JOURNAL OF AWARENESS
HOLISTENCE publications

Journal of Awareness
Volume / Cilt: 8, Issue / Sayı: 2, 2023, pp.205-220
E-ISSN: 2149-6544
https://journals.gen.tr/joa
https://doi.org/10.26809/joa.2013

Received / Geliş: 03.02.2023
Accepted / Kabul: 22.03.2023

RESEARCH ARTICLE/ARAŞTIRMA MAKALESİ

Examining the breaching of personal data in cyberspace from the perspective of psychological violence

Buse Akça

Lawyer, Istanbul No.1 Bar Association, IMDAT Association, Türkiye, e-mail: akcabuse09@gmail.com

Abstract

The digital world has taken an active role in people's lives day by day. In this context, information that directly or indirectly identifies the person has also found its place in the digital world. The right to privacy and the protection of personal data, which is also defined as a personal right, can be violated consciously or unconsciously in the digital world due to anonymity, speed and easy accessibility.

When it comes to the illegal capture, sharing and use of personal information by others without their consent, people are sometimes unaware that these actions are against the law. However, data breach acts can cause emotional trauma on the person. Emotional effects can sometimes be much more severe and irreversible than physical effects. For this reason, I carried out my study on the importance of data security and that the violation of personal data can also cause psychological violence. The research was carried out online by creating a questionnaire as a data collection tool with the quantitative research method. As a study group, it was aimed to reach people over the age of 18 in Turkey. In order to address the problematic of the research, an online questionnaire was created via Google Forms and this questionnaire was distributed on the online network and 50 people, 22 female and 28 male, were reached from Turkey by random sampling method.

In the survey, 17 multiple choice questions and 2 open -ended questions were asked. The questions are prepared within the scope of the determination of whether the personal data of the individuals have been violated and the psychological effects on individuals whose personal data are violated.

As a result; It is considered that the violation of personal data is directly proportional to the negative psychological effects on individuals.

Keywords: Personal Data, Virtual World, Cyber Bullying, Psychological Violence, Breach of Personal Data.

Citation/Atıf: AKÇA, B. (2023). Examining the breaching of personal data in cyberspace from the perspective of psychological violence. *Journal of Awareness*. 8(2): 205-220, https://doi.org/10.26809/joa.2013

Corresponding Author/ Sorumlu Yazar:
Buse Akça
E-mail: akcabuse09@gmail.com

1. INTRODUCTION

People are using digital channels to carry out daily activities as technology advances. The advantages and disadvantages of digital platforms actively involved in interaction are being discussed in today's virtual world. In this context, the problem of violence, which we have faced in recent years and which may be the biggest social problem of the coming years, emerges as one of the negative effects of digital platforms. In order to maintain the cultural, ethical, and psychological future of human society at a healthy level, it is necessary to analyze this problem in a multifaceted way.

According to the type of violence, physical violence, sexual violence, emotional violence, economic violence, and cyber violence can be classified with subheadings. The most common type of violence is physical violence (Polat, 2017). However, the number of violent acts carried out on digital platforms without physical contact with the developing technology has increased significantly. Violent acts carried out through digital platforms are generally referred to as "cyber violence". Cyber violence is defined as the repeated use of information and communication technologies by an individual or group to harm other individuals (Belsey, 2007) However, it should be kept in mind that violent acts can contain more than one type of violence.

Although the actions carried out by the use of digital platforms as a tool of violence are defined as cyber violence, digital environments can also be used as a tool of psychological violence. Because, psychological violence includes behavior patterns that a person or group does against a certain person and that aims to weaken the person emotionally and to harm him psychologically. At this point, psychological violence can be carried out in the physical environment as well as in the digital environment. Therefore, actions carried out with the instinct of emotionally wearing out the person and harming the person psychologically in the cyber environment can be considered as the online appearance of psychological violence. In this context, it cannot be said that there are sharp lines between cyber violence and psychological violence perpetrated online. Therefore, types of violence give birth to each other over time and the boundaries between them disappear (Kara & Uluc, 2019).

Psychological violence is carried out with all kinds of verbal and physical behaviors that can cause psychological intimidation of a person and damage to self-esteem (Orbay, 2022). In literature, psychological violence, also referred to as "Emotional Abuse," "Emotional Violence," or "Psychological Abuse," targets the identity and/or identity formation of the victim and are actions aimed at satisfying the social or individual needs of the perpetrator (Kolburan, 2021). In general, psychological violence encompasses actions that harm the victim psychologically and enable the abuser to exploit the victim psychologically (Polat, 2016). Since the perpetrator and victim do not need to be physically present in psychological violence acts, it is also possible to encounter psychological violence acts in the virtual world of the evolving world.

In this context, people may be exposed to psychological violence through different actions on digital platforms.

With technology becoming an indispensable part of our daily lives, people have started to share and interact with many of their own data, especially on social media platforms. With technology advancing day by day, information and communication technologies are rapidly encircling the social life of people. Thanks to information and communication technologies, it has become easier for personal data to be subjected to the collection, classification, and storage processes and to be easily presented when requested, and as a result, the risk of unfair use of this information about private life has also arisen. These technologies provide a suitable environment for the disclosure of personal data to others without obtaining the consent of the person and the transfer of information from the place where it is located to other places (Kılınc,2012).

In this context, the personal data shared by people through digital platforms can sometimes be used for malicious purposes. Sometimes, the personal data of people are violated by cyber-attacks without being aware of it. These actions

can also be referred to as personal data breaches, as well as actions that constitute elements of psychological violence and cause data subjects to experience psychological trauma as a result of privacy and privacy concerns. Because privacy and confidentiality concerns related to online platforms mainly involve the sharing of personal data without consent, such as the use of personal data by third parties and organizations (Boyd and Ellison, 2007). This concern creates effects such as making people feel insecure, helpless, and afraid. Because the processing of personal data at every step taken by people, the tracking of people both physically and online, the fact that companies or the state are more familiar with the information belonging to people than people's relatives evoke a dystopian social order. In such an order, the formation of a society of fear is inevitable(Ozkan,2020).

Psychological violence can arise in any environment where people are communicating with each other. Therefore, psychological violence is referred to as a social reality witnessed in the interpersonal, intergroup, mass communication, and even international communication processes (Yalın B. etc.).

In this article, it is aimed to investigate the relationship between personal data breach and psychological violence by focusing on how people whose personal data were violated before felt after the breach.

In this direction, first of all, personal data, psychological violence, and related concepts will be explained to ensure that the concept can be understood.

2. CONCEPTUAL FRAMEWORK

2.1. The Concept of Personal Data

Data belonging to people is information that is attributed great importance and desired to be known by people and communities for different reasons and purposes from the past to the present. Although the most basic reason for this desire is the feeling of curiosity inherent in humanity and related to psychological science, over time, the relationship of the desire to know personal data with different fields such as economic, sociological, and technological has come to the fore (Dulger, 2020). In this context, with the developing technology, personal information has started to be collected more easily and quickly. Because, thanks to the facilities and conveniences provided by technological tools, it has become possible to record, monitor, and process personal data in a much easier way. Such fast and easy sharing of personal information has brought risks to it. Thus, the necessity of protecting information belonging to individuals has come to the agenda.

The concept of personal data is a concept that belongs to the "self" and is considered in a wide range from name to image, preferences, feelings and thoughts. For this reason, the loss of the individual's control authority over these data brings the loss of the individual's freedom, autonomy, privacy, in short, the ability to be "self". The protection of personal data is an issue that is directly related to the protection of the individual and should be considered together with basic human rights (Izgi,2014).

Personal data in Turkey is protected as the right to request protection of personal data as part of the privacy of personal life under the heading of basic rights and freedoms in Article 20 of the Turkish Constitution in 2010. In 2016, the Turkish Personal Data Protection Law (PDPL) numbered 6698 came into force in this context. Personal data, although it does not have a uniform definition, is defined as any information related to an identified or identifiable real person in national legislation (PDPL) and doctrine. In this context, personal data includes not only information such as name, surname, Turkish ID number, address, image, and voice, but also information such as IP address, password, log records, etc. as technology advances. This is information that has the characteristics to identify or make a person identifiable. Some of the data contained in the scope of personal data are much more sensitive than others and need a level of protection (Atalay, 2019). The reason why some data are called sensitive and put under more effective protection in this way is due to the fact that these data have a closer relationship with the basic rights and freedoms of a person (Dulger, 2018). These data are referred to as special quality data. It is

possible to classify specially qualified personal data as sensitive data and other personal data as non-sensitive data (Kutlu and Kahraman, 2017). The distinction between personal data and specially qualified data is particularly evident in the matter of obtaining explicit consent in the process of processing personal data. According to national legislation; of a person of faith and political data, including race, ethnic origin, political opinion, philosophical belief, religion, sect, or other beliefs, costume and clothing, Association or trade union membership, health, sexual life, criminal convictions, and security measures, as qualified private data is considered. These data are limited in number and cannot be expanded. It is not possible to process these data without the explicit consent of the person concerned. Therefore, data of a special nature are subject to much stricter protection.

2.2. Processing of Personal Data

In the processing of personal data, it is mandatory to comply with legal and ethical rules, be accurate and up-to-date when necessary, be processed for specific, clear and legitimate purposes, be limited and proportionate, and be preserved for the duration specified in relevant legislation or necessary for the purpose of processing. (Article 4 of PDPL)

In Turkish law, personal data can only be processed in cases provided for by law or with the explicit consent of the person, according to Article 20/3 of the Constitution. This regulation also shows that the processing of personal data is generally prohibited. The reasons for compliance with the law are regulated in Articles 5 and 6 of the PDPL and compliance with the law in the processing of personal data primarily refers to the processing in accordance with the provisions of Articles 5-6 of the PDPL. In addition, according to Article 4 of the PDPL, general principles of compliance must also be ensured in the processing of personal data (Yucedag, 2019).

Personal data cannot be processed without the explicit consent of the data owner (relevant person) as specified in the law. However, the PDPL provides for exceptions to this rule. However, there are limits to these exceptions as well. For example, if a person's personal information shared on a social media platform is used for a purpose other than sharing, it may not be considered an exception and may be considered a personal data breach.

Processing of personal data in PDPL "Acquiring, recording, storing, keeping, changing, rearranging, disclosing, taking over, making available personal data in whole or in part by automatic or non-automatic means provided that it is a part of any data recording system, It is defined as "all kinds of operations performed on data such as classification or prevention of use" (PDPL art. 3 / I-e)."

Personal data processing refers to a series of processes including obtaining, recording, organizing, adapting, transforming, using, disclosing, combining, and deleting data (Kaya, 2011).

It can be said that every transaction regarding the transmission, storage, or destruction of data belonging to a natural person, together with the uploading of the data to a digital platform or electronic closed systems, is the processing of personal data. At the same time, any act of modifying personal data, including deletion and destruction, can also be considered data processing (Oguz,2018).

2.3. Violation of Personal Data

The concept of a data breach in the General Data Protection Regulation (GDPR) of EU legislation is defined as "an accidental destruction, loss, alteration, unauthorized disclosure, or access resulting from a security breach of personal data transmitted, stored or processed," while in our law, it is defined as "the illegal acquisition of processed personal data by others." (PDPL)

In this context, the violation of personal data can be defined as the unlawful seizure, recording, or giving to someone else of the information that determines the identity of the person or makes it identifiable, not being deleted, anonymized, destroyed, or disseminated when it should be deleted. Violation of personal data, which is protected as a constitutional right, is also a type of crime regulated in the Turkish Penal Code. Sometimes, real persons and sometimes legal

persons may commit an act of violation of our personal data at a moment that we do not know at all. Personal data has such a broad framework that data breaches can sometimes be carried out as a result of cyber attacks, while sometimes the information we provide to people in our immediate environment may be brought to the agenda by methods of unauthorized transfer to others. The most important and common point of the methods of violation of personal data affecting people is the danger of violation of privacy and confidentiality of private life.

2.4. Privacy and Confidentiality of Private Life

Privacy; It defines the individual space and what belongs to the individual. Any kind of information that individuals do not want to share with someone else refers to what is private (Dulger, 2020). Privacy is expressed in 3 different dimensions "spatial privacy" is the protection of the space in which individuals live; "individual privacy", includes the protection of individuals against unfair interventions; "information privacy" in the sense that the control of how the collection, storage, and processing of data of a private nature will be, belongs to individuals (Karagulle, 2015). Despite all the differences in privacy, it is understood that the common point is that people can maintain control in their own areas. At this point, it can be said that the amount of privacy areas where individuals can maintain their own control has also increased (Eroglu, 2018). At this point, people feel the need to provide control of their own data, and in case of violation of this need, findings such as anxiety, panic, and fear are observed in people.

Confidentiality of private life, on the other hand, is guaranteed in international documents on human rights and democratic constitutions in relation to the concept of privacy. The physical characteristics of the person, the person's religion, conscience, thoughts and opinions, information about health, education, employment status, family life, and communications with others are within the scope of private life (Kilinc, 2012). Private life is the life of a person that is not in front of others, is closed to the public, and is hidden from everyone. Private life is the right of a person to be respected, to want to be left alone, and to be able to continue his life in a way he does not want and does not want to be transferred to the public. A private living space is a section of a person's life that includes activities and behaviors that are known and shared with their relatives (Celik,2017). The relationship between the concepts of personal data and private life; arises from the source of private life. With this; The right to privacy is broader than personal data, and privacy also includes the protection of personal data (Akgul,2016).

The development of technology has led to one of the risks to privacy and confidentiality being the issue of who can access the personal information shared by individuals on the internet and social networking sites. In this context, it is important to identify and raise awareness of information that can be considered personal in discussions about online privacy and confidentiality threats and risks (Aïmeur, Gambs, and Ho, 2010).

In this context, it is inevitable for people to be uneasy and worried as a result of sharing their personal information without their consent. As a matter of fact, when the privacy and confidentiality of private life and the violation of personal data are evaluated together, it is highly likely that psychological trauma will occur in people whose data is unlawfully violated.

3. PSYCHOLOGICAL VIOLENCE

Violence is defined by the World Health Organization as "the possibility or possibility of causing injury, death and psychological harm to a person who is exposed as a result of the intentional application of physical force or power to someone else in the form of a threat or reality" (WHO, 2002). The following subheadings appear in the classification of violence according to the type of violence applied. 1. Physical violence 2. Sexual violence 3. Emotional violence 4. Economic violence 5. Cyber violence (Polat,2018).

Violence is subject to many classifications in the literature, and it is important to consider the emotional effects of violence on people among these classifications. Although the effects of violence on individuals are not measurable, it can be suggested that pressures felt indirectly and concretely (economic violence, media terrorism,

chronic unemployment, traffic accidents, unhealthy working conditions, etc.) should be included in the category of violence (Onbas, 2007). In this context, developing technology and social variability and the effects and indirect types of violence can also vary by being included in a broad category. Therefore, any form of behavior that can cause people to suffer physically or psychologically can be expressed as violence. In order to be able to recognize psychological violence, detailed theoretical and evidence-based knowledge of what it is needed. As the forms of communication increase, it becomes easier for discourses or actions to turn into psychological violence (Orbay, 2021).

Psychological violence has been subjected to many definitions in the literature. According to Ozerkmen and Golbasi; While psychological violence is violence against one's mental integrity by means of brainwashing, lying, indoctrination, and threats, according to Tutar, non-physical attitudes and behaviors that negatively affect the health and psychology of the individual, upset him, and cause him to feel pressured and threatened are psychological. it is evaluated within the scope of violence (Tutar, 2004). Although there are many definitions of psychological violence, in common; It can be considered as acts of violence that affect the person psychologically, wear them down, and put them under pressure.

Nowadays, digital environments can also turn into a tool, especially for psychological violence. For example, any action or undesirable image can be converted into an element of psychological violence by transferring it to a digital medium or by threatening to transfer it, as well as the act of violence itself can be transferred to a digital medium and reproduced (Peltekoglu and Tozlu,2017).

Violent acts in digital environments may contain elements of psychological violence, while cyber violence may contain elements. Because, Cyber violence is defined as acting in bad faith by an individual or group with the aim of harming other individuals through information and communication technologies. (Süslü, 2016). In addition, as a result of cyber violence acts, there are many psychological effects on the victim. Also, the example of psychological violence discussed in the study takes place in the cyber environment.

In this context, the types of violence that are intertwined with each other come across.

Violence, which can be carried out quickly and easily in digital environments, especially with the anonymity element in digital environments, is a reason that attracts the perpetrator to violence in the virtual environment rather than in the physical environment (Abınık, 2021). The violent person can sometimes do this consciously and sometimes unconsciously. Unauthorized seizure and processing of personal data of persons can be considered as psychological violence behavior both in terms of cyber violence behavior and in terms of its effects.

The psychological effects of violent acts committed in the digital environment on the victim are seen as sadness, intense stress, feeling worthless, being ashamed of learning information about oneself, and not loving oneself (Korkmaz, 2016), But these effects are also not limited in number. On the other hand, social effects include a decrease in self-esteem, distrust of others, being antisocial, having difficulty establishing a friendship relationship, and conflict in friendship relationships (Korkmaz, 2016).

Similarly, after a while, symptoms such as loneliness, fear, lack of self-confidence, restlessness, and excessive tension begin to appear in individuals who are exposed to psychological violence. If these actions continue for a long time, psychological diseases such as post-traumatic stress disorder and acute stress disorder may occur.

4. METHODOLOGY

The research was carried out online by creating a questionnaire as a data collection tool with the quantitative research method.

The questionnaire was prepared in the Turkish language via Google form. People over the age of 18 in Turkey have been identified as the target audience. This questionnaire was distributed over the online network and 50 people, 28 men and 22 women, were reached from Turkey by random sampling method. In the survey, 2 de-

mographic, 15 multiple choice, and 2 annotated questions were asked. The questions have been created in three stages in order to determine the psychological violence situation by asking about the personal data breach, how it is treated in the event of a personal data breach and how it is felt.

In this study, descriptive statistics were used to present data and Google forms was used as a tool. The questions have been prepared within the scope of demographics, internet usage habits, personal data sharing, personal data breaches, and the effects of these actions on the people whose data have been breached.

4.1. Participant Profile

As the study group, 50 people over the age of 18 from Turkey were reached. 28 of these people are men and 22 are women. While 56% of the participants in the conducted field study are female, 44% are male; the average age of the participants over the age of 18 is 27.

5. FINDINGS

With the developing technology, people's Internet usage is increasing in parallel. The field study also supports this situation, while 50% (25 participants) of the participants spend 5 hours or more on the Internet a day, only 2% (10 participants) of the participants spend less than 1 hour. It has been determined that all of the participants have a social media account. It is observed that 33 of the participants who have social media accounts have closed their profiles, while the profiles of 17 people are open to everyone.

In this context, it can be said that the frequency of participants' use of the Internet and digital platforms is quite high.

54% of participants (27 participant) answered "I will share if it is mandatory for me to enter the site" when asked if they would share information such as Turkish identity number and phone number that are required on the website.

Figure 1. Mandatory Information

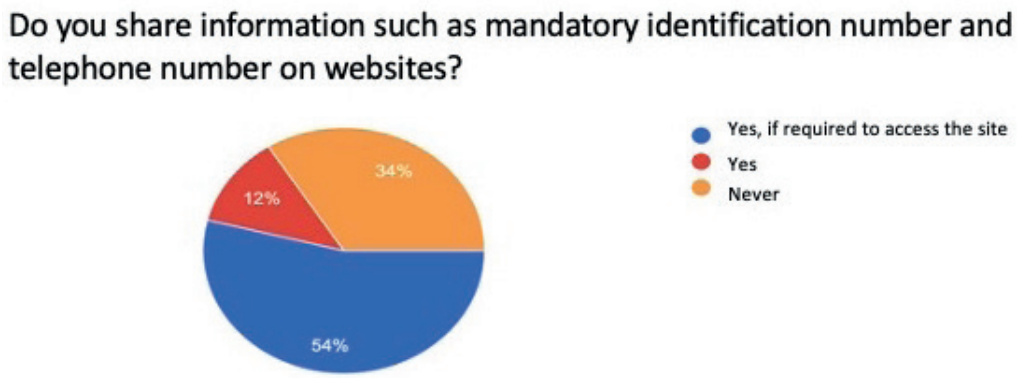
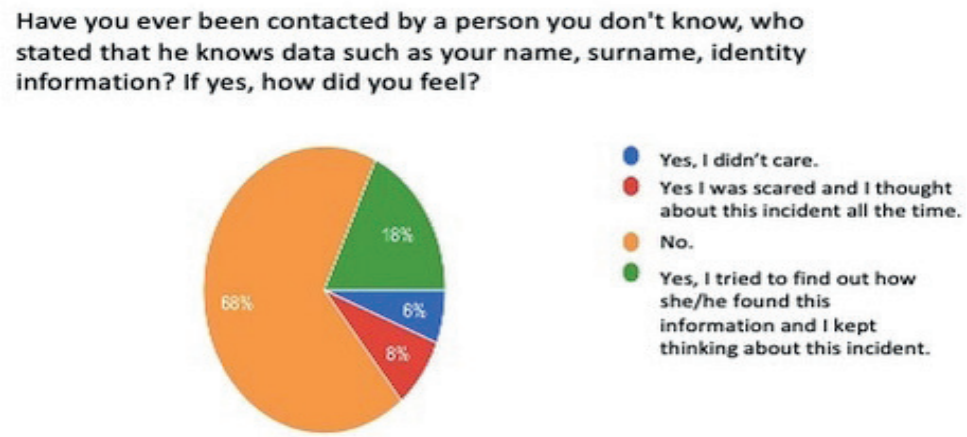


Figure 2. Personal Data Breach And Its Effects



Only 12% (6 participants) of participants said they never share the required information on websites. It can be concluded that individuals share their personal information willingly or unwillingly to access digital platforms. This shows a situation of being forced as a result of need.

When the participants were asked whether they had been contacted before by people who stated that they knew your personal data but did not know them and how they felt, it was found that 56% (28 participants) of those who said yes experienced a psychologically intense impact on the violation of their personal data. The answers given, together with comments written at the end of the survey are evaluated when individuals are noticing that their personal data has been breached as a result of anxiety, and tension, and the situation is constantly thinking in the form of effects observed.

More than 50% of the participants were called by people they did not know by giving their numbers to others, and as a result of this situation, they were worried, tense and constantly thought about this situation.

The issue of creating fake accounts, which is seen as an increase in the use of social media accounts, is a problem that comes up frequently as a view of the violation of personal data such as names, surnames, and photographs. 76% of the participants (38 participants) did not open a fake account on their behalf. While this number is low in the participant profile, it is a positive situation that only 1.9% of those who have fake accounts opened did not care about this situation, while the rest were both nervous and tense and constantly worried about who this person was.

Perhaps the most sensitive point for people is sharing their own photos, correspondence, audio, and video with others without their consent. When the participants were asked whether the screenshot of a photograph or correspondence they did not want before was forwarded to someone else via the internet/message; 50% of those who answered yes have encountered this situation once and 50% of them have encountered this situation many times.

Out of 21 people who answered yes, 5 people stated that they were nervous, 9 people said that

Figure 3. Personal Data Breach And Its Effects

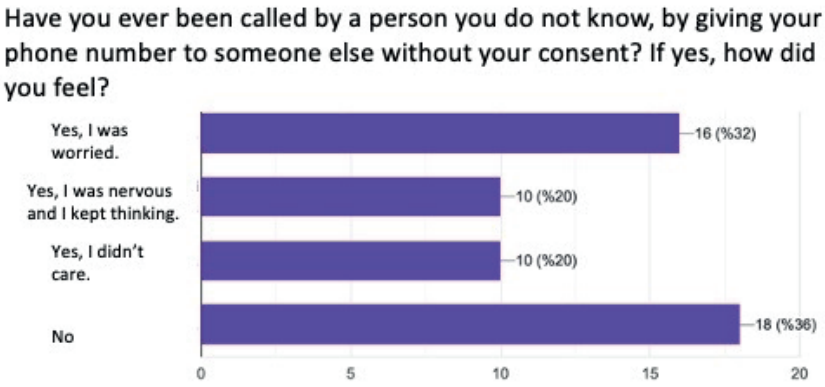
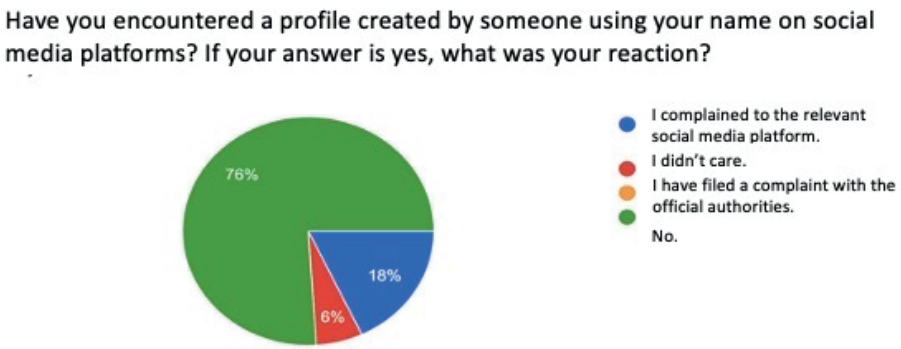


Figure 4. Fake Account



the thought that everyone could see this tired them, and 7 people said that they were ashamed and did not know what to do which reduced their communication with people.

Considering that most of the participants have social media accounts, it is important to determine the risk of hijacking the passwords of the social media account. The password of the social media account of 34% of the participants (17 participants) was compromised. Of the people whose passwords were compromised, more than 50% of the accounts complained/had them registered.

23.4% opened a new account and informed the people around them that the other one did not belong to them, 11.7% applied to the official authorities, and the rest did nothing. As can be seen, the number of applications to official authorities is quite small, which may indicate a lack of faith in justice, as well as a low level of awareness. Without the knowledge of the participants, 8 people from those whose audio/video recordings were transmitted to other people/platforms became restless and constantly thought about this situation.

7 people felt helpless, and 7 people were worried and thought about who they saw.

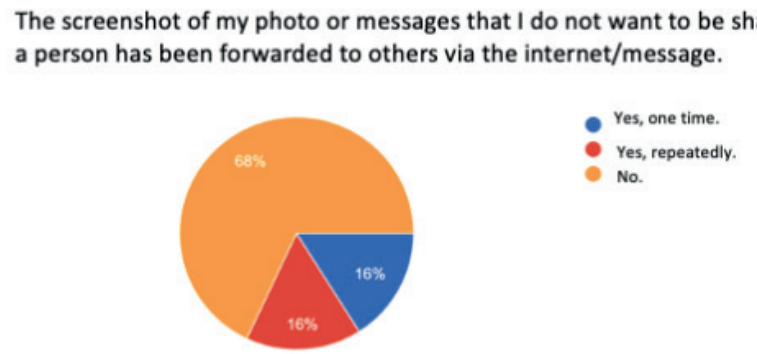
Among the participants, 69% of those whose passwords were seized were uneasy and constantly checked their accounts. On the other hand, 23% of them thought that they were a person who did not love themselves and were tense. 6% questioned the reason for this action.

Nowadays, fraud acts that we are frequently faced with can also be considered as a violation of personal data by means of capturing people's information through cyber environments. More than 50% of the participants have previously tried to make transactions by calling someone they think is a fraudster on behalf of banks/telecommunications companies, asking for their information. And most of those who said yes were nervous and nervous.

The participants were asked "how did you feel if your personal data was used without permission? What was this process like for you? in the evaluation of the open-ended questions asked

Figure 5. Using A Fake Account And Its Effects On People

Figure 6. Sharing Unwanted Photo/Correspondence



in the form of "; It has been determined that this process is an unsettling, worrying and frightening process for the participants, containing restlessness. At the same time, some of the respondents consider the security measures to be quite inadequate.

The following responses were given by the participants; "disturbing", "I've been too worried and scared"," It was a very worrying and frightening process."," I think that the security measures are quite inadequate and the studies on this subject are also quite inadequate. If we think in terms of access to the applications to be developed, I believe that the cost does not allow this."," It was a tiring and extremely stressful period when I was nervous."," I got worried and cut off my involvement with social media. But banks, telecommunications etc. I couldn't resolve my concerns about it.", "I'm sad, I'm depressed","I felt insecure I was always on the alert","Being disturbed is bad.","It was a process full of restlessness and anxiety, I felt like everyone was watching my private life.","I didn't know what to do,

Figure 7. Sharing Unwanted Photo/Correspondence

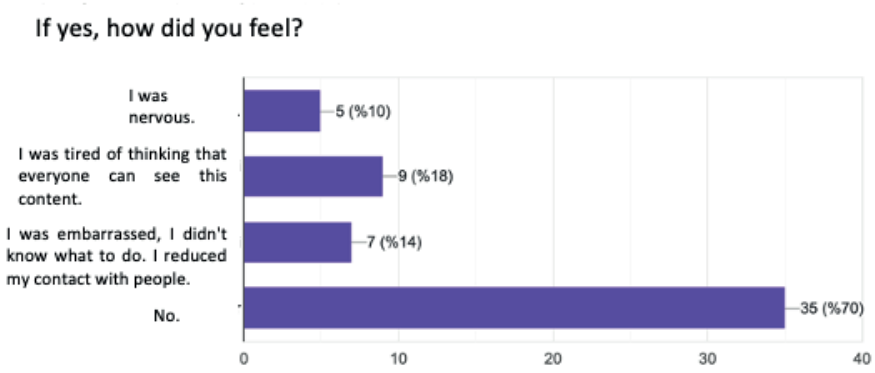


Figure 8. Hacking Social Media Password

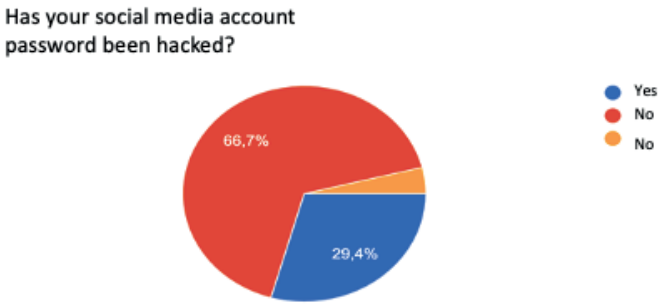


Figure 9. Reactions As A Result Of The Seizure Of The Social Media Password

I said delete it but I'm still not sure if it's deleted I'm paranoid","It still has its effects I don't trust anyone","Tiring", "You constantly feel tense, anxious, restless. It's like you have a bomb with the pin in your hand and you're waiting in anticipation when it will explode.", "I don't like it, but it has become an unavoidable reality that we have to accept in the new age."

As part of the fieldwork, the participants were asked "Is there an event you would like to share with us?" was asked as an open-ended question. It was observed that the participants mostly stated that their personal data, which is unknown how they were accessed, was seized by others, this situation made them nervous and they constantly thought about these events, they did not feel safe in their daily lives, they did not trust security measures, and sometimes they did not care because justice was not provided anyway. In this context, it can be said that as a result of the violation of the personal data of the participants, their daily lives were affected and they had uneasy and restless periods.

6. DISCUSSION

The violation of personal data, which is strengthened by the privacy and confidentiality of private life, can sometimes have destructive consequences on the person. Personal data is referred to as any information that defines the person and makes them "who they are". In the research, the participants were asked questions that did not use the concept of "personal data" but rather questions about their personal information, photos, and conversations. The belief was that clearer and more specific information could be obtained by having the participants respond within the scope of "violation of their own information". In this context, as detailed above, personal data encompasses a wide range and includes phone number, correspondence, photos, password, and ID number provided by the participants (Yuksel, 2016).

As technology advances, the use of the internet, smartphones, and social media platforms has increased. According to the household information technology use research, the internet usage

Figure 10. Effects As A Result Of Social Media

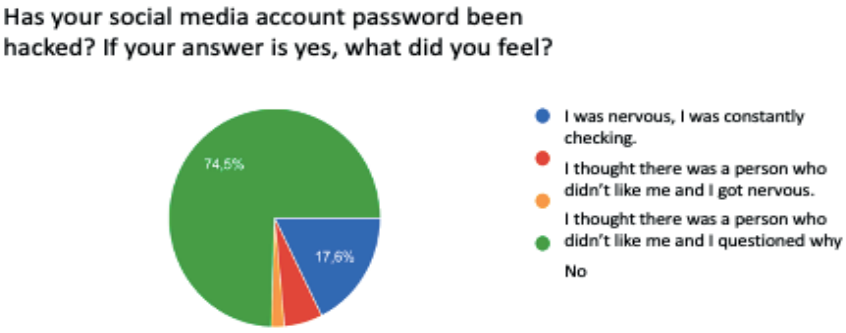
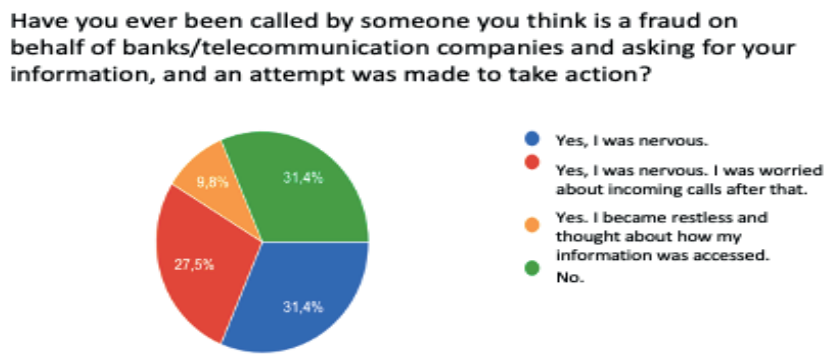


Figure 11. Fraud In The Virtual Environment



rate among individuals aged 16-74 was 82.6% in 2021 and 85.0% in 2022. (Household Information Technology Use Research, 2022) Supporting this result, all of the participants use the internet and 50% spend over 5 hours a day on the internet while only 2% spend less than an hour. These rates can indicate a suitable environment for experiencing online risks. Technology facilitates human life and contributes positively to social development as a measure of progress and modernization, but also brings some problems and dangers caused by the unconscious use of the internet (Bolisik and Muslu, 2019).

The participants have social media accounts and 33 participant of them have their profiles set to private while 17 participants have their profiles set to public. 54% of the participants (27 participants) responded that they would share information such as their national ID or phone number if it is required to access the site, while 12% (6 participants) answered yes. In this context, it can be seen that the participants have higher awareness of their social media accounts, but they are not hesitant to share personal information if necessary. Basically, when digital platforms offer them options, they act according to the concept of "me and privacy", but when it comes to mandatory information sharing, the "access to the platform" is given more importance. This result is supported by many studies which show that individuals can easily share their personal information without reading the conditions, especially in situations where they think they will benefit from it (for example, when registering on a website to access necessary information) (Eroglu, 2018).

The results show that over 50% of the participants reported that their phone numbers were called by unknown individuals, which led to feelings of concern, stress, and constantly thinking about the situation. This suggests that the participants felt like they were being monitored and not secure. This highlights the participants' privacy concerns. Previous research has shown that the belief that personal information is not under the individual's control increases privacy concerns (Dinev and Hart, 2005; Ridley-Siegert, 2015; Klein, 2004; Eroglu, 2018). This concern is also evident among the participants, as they experience feelings of anxiety, fear, and constant thinking.

Considering that all participants use social media, it is highly likely that the social media account will be compromised by third parties. Because, the opening of social media by others on their behalf and the seizure of accounts by third parties as a view of the violation of personal data such as first name, last name, photo is a problem that is frequently raised. However, contrary to what was expected, 76% of the participants (38 participants) did not have a fake account opened by someone else in their name. While this ratio reflects a positive result, only 1.9% of those who opened fake accounts by third parties did not care about this situation, while the rest were both nervous, nervous and restless, constantly thinking about who this person is. These rates in the study lead to the conclusion that most of the participants are psychologically affected by opening an account on their behalf. In addition, the password of the social media accounts of 34% of the participants was compromised. Of the people whose passwords were compromised, more than 50% of the accounts complained/had them registered.

23.4% of them opened a new account and informed the people around them that the other one did not belong to them, 11.7% applied to official authorities. It was found that the majority of the participants reacted against the seizure of their passwords by third parties, but there was very little recourse to official authorities. This situation shows that awareness is low in terms of the legal process.

Photos, correspondence, audio and videos of people are the most well-known examples of privacy and private life. In the Declaration on Mass Media and Human Rights No. 428 of 1970 published by the Council of Europe, "The right to privacy of private life actually includes the right of a person to continue his life with minimal interference. Privacy, family and home life, physical and moral integrity, honour and dignity of the person, to prevent misidentification, irrelevant facts, and the disclosure of embarrassing private photos were not published without

permission, private communication to protect against the abuse of the use of secret prevent disclosure of information that is given or received within that scope takes place." defined by their statements (Duman, 2012). The feelings and reactions of the participants in the face of the disclosure of their private lives by sharing their photos and writings; stretching has been identified as reducing communication with people by tiring of the thought that everyone can see it, being embarrassed and not knowing what to do. Only 2% of the participants stated that they did not feel anything. This rate is quite low and shows that people are psychologically affected repeatedly as a result of the violation of their own and private life data.

In recent years, the number of frauds through technological tools has increased. In the study carried out by Tekkanat et al., it was concluded that 94% of the fraudsters were successful through phone fraud and that fraudulent activities were parallel to the same speed with the emerging technologies (Tekkanat etc., 2018) Another dimension of the breach of personal data by people close to them or people they do not know is "internet fraud". In this context, in addition to the data breach that endangers only the privacy and private lives of the people, data breaches that can interfere with the economic situation of the people are also investigated. Among the findings in the study; More than 50% of the participants were exposed to fraud in the digital environment. Findings such as anxiety, anxiety, uneasiness, constant thinking, and hesitation in subsequent calls were observed in people who were victims of fraud. When these data are compared with the other results in the study, it has been determined that the participants' personal data has been violated most by fraudulent method.

Finally, in the open-ended questions asked to the participants, it is concluded that the violation of their personal data leads them to feel insecure, to lead an anxious and anxious life, to constantly think about these events.

In the literature, in similar studies that are often conducted; acts of violation of personal data are referred to as one of the acts of "cyber violence" (Patchin and Hinduja, 2006; Ozkaya, 2023; Cengiz, 2021; Seckin and Selcuk, 2023;). Similarly, the Council of Europe has addressed cyber violence in six separate subheadings and expressed the violation of privacy through the use of information and communication technologies as a type of cyber violence(Council of Europe, 2018).

When cyber violence is briefly defined as violent acts carried out through technological means, we support the examination of acts of violation of personal data in the literature under the category of cyber violence, while at the same time we argue that this act can also be considered as an act of psychological violence. Because; As mentioned before, the types of violence are the types that give birth to each other and intertwine with each other. Symptoms seen in the victim person as a result of cyber violence actions; often there is sadness, fear, shame, helplessness, feeling worthless, frustration, intense stress, anxiety, depression, post-traumatic stress disorder, etc. their findings (Beran and Li, 2005; Patchin and Hinduja, 2006). In addition; According to Dilmac; individuals explain that they do not feel safe in the virtual world and are afraid of losing control of personal data (Dilmaç,2020). In our study, which supports this, it has been concluded that the people whose personal data have been violated are afraid, worried and nervous. In this context, psychological violence and cyber violence are quite similar to each other in terms of their consequences.

When the problems related to the definition of psychological violence are examined, first of all, it is necessary to determine which of the large categories (such as control, emotional violence, verbal violence) constitute psychological violence or to be included in the definition of psychological violence, and which of the different types of psychological violence are independent factors from each other, It is also a priority problem to determine whether it is perceived as harmful or not (Boyacioglu etc., 2020). In this context, psychological violence is a type of violence whose definition expands and evolves over time, and it is an undeniable fact that the increase in psychological violence acts in the virtual environment with the development of technology. When psychological violence is defined as acts that do not

involve physical violence against a person in general terms, disrupting the mental and spiritual balance of the person with words or actions, and when considered together with the intensity of the emotions and thoughts felt as a result of the acts of violating the personal data of the participants, these acts can also be considered as an act of psychological violence. can be said to be acceptable. In this context; In the study, it was seen that people whose personal data were violated experienced intense psychological effects.

7. CONCLUSION AND SOLUTION SUGGESTIONS

It has been determined that all of the participants have social media accounts in terms of the environment suitable for the violation of personal data in digital environments and that some of the participants are using their accounts publicly. 50% of the participants spend 5 hours or more on the Internet. Only 2% of the participants spend less than 1 hour on the Internet. The vast majority of participants share their data without thinking if it is necessary for access to Internet sites. While this situation shows that the level of awareness is low, it shows that data sharing as a condition of service is carried out too much, even though it is illegal. People prefer to meet their needs more in the balance between Decency and data security. In this context, it can be determined that there is not much awareness of the protection of personal data.

About 50% of the participants have been subjected to a data breach at least once and in this case have experienced anxiety, restlessness, and constant thinking. It has been determined that the application rate to official authorities is quite low. When the violation of personal data is also considered within the scope of private life and privacy, it has been observed that signs of psychological violence have been detected in the victim. It is possible to say that along with psychological violence, there are also indicators of cyber violence. Because types of violence can sometimes manifest themselves intertwined with each other.

Therefore, actions taken with the instinct of emotionally wearing out and psychologically harming the person in the cyber environment can be considered as the online appearance of psychological violence.

Since personal data breach acts in digital environments are carried out in the cyber environment, sometimes it is considered as an act of cyber violence, but it can also be an online appearance of psychological violence. In light of all these data, in order to produce a solution to this global problem consciously and effectively use digital platforms to protect shared data-conscious users who are aware of what needs to be done to increase the number of, if supported by the implementation of sanctions and the legal regulations on this subject, literally, to ensure the security of data, or will help to minimize the problems. In addition to media literacy, the necessity of raising personal data literacy in the digital environment and awareness of the training to be given from a young age are important concepts that need to be brought to consciousness. Dos and don'ts on different platforms for the protection of personal data, general information will be given with regard to data security, training, of all ages, from PDPL for users, private sector, civil society organizations, the written and visual media, universities, and in cooperation with the school at every level should be provided. Because personal data breaches can have a great impact on people financially and spiritually, and sometimes they can lead to psychological trauma by using them as a means of violent acts.

REFERENCES

ABINIK, N. (2021). Bir Psikolog Gözünden Siber Şiddet [online] Retrieved from https://dijitalsiddet.org/bir-psikolog-gozunden-siber-siddet/ [Date of Access: 20/11/2022]

AÏMEUR, E., GAMBS, S. & HO, A. (2010). Towards a privacy-enhanced social networking site. 2010 International Conference on Availability, Reliability and Security. 172-179. Retrieved From: https://www.academia.edu/54544136/Towards_a_Privacy_Enhanced_Social_Networking_Site

AKGUL, A. (2016). *Danıştay ve Avrupa İnsan Hakları*

Mahkemesi Kararları Işığında Kişisel Verilerin Korunması. İstanbul: BETA, İkinci Basım, ISBN: 9786053336471.

ATALAY, A. Ö. (2019). Ceza Muhakemesi Hukukunda Moleküler Genetik İncelemelerin Özel Nitelikli Kişisel Verilerin Korunması Açısından Değerlendirilmesi . *Journal of Penal Law and Criminology* , 7 (2) , 127-184.

BELSEY, B. (2007). Cyberbullying: A real and growing threat. *ATA Magazine*, 88(1), 14-21.

BERAN, T. , LI, Q. (2005). Cyber-Harassment: A Study of a New Method for an Old Behavior. *Journal of Educational Computing Research*. 32(3), 265-277.

BOLIŞIK, B. , MUSLU, K. G. (2009). Çocuk ve gençlerde İnternet kullanımı. *TAF Prev Med Bull*, 8(5), 445-450.

BOYD, D. M., ELLISON, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.

BOZKURT, YÜKSEL A. E. (2016) *Bulut Bilişimde Kişisel Verilerin Korunması*, Ankara: Yetkin. ISBN: 978-605-05-0114-8

Cybercrime Convention Committee, "Mapping Study on Cyberviolence," Council of Europe, July 9, 2018, https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c.

CENGİZ, G. (2021). Siber Suçlar, Sosyal Medya ve Siber Etik. *İletişim Çalışmaları Dergisi.* 7(3), 407-424.

COBUTOĞLU, S. (2020). Latife Tekin'in "Manves City" Adli Romaninda Toplumsal Cinsiyet Ve Kadina Yönelik Duygusal Şiddet. *Yeni Türk Edebiyatı: Hakemli Altı Aylık İnceleme Dergisi*, 0(22), 79 - 102.

DİLMAÇ, J.A. (2020). Dijital Ortamda Sapkınlık: Siber Zorbalık. *Turkish Studies-Social Sciences.* 15(3). 1087-1099.

DİNEV, T. & HART, P. (2005). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10(2), 7-29.

DUMAN, B. (2012). *Adiye Basın Sözcülüğü*. Türkiye Barolar Birliği Dergisi, (101), 293-316

DULGER, M. V. (2018). İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması* . İ*stanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* , 5 (1) , 71-144.

DULGER, M. V. (2020). *Kişisel Verilerin Korunması Hukuku.* İstanbul : Hukuk Akademisi, Third Edition, ISBN: 9786058101524.

EROĞLU, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi . *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi* , 35 (2) , 130-153.

İZGİ, M.C. (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri. *Türkiye Biyoetik Dergisi*. 1(1), 25-37.

KARA, Z. & ULUÇ, M. A. (2019). Şiddetin Cinsiyeti: Bir Modern Toplum Anksiyetesi. *Şarkiyat*, 11(3), 1566-1581.

KARAGULLE, A.E. (2015). Günümüzde Değişen Mahremiyetalgisinin Sosyal Ağlar Bağlaminda İncelenmesi. Tez (Yüksek Lisans).İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Medya ve İletişim Sistemleri Ana Bilim Dalı.

KAYA, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi . *Journal of Istanbul University Law Faculty* , 69 (1-2) , 317-334 .

KILINÇ, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi.* 61 (3), 1089-1172.

KOLBURAN, G., (2021). Duygusal İstismar Tanım ve Kavramsal Çerçeve. *Adli Psikoloji Bakış Açısıyla Duygusal İstismar.* Eds: G. Kolburan. 31-47. Ankara: Seçkin, Second Edition, ISBN: 978-975-02-7323-0.

KORKMAZ, A. (2016). Siber Zorbalik: Fizikselden Sanala Yeni Şiddet. *E-Kurgu Anadolu Üniversitesi İletişim Bilimleri Fakültesi Uluslararası Hakemli Dergisi* (*Online Journal of the Faculty of Communication Sciences)*.24 (2), 74-85.

KUTLU, Ö. & KAHRAMAN, S.(2017). Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi* 5(4), 45-62.

KLEIN, S., (2004). The privacy debate: this time it's personal. The Guardian Newspaper.

OĞUZ, S. (2018). Kişisel Verilerin Korunmasi Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*. 13 (2),121-138.

ORBAY, İ. (2022). Görünmeyene Işık Tutmak: Psikolojik Şiddet. *Journal of Society & Social Work*. 33(1), 267-290.

ÖZERKMEN, N. & GÖLBAŞI, H.(2010) Toplumsal Bir Olgu Olarak Şiddet.*Akademik Araştırma ve Dayanışma Derneği.* 15,23-37.

ÖZKAYA, P. (2023). Dijital Dünyada Çevrimiçi Riskler, Bilişim Suçlari Ve Mağdur Çocuk. Türkiye Adalet Akademisi Dergisi. (53) , 13-42.

ÖZKAN, O. (2020). *Kişisel Verilerin Korunması*. Tez (Yüksek Lisans). Ankara Üniversitesi Sosyal Bilimler

Enstitüsü Özel Hukuk Anabilim Dalı.

PATCHIN, J. W. & HINDUJA, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 148–169.

PELTEKOGLU, F. B. & TOZLU, E. (2017). Medya Yansımaları Ekseninde Kadına Şiddet Sorunsalı ve Halkla İlişkiler . *Marmara İletişim Dergisi* , (28) , 1-19 .

POLAT, O. (2016). *Adli Psikolojiye Giriş*. Ankara: Seçkin, First Edition, ISBN: 9789750240706.

POLAT, O. (2017). Şiddet. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*.22(1),15-34.

RİDLEY-SİEGERT, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice,* 17, 30-35.

SEÇGİN, L. & TARI SELÇUK, K. (2023). Sanal Ağların Distopyası: Kadına Yönelik Dijital Şiddet. *Dünya İnsan Bilimleri Dergisi* , 2023 (1) , 203-217.

SÜSLÜ, D. P. (2016). *Lise Öğrencilerinde Siber Zorbalık ve Siber Mağduriyetin Benlik Saygısı Anne, Baba ve Akran İlişkileri Açısından İncelenmesi.* Tez(Doktora). Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü.

ŞAHİN, S. & TÜRK, M. (2010). Çalışanlarda Psikolojik Şiddet Algılaması ve Kadın Çalışanlar Üzerine Bir Araştırma. *Çukurova Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*.14 (2), 1-9 .

TEKKANAT, E., TOPALOĞLU, M. & YILMAZ, O. (2018). Bilişim Suçları ve Psikolojik Etkileri Açısından Türkiye'de Telefon Dolandırıcılığının Etkin Analizi. *Journal of Ege Education Technologies*. 2(2), 44-54.

TURKISH PERSONAL DATA PROTECTION LAW no. 6698.

TUTAR, H. (2004). İşyerinde Psikolojik Şiddet Sarmalı: Nedenleri ve Sonuçları . *Yönetim Bilimleri Dergisi.* 2 (2) , 85-108 .

YALIN, B., ONBAS, K. & KARAOGLU, S. (2018). Psychological Violence In Social Media: "Sharing" Culture As Pressure, Exploitation, Threat. *The Journal of Academic Social Science Studies International Journal of Social Science.* 73, 281-297.

YÜCEDAĞ, N., (2019).Kişisel Verilerin Korunması Kanunu Kapsamında Genel Ilkeler. *Kişisel Verileri Koruma Dergisi*. 1(1), 47-63.

WORLD HEALTH ORGANIZATION. (2002). World Report on Violence and Health. Geneva: WHO. Retrieved From: https://apps.who.int/iris/bitstream/handle/10665/42495/9241545615_eng.pdf