kimi zaman kullanıcının başka bir kullanıcı tarafından ayrımcılığa uğradığında ya da doğrudan Tiktok tarafından uygulanan bir ayrımcılık söz konusu olduğunda ortaya çıkmıştır. X ve Instagram gibi Türkiye'de kullanımı yaygın olan sosyal medya uygulamalarında ise taciz ve siber zorbalığın yaygın olması bireylerin normal hayatlarında karşılaşabilecekleri şiddet unsurlarının ağa da taşındığını göstermektedir. Kullanıcıların paylaştıkları bir görsel ve fikir kaynaklı ya da hiç tanımadıkları insanlar tarafından sadece dolandırıcılık amaçlı atılan iftiralar sonucunda uğradıkları veri şiddeti konusunda şirketler de herhangi bir girişimde bulunmamıştır. Bu yüzden kullanıcılar yaşadıkları mağduriyetlerin giderilmesi için her yolu denedikleri ve son seçenek olarak şikâyet platformuna başvurduklarını belirtmişlerdir. Facebook'ta ise gizlilik ihlallerinin ve veri güvenliğinin kullanıcılara veri şiddeti oluşturduğuna dair şikayetlerin sıklıkla gerçekleştiği görülmüştür. Kullanıcıların yasal olmayan yollarla erişilen hesapları, fotoğraf ve videolarının kullanıcılara veri şiddeti oluşturmuştur.

Kullanıcıların oluşturdukları şikayetler ve şikâyet konularında dikkat çeken bir husus kullanıcıların platformlara duyduğu koşulsuz güven karşısında veri şiddetine uğradıklarıdır. O halde birer teknolojik tasarım ürünü olan sosyal medya ortamlarında veri şiddetine nelerin neden olduğu ve bunun nasıl üstesinden gelineceği noktasında yeni veri etiği savunulabilir. Bu araştırmada incelenen sosyal medya ortamlarında olduğu gibi teknolojik tasarımların içerisine etik girmediğinde bunun gibi veri şiddeti örnekleri ortaya çıkacaktır. Bu yüzden bilgisayar mühendisleri, veri bilimciler ya da bu süreçlerden sorumlu olanlar "etik tasarım" ilkelerine uygun bir biçimde hareket etmelidir. Aksi halde ayrımcı ve eşitsizlikçi tasarlanan teknolojiler veri şiddetinin yeni ve daha ağır örneklerini ortaya çıkaracaktır. Elisa Holmes (2005: 175) da konuya teknik ve etik iki ayrı bakış ikileminin sorunları çözmede bir katkı sağlamadığını belirtmektedir. Teknik ve etik arasında kalan tasarımcıların etik yerine tekniği öncelemesi bu doğrultuda sorunun asıl kaynağıdır. Eşitsizlikçi olmayan ve ayrımcılık üretmeyen, veri şiddetine neden olmayan teknolojik ürünler tasarlayabilmek için teknik ve etiğin birleştirilmesi zorunludur. Aksi halde bu araştırmada görüldüğü üzere kullanıcıların talep ettiği sorunların çözümleri çözüme direnecektir. Bunun yerine kullanılan teknolojinin sürekli veri şiddeti içereceği kanıksanmış ve yaygınlaşmış bir uygulama olarak kalacaktır. Burada bu tür teknolojilerin kullanıldığı ülkelere de görevler düşmektedir. Kullanılan teknolojilerin insanlara veri şiddeti doğurduğu bir durumda devletlerin yasal süreçlerle kullanıcıların koruması söz konusu olabilir. Uygun yasalar ve yaptırımlarla teknolojik şirketler bu yönde adım atmaya zorlanabilir ve kullanıcılar korunabilir. Böylelikle bu çalışmada tespit edilen sosyal medya platformlarının veri şiddetiyle ilişkili yeni boyutlarının anlaşılmasına katkı sağlanabilir ve platformların sorumluluklarının daha iyi kavranması desteklenebilir.

Yazar Bilgileri

Author details

1-(**Sorumlu Yazar** Corresponding Author) Arş.Gör. Dr., Aksaray Üniversitesi, İletişim Fakültesi, Radyo, Televizyon ve Sinema Bölümü, hasanhkayis@gmail.com

Destekleyen Kurum/Kuruluşlar

Supporting-Sponsor Institutions or Organizations:

Herhangi bir kurum/kuruluştan destek alınmamıştır. None

Çıkar Çatışması

Conflict of Interest

Herhangi bir çıkar çatışması bulunmamaktadır. None

Kaynak Göstermek İçin

To Cite This Article

Kayış, H. (2025). Data violence in networked environments: A study on user experience. *Yeni Medya* (18), 106-123, https://doi.org/10.55609/yenimedya.1626763.