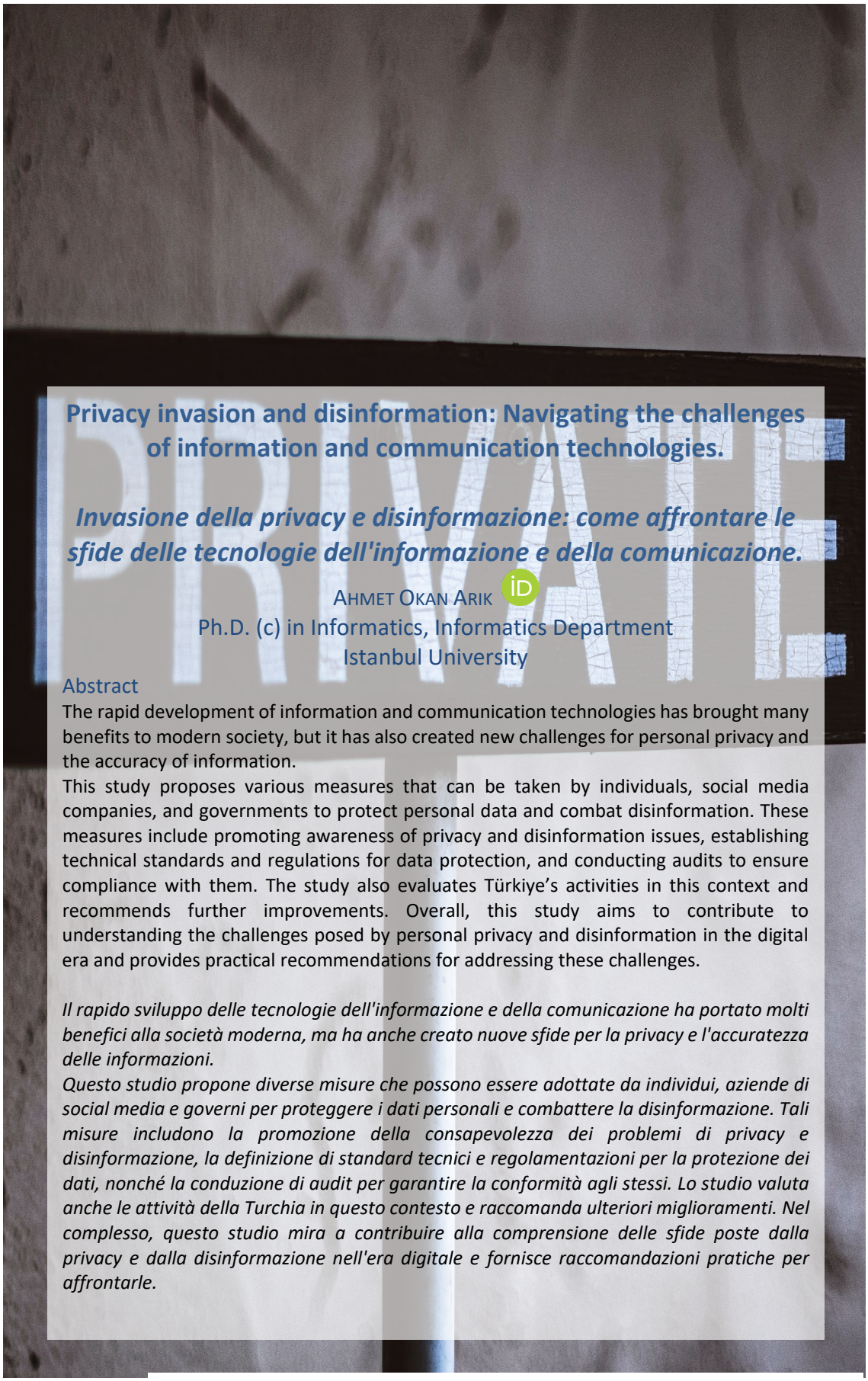
Okan Arik A, 'Privacy invasion and disinformation: Navigating the challenges of information and communication Technologies' (2023) 1 EJPLT, 208-219.
DOI: https://doi.org/10.57230/EJPLT231AOA

EJPLT
ISSN 2704-8012



Privacy invasion and disinformation: Navigating the challenges of information and communication technologies.

Invasione della privacy e disinformazione: come affrontare le sfide delle tecnologie dell'informazione e della comunicazione.

AHMET OKAN ARIK
Ph.D. (c) in Informatics, Informatics Department
Istanbul University

Abstract

The rapid development of information and communication technologies has brought many benefits to modern society, but it has also created new challenges for personal privacy and the accuracy of information.

This study proposes various measures that can be taken by individuals, social media companies, and governments to protect personal data and combat disinformation. These measures include promoting awareness of privacy and disinformation issues, establishing technical standards and regulations for data protection, and conducting audits to ensure compliance with them. The study also evaluates Türkiye's activities in this context and recommends further improvements. Overall, this study aims to contribute to understanding the challenges posed by personal privacy and disinformation in the digital era and provides practical recommendations for addressing these challenges.

Il rapido sviluppo delle tecnologie dell'informazione e della comunicazione ha portato molti benefici alla società moderna, ma ha anche creato nuove sfide per la privacy e l'accuratezza delle informazioni.

Questo studio propone diverse misure che possono essere adottate da individui, aziende di social media e governi per proteggere i dati personali e combattere la disinformazione. Tali misure includono la promozione della consapevolezza dei problemi di privacy e disinformazione, la definizione di standard tecnici e regolamentazioni per la protezione dei dati, nonché la conduzione di audit per garantire la conformità agli stessi. Lo studio valuta anche le attività della Turchia in questo contesto e raccomanda ulteriori miglioramenti. Nel complesso, questo studio mira a contribuire alla comprensione delle sfide poste dalla privacy e dalla disinformazione nell'era digitale e fornisce raccomandazioni pratiche per affrontarle.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Protection of Personal Data; Disinformation; Fake News; Artificial Intelligence; Social Media.

Summary: Introduction. – 1. Personal Privacy & Personal Data. – 2. Protection of Personal Data and Disinformation. – 2.1. Social Media, Personal Data Breaches and Disinformation. – 2.2. The Use of Technology in the Creation and Detection of Disinformation. – 3. Result and discussion.

Introduction.

The concept of technology consists of the Greek words “techne” meaning craft, art, and “logos” meaning word, and it is known to mean talking about arts when it was first used.[1] Today, technology is a functional concept that has outputs to shape people's environment and facilitates people's lives day by day. The invention of writing, which laid the groundwork for the cumulative nature of science and followed by parchment and paper, facilitated the recording and dissemination of thoughts and actions. Mass production of information was achieved with the invention of block printing and its successor printing press. The following important technological development in the field of communication was the telegraph, which made communication independent from transportation boundaries. After developments such as the invention of electricity and the industrial revolution, the social structure changed significantly, and urban life emerged.

Today, the foundations of the Internet, which is one of the basic technologies of the modern world, were laid in 1962 with experiments within the scope of the Defense Advanced Research Projects Agency (DARPA) in the USA. With the development of the World Wide Web technology, an important milestone in communication and information technologies after the Internet by Tim Berners, the Internet has spread globally, and a worldwide information sharing network has been established.[2] When the web was first developed, users as consumers could only interact one-way with content on static websites. Then, users could create and share content thanks to the development of Web 2.0 technology. Thus, individuals who have become both consumers and producers have acquired a new communication tool that allows communication independent of location. Toffler defines these individuals with the concept of “prosumer” meaning content producer and consumer. On the other hand, Henry Jenkins states that Web 2.0 users will democratize the media.[3]

Disruptive technologies such as artificial intelligence, which has recently gained popularity, and the Internet of Things, which is one of the main reasons for the increase in the amount of data generated today by significantly increasing the number of internet-connected devices, the rapidly increasing rate of digitalization and the

[1] R Tulley, ‘Is There Techne in My Logos? On the Origins and Evolution of the Ideographic Term—Technology’ (2008) 4 International Journal of Technology, Knowledge and Society 93.

[2] K Jacksi and S Abass, ‘Development History Of The World Wide Web’ (2019) 8 International Journal of Scientific & Technology Research 75.

[3] H Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York University Press 2006); A Toffler, *The Third Wave* (Bantam 1984).

cheapening data storage and processing costs are giving data a golden age. Apart from disruptive technologies, another development that has significantly increased the size of the data generated is the coronavirus outbreak that emerged in 2019 and affected the whole world. Following the coronavirus outbreak, the internet, which has become the most important tool for individuals to conduct their business and social lives, has significantly increased its influence and effectiveness in many areas. Search engines, satellites, researchers, security agencies, advertisers, and data professionals process terabytes of data every day. A considerable amount of such data is about people - their personal characteristics, ideas, habits, actions, conversations, and preferences - or might be used to generate such data.[4] As of April 2022, it is known that 63% of the world's population, approximately 5 billion people, have access to the internet, and 93% of them use social media.[5] In 2022, 347,200 tweets, 5,900,000 Google queries, 1,700,000 Facebook posts, and 231,400,000 emails were sent per minute. In 2022, the amount of data generated was 97 zettabytes, which is expected to increase to 181 zettabytes by 2025.[6]

The increase in the number of devices connected to the Internet and the increase in the use of social media with a participatory culture make it difficult to solve the problems of protecting personal privacy and accessing accurate information in the virtual environment, which are the problems of today's modern people. Cases such as Russia's manipulation and manipulative fake news on Twitter targeting the 2016 US elections and Facebook's Cambridge Analytica scandal, which involves personal data breaches for manipulation and propaganda purposes, are of great importance in terms of showing the impact and problems that these problems may cause.[7]

In the first part of the study, personal privacy and personal data privacy, privacy violations, and legal regulations established to prevent violations will be discussed. In the second part, the concepts of disinformation and fake news will be defined, and the role of technology in designing and detecting disinformation will be evaluated. Finally, in conclusion, the role of protecting personal data in the fight against disinformation and the steps taken by Türkiye in the fight against disinformation will be evaluated, and the actions to be taken by the stakeholders will be discussed.

1. Personal Privacy & Personal Data.

Confidentiality refers to the unknowability towards the part of the individual that is defined as confidential by others. Literature defines the concept of confidentiality into two main dimensions.[8] These are relational privacy and informational privacy.

[4] J Hoven, 'Information Technology, Privacy, and the Protection of Personal Data' in *Information Technology and Moral Philosophy* (Cambridge University Press 2008).
[5] 'Data Never Sleeps 10.0' (2023) <https://www.domo.com/data-never-sleeps> accessed 8 February 2023.
[6] Statista, 'User-Generated Internet Content per Minute 2022' (2022) <https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/> accessed 8 February 2023.
[7] N Grinberg and others, 'Fake News on Twitter during the 2016 U.S. Presidential Election' (2019) 363 Science (New York, N.Y.) 374.
[8] J Holvast, 'History of Privacy', in *The History of Information Security* (Elsevier 2007).

Relational privacy concerns the boundaries of people's relationships with other people. Examples could be provided for this type of privacy, such as determining who may or may not enter the property one owns or who may have physical contact with oneself. Accordingly, this type of privacy is also called territorial or bodily privacy.[9] Informational privacy is related to collecting, storing, and processing personal data. The common point in both privacy groups is that the individual has control over his/her privacy within the scope of explaining or withholding the information he/she wants and is free to exercise his/her control. For example, an individual may want his/her past to be unknown to others because he/she does not want his/her past decisions or experiences to affect his/her future and is afraid of being secretly watched or listened to. In this way, being able to choose the areas about oneself that one wants to keep private saves one from social pressure and allows one to lead a free life in line with one's own decisions.

Information privacy, defined by Westin as the right to choose by whom personal information is known, is now accepted as a valid definition for data privacy.[10] In the past, when the Internet was not developed or widespread, if personal data such as phone numbers, address information, or identity numbers were leaked or accessed by unauthorized persons, this leakage could only reach a limited geography. However, rapidly increasing mandatory digitalization on a global scale, especially with the coronavirus pandemic that started in 2019 leads to the global accessibility of individuals' communication, personal or any financial data in case of data leakage. [11] [12] However, due to the nature of the Internet, there are problems and risks associated with cybersecurity. Therefore, unauthorized access due to cybersecurity breaches can lead individuals to face fraud, identity theft, impersonation, discrimination, and even physical harm.

The first recorded violation of personal privacy, which determines the individual's freedom and is within the scope of fundamental human rights, dates back to the 15th century.[13] The violation was recorded as the interception of correspondence between two individuals for the purpose of the conspiracy by Governor Bradford in England. In addition, intrusion into the household for the purpose of eavesdropping, media activities that damage individuals' privacy, and wiretapping are among the frequent violations of personal privacy in the past.[14]

Today, advanced communication and information technologies increase the attack surfaces that will damage personal privacy and leave individuals vulnerable to cyber-attacks that many do not even know to exist. For example, video surveillance systems for security purposes, biometric systems used for secure access, genetic data used in deoxyribose nucleic acid analysis, global positioning systems used for location tracking, Bluetooth, a low energy consuming narrow range wireless communication technology,

[9] EPIC and Privacy International (eds), Privacy and Human Rights 2002: An International Survey of Privacy Rights and Developments (Epic 2002).

[10] A Westin, *Privacy and Freedom* (Ig Publishing 2015); J Ziegeldorf, O Morchon and K Wehrle, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7 Security and Communication Networks 2728.

[11] McKinsey, 'COVID-19 Digital Transformation & Technology' (2020) <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever> accessed 12 February 2023.

[12] C Bekara, 'Security Issues and Challenges for the IoT-Based Smart Grid' (2014) 34 Procedia Computer Science 532.

[13] R Hixson, *Privacy in a Public Society: Human Rights in Conflict* (1st Edition, Oxford University Press 1987).

[14] Holvast (n 8).

Wi-Fi within the scope of IEEE 802.11 wireless network protocols, database where data is kept in a virtual environment, digital twin, internet of things, artificial intelligence and other advanced technologies can contain many so-called zero-day vulnerabilities as well as the benefits they provide. Therefore, all organizations that collect, process, or store personal data should identify, analyze, evaluate, and assess the cyber risks they are exposed to and take action according to the assessment results. In this context, organizations should improve their cyber capabilities and comply with national and international legal regulations (e.g., Kişisel Verileri Koruma Kanunu (KVKK), General Data Protection Law (GDPR)), and sectoral technical standards. In addition, organizations should establish effective internal control and audit mechanisms for the control and supervision of these processes to ensure and increase effectiveness and efficiency of the processes. Otherwise, the money and power value of data, which has increased incomparably in the past, may cause the company responsible for data breach cases to lose brand value, lead to a decrease in the number of customers and revenues, and cause the organization to be fined severely by the authorities. Another result that shows the increasing data value is that the average cost of data breach cases reported in 2022 was determined to be 4.35 million dollars. This figure has been increasing continuously compared to previous years.[15]

In some way, all countries and societies in the past and present have limited access to various types of personal data. There are propriety, traditions, technologies, laws and regulations, as well as combinations of these, that forbid or restrict the usage or compromise of personal information.[16] The fact that violations of personal privacy and personal data undermine privacy, one of the most fundamental individual rights enshrined in the Universal Declaration of Human Rights in 1948, has forced lawmakers to take action on this issue. The US Privacy Act, one of the first and important laws in terms of anonymity and personal privacy, was passed in 1974 to cover mandatory practices for the anonymity and privacy of individuals.[17] The law in question covered the principles of notice, consent, individual access and control, purposeful use, adequate security, data minimization, and accountability. The European Union, on the other hand, included the principle of explicit consent among these principles with the comprehensive law enacted in 1995.[18] The main objective of the regulation was to align data protection laws across EU member states and guarantee the rights and freedoms of individuals in the processing of personal data. The law provided the data subject with rights of access, rectification, objection and deletion, as well as ensuring lawfulness, fairness and transparency. It also aimed to ensure data protection in cross-border data transfers. To implement the law, each EU member state was expected to establish a national data protection authority. The Directive laid the foundation for data protection in the EU and the General Data Protection Regulation in 2018 paving the way for

[15] IBM, 'Cost of a Data Breach' (2022) <https://www.ibm.com/reports/data-breach> accessed 12 February 2023; Security Magazine, 'Data Breaches in 2022' (2022) <https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022> accessed 12 February 2023.

[16] V Hoven (n 4).

[17] J Eden, 'When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID' (2005) 4 Duke Law & Technology Review 1.

[18] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

subsequent regulations that further enhance privacy rights and data protection standards.

Today, the GDPR established by the European Union and the KVKK in force in Türkiye aims to ensure individuals' privacy and data by holding organizations responsible for the data they collect, process and store. The GDPR is a comprehensive data protection law that has developed in response to the need for stricter privacy regulations in the context of rapidly evolving technological developments.[19] Building on the Data Protection Directive of 1995, the GDPR was developed to address the challenges of the internet and social media in protecting personal data. In 2012, the European Commission proposed a reform to protect the privacy of individuals and make organizations that process personal data accountable for it. Following this, the GDPR was proposed by the European Parliament in 2016. The law includes stricter rules for consent, strengthened individual rights, stringent obligations for data controllers and processors, and strict penalties for non-compliance. The fact that international firms have EU citizen stakeholders extends the law beyond EU borders. In conclusion, the GDPR is an important development that puts individuals in an empowered position and emphasizes the importance of data protection and privacy rights with increasing digitalization. KVKK, like other data protection and personal privacy protection laws, was developed in response to individual privacy and data protection concerns.[20] Influenced by the EU's Data Protection Directive, Turkey recognized the need for a comprehensive legal framework for the collection and processing of personal data within its borders and jurisdiction. The law, modeled on the EU's GDPR, entered into force on April 7, 2016. The law sets out principles such as data subject rights, purpose limitation and strictly defines the roles of data controllers and processors. Following a two-year transition period following the law, compliance with the law is overseen by Turkey's Personal Data Protection Authority. With the law, Turkey aims to protect personal data, comply with international standards and ensure transparent and secure data processing within the country. Amendments and additional regulations are made to improve the law and to address subsequent challenges arising from technological developments, etc.

2. Protection of Personal Data and Disinformation.

Many disciplines have intensively studied the concepts of disinformation, misinformation and fake news. Misinformation is unintentionally false or misleading, while disinformation is intentionally false or misleading.[21] Claire Wardle and Hossein Derakhshan define misinformation as the unintentional dissemination of false photographs, dates, statistics, translations, and satire that is taken seriously, while disinformation is the intentional dissemination of manufactured or intentionally

[19] General Data Protection Regulation (GDPR) (2016/679).

[20] Kişisel Verilerin Korunması Kanunu 2016.

[21] C Jack, 'Lexicon of Lies: Terms for Problematic Information' [2017] Data & Society

manipulated audio or visuals.[22] Today, it is the most comprehensive definition close to current, considering technologies such as deep fake technology, which allows the imitation of another person created with deep learning technology, and ChatGPT, which can synthesize fictional text.

Although the concepts of disinformation and misinformation are often used interchangeably, they have differences, as seen in the definitions mentioned. Misinformation is a concept that has been discussed in the literature before the concept of disinformation, which has increased in popularity and academic interest in recent years.

Freelon and Wells state that while the mere inaccuracy of messages is sufficient to use the concept of misinformation, disinformation is created to produce various effects other than having false or misleading content.[23] The assumptions underpinning the political decision-making process are targeted at this point in order to create this effect. Therefore, disinformation is intensively studied in political contexts and issues. Apart from its impact on decision-making processes, disinformation is designed to create divisions between allies, conflict between ethnic groups, create dichotomies between individuals and groups, or manipulate the masses in national decision-making. Rubin defines disinformation for manipulation as three different factors: materialism, gaining domestic and foreign political influence, and causing problems.[24] In these concepts, both containing false messages, distinguishing disinformation from misinformation requires reading intentions. In summary, instead of working on the distinction between these two concepts, which require relative subjectivity, some studies in the literature examine the concepts of misinformation and disinformation under the umbrella of fake news.[25]

2.1. Social Media, Personal Data Breaches and Disinformation.

The history of content containing false and misleading information that we frequently encounter on social media platforms may be traced back to the invention of the printing press.[26] Depending on the context, such content can cause economic, political, and social harm and even influence elections by disseminating fake news, as in the US.[27] For example, Cambridge Analytica, which influenced the US elections, was established as a political consulting firm in the UK. The company collected the personal data of approximately 87 million people on Facebook and classified people into 200 different profiles using various data mining methods. As a result of the analysis, individuals

[22] C Wardle and H Derakhshan, 'Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making' (Council of Europe 2017) <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html> accessed 28 January 2023.

[23] D Freelon and C Wells, 'Disinformation as Political Communication' (2020) 37 Political Communication 145.

[24] V Rubin*, Misinformation and Disinformation: Detecting Fakes with the Eye and AI* (1st ed. 2022 edition, Springer 2022), 7-8.

[25] V Rubin, 'Disinformation and Misinformation Triangle: A Conceptual Model for "Fake News" Epidemic, Causal Factors and Interventions' (2019) 75 Journal of Documentation 1013; Rubin (n 20); Rubin.

[26] B Collins and others, 'Trends in Combating Fake News on Social Media – a Survey' (2021) 5 Journal of Information and Telecommunication 247.

[27] C Silverman, 'This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook' (BuzzFeed News, 2016) <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook> accessed 20 January 2023.

classified among the profiles were shown content and advertisements on Facebook to change their voting preferences. This scandal, which targets approximately one-third of the US population, has led individuals to think about and change their behavior regarding the internet and to protect their data.

Studies show that uninformed social media users undeniably contribute to the spread of disinformation, misinformation or fake news content. For example, in their study, Gabielkov, Ramachandran, Chaintreau, and Legout found that 59% of users shared shortened URL (bit.ly) links on Twitter without reading them, while Glenski, Pennycuff, and Weninger found that 73% did so on Reddit.[28] These data show how disinformation can easily reach large masses through bot networks and unconscious social media use.

As part of its fight against disinformation and manipulation, Facebook identified and removed 150 networks of fake accounts, pages and groups between 2017 and 2020 that exhibited Coordinated Inauthentic Behavior (CIB), which aims to mislead individuals.[29] The report found that CIB networks were most prevalent in Russia with secret services and media organizations, Iran with state institutions, Myanmar with military or police forces, the United States with political actors, public relations firms and media websites, and Ukraine with public relations agencies and political parties. The report states that the countries most targeted by CIB networks are the US, Ukraine, the UK, Libya and Sudan.[30]

2.2. The Use of Technology in the Creation and Detection of Disinformation.

The generation and dissemination of disinformation are some of the malicious use scenarios of technology. Bot networks consisting of a large number of internet-connected devices play an important role in the creation and dissemination of disinformation as well as distributed denial of service attacks. Artificial intelligence services capable of synthesizing text, such as deep fake technology that enables audio and video impersonation, clickbait content headlines, and ChatGPT, which can write fake news articles, may be used as sources of disinformation.[31] These technologies can play an important role in manufacturing consent by spreading to large masses through bot networks to influence and manipulate the masses or propaganda.

ChatGPT is a language model developed by OpenAI. ChatGPT uses the "Generative Pre-trained Transformer (GPT)" architecture based on deep learning techniques. It uses pre-trained transformer architecture to understand context when processing text data

[28] M Gabielkov and others, 'Social Clicks: What and Who Gets Read on Twitter?' (2016) 44 ACM SIGMETRICS Performance Evaluation Review 179; M Glenski, C Pennycuff and T Weninger, 'Consumers and Curators: Browsing and Voting Patterns on Reddit' (2017) 4 IEEE Transactions on Computational Social Systems 196.

[29] N McCarthy, 'Infographic: Russia & Iran Are Facebook's Top Sources Of Disinformation' (Statista Infographics, 2021) <https://www.statista.com/chart/24930/coordinated-inauthentic-behavior-networks-removed-by-facebook/> accessed 15 October 2022.

[30] Facebook, 'Coordinated Inauthentic Behavior Report' (2021) <https://about.fb.com/news/2021/11/october-2021-coordinated-inauthentic-behavior-report/> accessed 22 February 2023.

[31] N Dhanjani, 'AI Powered Misinformation and Manipulation at Scale #GPT-3' (O'Reilly Media, 25 May 2021) <https://www.oreilly.com/radar/ai-powered-misinformation-and-manipulation-at-scale-gpt-3/> accessed 20 January 2023; W Knight, 'AI Can Write Disinformation Now—and Dupe Human Readers' [2021] Wired <https://www.wired.com/story/ai-write-disinformation-dupe-human-readers/> accessed 20 January 2023.

and an enhanced self-attention mechanism to understand word relationships.[32] ChatGPT can interact with users naturally and fluently, thanks to the technologies mentioned. It may perform tasks such as answering user questions, following instructions, making suggestions, and creating text. ChatGPT, which may be integrated with a user-friendly interface, is used extensively for different purposes.

Another deep learning based technology, deep fake, can be applied to all areas of digital media. Therefore, there are many scenarios for the malicious use of these technologies: Users can place a target's face on another body in photos or videos and manipulate the target's facial expression by using their own face in a re-enactment application. Lip movements can be copied to a speaker in a video with a lip synchronization application, and fake video content can be circulated with audio generation. In addition, with the ability to generate automatic text, it is possible to make a topic a hot topic on social media, direct the masses, and trigger bot networks. With the ability to generate images, real-looking fake accounts can be created on social media by designing human faces that have never existed before. Through these fake accounts, communication can be established with the individuals to be defrauded, and various fraud or intelligence activities can be carried out using these methods.

Artificial intelligence also plays an important role in detecting disinformation as an antidote. Natural language processing, machine learning and deep learning methods, which are sub-fields of artificial intelligence, are used to detect disinformation and fake news in social media with artificial intelligence. According to Shu et al., there are two important stages in generating detection models using these methods.[33] The first stage is the feature extraction step. It involves extracting semantic and syntactic features of the text using natural language processing methods, as well as data such as the source, title, and whether there are images in the content. The second area of feature extraction is the user sharing the content and the network they are connected to. In order to determine the reputation and credibility of the user within the scope of the user and the content he/she produces, various attributes such as the demographic information of the user, the year of registration on the relevant social media platform, the number of followers and the number of people he/she follows, and the number of content he/she shares are extracted in this context.[34] The feature extraction within the scope of the network includes the attributes extracted from the interaction area created by the user according to their interests, topics and relationships. The next important stage after feature extraction is the detection model building stage.

Fake news detection models are divided into two different groups. These are content-based and social context-based models. Content-based models are used to detect misinformed content by examining studies involving information confirmation and the misinformed text's stylistic features. Social context-based models are auxiliary models usually used in conjunction with content-based models to increase the success of fake news detection. These models are divided into viewpoint-based and

[32] A Vaswani and others, 'Attention Is All You Need' (arXiv, 5 December 2017) <http://arxiv.org/abs/1706.03762> accessed 21 April 2023.

[33] K Shu and others, 'Fake News Detection on Social Media: A Data Mining Perspective' (2017) 19 ACM SIGKDD Explorations Newsletter 22.

[34] C Castillo, M Mendoza and B Poblete, 'Information Credibility on Twitter' (2011).

propagation-based models.[35] Viewpoint-based models are models that deal with the reactions to a post containing misinformation on social media. Propagation-based models, on the other hand, assume that content credibility is highly correlated with the credibility of related social media posts and examine related posts on social media to estimate content credibility.

3. Result and discussion.

Fake images, sounds and texts produced by artificial intelligence in a very realistic manner are used by states and organizations to manipulate and direct society by creating and disseminating fake news and disinformation on social media. Disinformation campaigns utilize the anonymity and connectivity features of the internet to create fear, anxiety and panic in society, disrupt social order, create social unrest, incite people to riot and create social division.

Social media platforms analyze users' posts and interactions to determine the preferences, behaviors and habits of the target audiences they define. By processing this data, which is used for advertising and marketing, it is aimed to offer product/service recommendations that match the target audience or similar content suggestions to ensure that they spend more time in the application. These recommendations cause users to encounter more content similar to their own views, thus increasing the likelihood of being exposed to false and misleading information. In order to prevent this problem, laws that set rules on the processing of personal data, such as KVKK and GDPR, restricting the collection of data that will enable users to be micro-targeted on social media will reduce the impact of fake news that cannot reach its target.[36] For example, in 2018, a study showed that organic sharing of anti-vaccine fake news decreased by 75% when accounts spreading disinformation about vaccines were blocked from advertising.[37] The sensitivity of these regulatory laws to transparent data processing processes and the continuity of audit activities are also important in combating disinformation. In addition to legal regulations, authorities should actively combat disinformation through public education and awareness-raising efforts to protect national security and interests, various internet regulations such as liability agreements with social media platforms, and international cooperation agreements.

In the context of combating disinformation and fake news, individuals should limit their data accessible on the internet in order not to be targeted in disinformation campaigns. Otherwise, publicly accessible personal data can create a convincing and trustworthy profile image on social media accounts that produce disinformation. In addition, individuals who use social media to get news should verify the news with fact-checking tools such as Google Fact Check before taking action following a news story and acting based on confirmed information. Individual measures can not only prevent

[35] Shu and others (n 33).

[36] A Campbell, 'How Data Privacy Laws Fight Fake News' (2019) NA Just Security <https://www.osti.gov/biblio/1598114> accessed 22 February 2023.

[37] L Chiou and C Tucker, Fake News and Advertising on Social Media: A Study of the Anti-Vaccination Movement (National Bureau of Economic Research 2018).

the spread of disinformation and fake news but also help protect personal data and create a healthy communication environment on social media platforms.

Social media organizations are one of the most important stakeholders in the fight against disinformation and fake news. Content that is very similar to the truth, which is the source of disinformation produced by artificial intelligence, significant amounts of social media flow data, the anonymity provided by the internet and the unconscious use of social media make it difficult to track and detect disinformation. Artificial intelligence, which plays a role in generating fake content that is very close to the truth, can also be used to detect and monitor disinformation. Real-time data processing technologies using natural language processing and deep learning methods can detect misinformation at a rate close to the real-time data flow of social media. The use of artificial intelligence by social media organizations and even intelligence agencies within the scope of social media intelligence is one of the technical measures that can be taken in the fight against disinformation and fake news. In addition to these, social media organizations should fulfill their responsibilities in combating disinformation by taking steps such as blocking fake accounts, labeling false information according to users' reporting and autonomous systems, and raising awareness among users.

Türkiye, which ranks 7th in the world among the most active social media users with its young population, is the target of intensive disinformation campaigns. [38] Disinformation campaigns carried out as fifth-column activities aim to create social unrest and divisions in Türkiye, which hosts various ethnic elements and many refugees, and to persuade the society. In addition to these reasons, sharing false reports and fake news on social media after the Kahramanmaras earthquake on February 6, 2023, interrupted search and rescue and relief activities in the field. As part of the fight against disinformation, the Center for Combating Disinformation was established on August 5, 2022, under the Communications Directorate of the Presidency of the Republic of Türkiye, the Center for Combating Disinformation started publishing a weekly disinformation bulletin on October 11, 2022, and on October 18, 2022, the Law on Amendments to the Press Law and Certain Laws introduced articles on combating disinformation and established various requirements for social media platforms, such as the obligation to open representative offices in Türkiye.[39] With these actions, Türkiye can be said to have an active anti-disinformation policy. In addition, providing personal data protection and media literacy training in schools will be effective in creating a society of conscious social media users.

[38] 'Reuters Institute Digital Report' (2018) <https://www.digitalnewsreport.org/./survey/> accessed 22 February 2023; 'Twitter Stats' (2023) <https://datareportal.com/essential-twitter-stats> accessed 22 February 2023.
[39] Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun 2022.