HOW TO FIGHT DIGITAL GENDER-BASED VIOLENCE: A GUIDE

Extended 2nd Edition











Authors:

Gülüm Şener İlden Dirini Nurcihan Temur Şebnem Ahi Şevket Uyanık Zeynep Özarslan

Translation: Sevda Akyüz, Ahu Sıla Bayer

Design: Fatih Akdoğan

December, 2022

The guide is copyrighted by the writers themselves. All content is CC AttributionNonCommercial 4.0 Unported License.



Contents

1. WHAT IS DIGITAL GENDER-BASED VIOLENCE?		
Defining Characteristics	6	
Online Violence: Continuation of Offline Violence	6	
Digital Violence? Cyber Violence? Virtual Violence? Or Online Violence?		
Who's Exposed to Digital Violence?		
Intersectional Discrimination and Digital Violence That Affect Different Demographic Statuse		
Who are The Perpetrators of Digital Violence?	8	
2. DIGITAL SECURITY TIPS	9	
Digital Footprint	9	
Internet Safety	10	
Connection Security	10	
Device Security	11	
Password Security	11	
Social Media Security	12	
E-Mail Security	13	
Secure Messaging	13	
Search Engine Security	14	
Website Security	14	
Deleting Metadata	14	
Open Source	14	
3. TACTICS AGAINST DIGITAL HARASSMENT	15	
4. LEGAL ASPECTS OF DIGITAL VIOLENCE IN TURKEY	17	
5. GLOSSARY OF DIGITAL VIOLENCE	28	
REFERENCES	33	



1. WHAT IS DIGITAL

GENDER-BASED VIOLENCE?

As internet access increased, the widespread use of mobile information and social media brought on digital violence, which is a new form of gender based violence.

Women actively using social media and internet platforms encounter threats and comments directly targeting their gender, sexual identity and personal security.

Violence against women of all ages, ranging from women to girls, is considered a violation of human rights and a type of sexist discrimination. In the Istanbul Convention,¹ violence is defined not only in physical, but also sexual, psychological and economic forms, and as a consequence of gender-based inequality.

Gender-based violence includes domestic violence, spouse violence, violence witnessed during dating, and digital violence.

Digital gender-based violence is not categorized under any type of violence. What is being suggested hereby is its being classified as a new type or form of violence, as it contains cases that overlap with all other types of violence.

Digital violence based on gender violence may be defined as the violence which takes place on digital media, which is directed towards us due to our gender-based identitites, influencing our lives us at an unproportional extent.

¹ Istanbul Convention, E. (2011). Council of Europe Convention on preventing and combating violence against women and domestic violence. Violence against women and domestic violence. https://rm.coe.int/1680462545

Defining Characteristics

In the study titled "Voices from digital spaces: technology related violence against women," five defining characteristics of digital violence against women have been listed:

- Anonymity: The perpetrator may not be known by the victim.
- **Action Distance:** The abuse may be directed from any distance without physical contact.
- **Automation:** The online abusive acts or cyber bullying require less time and effort.
- Accessibility: The technological variety and economic feasibility render women as easy prey for perpetrators.
- **Distribution and Continuity:** Texts and photos copied on the internet can spread without limits or can stay there for a long time.



Online Violence: Continuation Of Offline Violence

Women are subjected to different forms of violence in real life (offline life) due to gender-based inequalities. Those same inequalities target and threaten the security of women in cyberspace (online life) in different demographic statuses.

It must not be forgotten that digital violence is not a separate concept from violence in 'offline' life; and that it is a continuation of offline violence (domestic violence, violence against women) fed by the same inequalities.

The gender stereotypes that involve inequality and sexism in offline environment are also valid in online environment.



Digital Violence? Cyber Violence? Virtual Violence? Or Online Violence?

When the relevant studies and reports are examined, it can be seen that the digital violence women are subjected to is not entirely conceptualized. We encounter this subject under different headings: cyber violence, virtual violence, digital violence or online violence.

As the number of studies on the subject increases, concepts will be formulated more precisely, but it is vital that the definitions are evaluated with a feminist perspective. Different organisations may prefer to use different terms for these similar or closely related concepts. As scholarly literature grows on gender-based digital violence, it is likely to reach a consensus on these concepts.

² Fascendini, F., & Fialová, K. (2011). Voices from digital spaces: Technology related violence against women. Association for Progressive Communications (APC)

Who's Exposed To Digital Violence?



Gender-based violence as a result of online abuse may target both men and women. Similarly, children can also be subjected to online abuse and violence. However, due to the fact that online abuse and gender-based violence stems from the same structural inequalities and sexual discrimination as the other types of violence, the rate of violence women are subjected to is higher.³

According to the data in the UN report titled "Cyber Violence Against Women and Girls – a Worldwide Wake up Call," the probability of women's exposure to violence all over the world is 27 times higher than that of men. Just like any area, the internet is also a domain where gender-based violence is seen.

According to the 'Türkiye'de Dijital Şiddet Araştırması'⁵ (Research on Digital Violence in Turkey), carried out by Toplumsal Bilgi ve İletişim Derneği (Social Information and Communication Foundation) in cooperation with KONDA,

- One in five persons in Turkey is subjected to digital violence.
- The majority of the digital violence victims are made up of young ones. Teenagers between 15-17 years of age are subjected to digital violence in a rate of one fifth, whereas this figure is one of three young people between the ages of 18-32. The former group is exposed to violence due to their physical appearance and ages, while the latter is subject of digital violence because of their political views and pyhsical looks.
- Women express to have become subjects of digital violence due to their gender (52%) and their physical looks (21%); while men report that they are exposed to digital violence to a greater extent due to their political views (30%). One in 10 women in Turkey are victims of this type of violence exhibited by their narratives or family members.
- 51% of women in general receive harassing messages on digital platforms, in the form of texts, voice or Video messages. 46% of women are being stalked by perpetrators.
- The digital platforms where violence is mostly observed are Instagram, Facebook and Twitter, with figures of 53%, 35% and 19% respectively.
- Digital media users usually report having been abused and shown digital violence by followers they do not know and trawlers.
- When the types of digital violence are observed in detail, the majority of examples are made up of verbal insults, use of bad language, threats, abusive messages and stalking.
- The principal methods used to fight digital violence are blocking/restricting the users (65%) or reporting within the application (39%).

³ IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women.

⁴ UN. (2015). Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call. http://www.unwomen. org/-/media/headquarters/attachments/sections/library/ publications/2015/cyber_violence_gender%20report. pdf?vs=4259

⁵ TBİD. (2021). Türkiye'de Dijital Şiddet Araştırması. https://dijitalsiddet.org/dijital-siddet-raporu/

Intersectional Discrimination And Digital Violence That Affect Different Demographic Statuses Of Women

Women can be exposed to cyber bullying based on their education, age, ethnic background, sexual orientation or relationship status.

In the report titled "Gender based Violence and Online Abuse," it is concluded as a finding that women who are more visible in online and offline environments can be exposed to abuse to a greater extent in online platforms. LBTQ+ women, female journalists (including blog writers), women active in tech industries, female public figures (artists, writers, and so on), female politicians, female academics, and feminist activists can be openly targeted from time to time by the perpetrators of digital violence.

Who Are The Perpetrators Of Digital Violence?

The perpetrators of digital violence can be ex- or current spouses/partners, neighbours, work/school friends, relatives or strangers.

The perpetrators of digital violence use information and communication technologies, such as social media, messaging apps, Global Positioning System (GPS)-based apps, smart phones and/ or e-mail, with the purpose of causing anxiety in their victims about their personal security. The perpetrators are generally committed to gaining and maintaning control, and technology is only one of the tools they use to make this possible.⁷

Most online abuse and gender-based violence is committed via anonymous or fake name accounts, which makes it hard to track down the perpetrators.



⁶ ibid.

⁷ UN Women (2020).Toplumsal Cinsiyete Dayalı Siber Şiddet Rehberi, https://2020.atesbocekleri.info/



2. DIGITAL SECURITY TIPS

The examples of software and applications referred to in this section have been added to this guide after their currency and reliability have been checked. The reader is strongly advised to revisit the websites hereby mentioned, and check to see if the information is still up to date.

Even though it is not possible to talk about a 100% security on the Internet, users can still establish more secure communication. Internet users can improve their new media literacy and use the right methods and tools to ensure digital security at different levels.

Digital Footprint



Every move and click of internet users are recorded for later use; and personal information turn into lucrative data for corporations. We leave a lot of digital footprints with our online activities on a daily basis.

Today, anyone can get a lot of information about you by a simple Google search. They don't need to be a **hacker** to do that. Your voluntary shares on social media reveal your daily routines, private information, personality, mood, and social life to others. People or groups with malicious intent can harm you by collecting this data.

Internet Safety



- On a browser you open in **Incognito mode**, you can search the web to find out about your personal information, analyze the results, and detect **what kind of information is public about you**.
- Clear your browser **history** and **cookies** in your devices often. If you do not work in your own devices, use 'Incognito mode.'
- You may restrict your followers or those who see your shares on social media by changing your customized choices by clicking 'preferences'. You may also interfere with third party applications accordingly.
- You can also request platforms like Google, Facebook, Instagram, and Twitter to share the information they gathered on you and download them to your computer. This way, you can see and archive your activities so far using these accounts. However, this will not delete your data from the internet.

To download your Google data:

https://takeout.google.com/

To download your Facebook data:

https://www.facebook.com/help/212802592074644

To download your Twitter data:

https://help.twitter.com/tr/managing-your-account/how-to-download-your-twitter-archive

To download your Instagram data:

https://www.instagram.com/download/request

To download your Linkedin data:

https://www.linkedin.com/psettings/member-data



Connection Security

- Do not use your personal password or do online shopping on computers in public places like internet cafes, photocopiers or stationery stores to get print outs or send email. If you access your email or social media accounts on unknown devices, do not forget to **log out** when you are done.
- Your passwords and personal data can be hacked over public access WIFI. Try not to use such connections.

Device Security



- Always use **passwords** and **screen locks** in your devices (computer, tablet, smart phone, etc.) to prevent access by others. The data in your digital devices belong to you and unauthorized people should not ask for your passwords or use your devices and check the information on them.
- In a healthy relationship, people do not feel the need to restrict and check up on each other. If your partner expects you to send your location, take and send photos from everywhere you go, and answer every message instantly, this is an indication that he is stalking you.



Password Security

- Your passwords for internet platforms and digital devices should not be simple or easily predictable. They should not contain names, birthdates, ID numbers, wedding anniversaries, phone numbers, etc.
- In your passwords, try not to use your personal information that can be predicted by people in your life. Your partner, spouse, friend, etc. may find out what your password is and use it to check up on your online communication with others. Your password is personal, and no one has the right to know it.
- Prefer passwords that are not coherent wholes, and that contain numbers, upper and lower case letters, as well as signs. For example: N/1i2*H3-a4!X8
- Set different passwords for all the services, websites, social media platforms. Don't use the same password for a variety of sites because if it is hacked, it can be tried in other platforms as well.
- Renew your password at least every six months.
- Your answers to the security questions when setting your password should not be 'real.' For
 example, if you choose the name of your first pet as your security question, you should not
 give the real name of your pet as it can be easily guessed by others. Similarly, it can also be
 predicted through the information you share on social media.
- As it is difficult to remember all these passwords, you can use two open source and free software programs to store and manage them: keepassx.org and encryptr.org. For IOS and Android cell phones, you can use the apps you may achieve from keepass.info, bitwarden.com, strongboxsafe.com and http://keepassium.com. With the help of these programs, you can safely keep all your passwords using one main password.
- Make sure to use the two-step verification system. You can protect your accounts on social
 media platforms like Facebook, Twitter, Instagram by using this two-step verification. In this
 system, if someone tries to access your account from a different device, you get a warning
 message. So, if you activated the two-step verification, they cannot access your account even if
 they know your password. You can activate this system in the Settings/Security Settings sections

of your social media and email accounts. In order to protect your Google/Gmail account, you can set up **Authenticator** and use this two-step system.



Social Media Security

- You can check who gets to see your information other than the social media platforms you shared them with if you read the User Agreement carefully and in detail. The user agreements that we usually approve without reading may contain articles stating that our data is shared with corporations.
- You can check and restrict who you want to share your social media profile and posts in the **Privacy Settings/Security Settings** sections. To do that, just visit these sections in your social media platforms and manage the settings in detail.
- If you activate **Timeline Approval** and **Tag Approval** features on Facebook, your approval will be asked when your friends or acquaintances want to tag you in a post or share something on your timeline.
- When you receive irritating messages/posts, you can use the **Report** feature offered by social media platforms, **block the perpetrator** of digital violence, and get their account to be closed.
- You can also report discriminatory, sexist comments or hate speech posts directed at others on social media platforms to contribute to the fight against digital violence.
- You can get help from Facebook's support center about private images shared without consent: https://www.facebook.com/safety/notwithoutmyconsent
- If you are targeted and subjected to humiliating, insulting and discrediting messages by people
 or groups known or unknown to you on social media, you can get a screenshot, gather evidence,
 and start the legal process. Make sure that the name of the sender, as well as the date and time
 of the post appear on the screenshot. You can ask for legal support from the bar associations;
 get information from civil society organizations and centers working on gender and women's
 rights.
- You will see many applications that you do not use in all social media platforms (Twitter, Facebook, Instagram, Linkedin, Youtube, etc.). These are tasked with reading and writing messages or texting on your behalf. Make sure to remove the unused ones.
- Social media facilitates stalking between people and may feed their obssessions. The
 perpetrators may track your activities, get information about you and your location to gain
 control over you on social media unless you block them. If you feel threatened, you can block
 the perpetrator and delete them from all means of communication. You can create a safe
 communication environment with "zero communication."
- The perpetrators may try to befriend your friends on social media to track your activities. In that
 case, you can inform your friends, and ask them not to share any information related to you, and
 to support you.

- If you suspect you are being followed, **avoid sharing your location** as much as possible. Regularly clean your location history on your devices.
- In a trusting relationship, your partner wouldn't interfere with what you share on social media or who you befriend. Your social media profile is personal; and you should be in charge of its content.
- You can visit the links below for security suggestions against digital harassment/online violence on social media platforms:

Google:

https://learndigital.withgoogle.com/dijitalatolye/course/online-safety/module/3000

Facebook:

https://www.facebook.com/safety/bullying

Twitter:

https://help.twitter.com/tr/safety-and-security/cyber-bullying-and-online-abuse

Linkedin:

https://www.linkedin.com/help/linkedin/answer/43796/taciz-veya-guvenlik-endisesi?lang=tr

Youtube:

https://www.youtube.com/intl/tr/about/policies/#community-guidelines



E-Mail Security

- Do not click on generic private messages or email claiming you won something, from a sender whose origin you do not know. They may be carrying a virus and aiming at stealing your personal information.
- You can encode and safely send your email messages via software like **PGP** (**Pretty Good Privacy**), **TutaNota.de**, **ProtonMail**.
- You can have an alternative e-mail address from **RiseUp** etc, form e-mail groups and get more secure communication service.



Secure Messaging

• You can use **Signal** as a more secure alternative to messaging apps like Whatsapp and Telegram. Signal offers end-to-end encoded messages for your short texts as well as clearing your chats from all servers after having been read, and two-step confirmation.



Search Engine Security

• You may want to prefer an alternative search engine to Google like **DuckDuckGo**, which is not commercial, and does not track or sell your personal information.





- You should prefer websites starting with the more secure **https://** instead of **http://** website addresses.
- You can add the extensions **HTTPS Everywhere** and **PrivacyBadger** on your web browser, produced by Electronic Frontier Foundation. This way, you can stay away from commercials and cookies and have a more secure communication.
- You can verify the security of a link sent to you by a friend or unknown user by consulting websites such as **phishtank.com** or **urlex.org** before clicking on them.



Deleting Metadata

- Make sure to turn off the geotag feature on your mobile phone when you take photos or shoot videos.
- You may also use apps for your mobile phones such as Simple Gallery and the like (https://simplemobiletools.com/)



Open Source

- Try to choose open source apps or programs in order to decrease corporation monitoring because many closed source apps ask to access your private data in your devices. Open source free apps do not ask for such permissions, and they do not store your personal data for commercial purposes.
- You can download **F Droid** in Google Play for Android phones and find the open source equivalents for the apps you are currently using.



3. TACTICS AGAINST

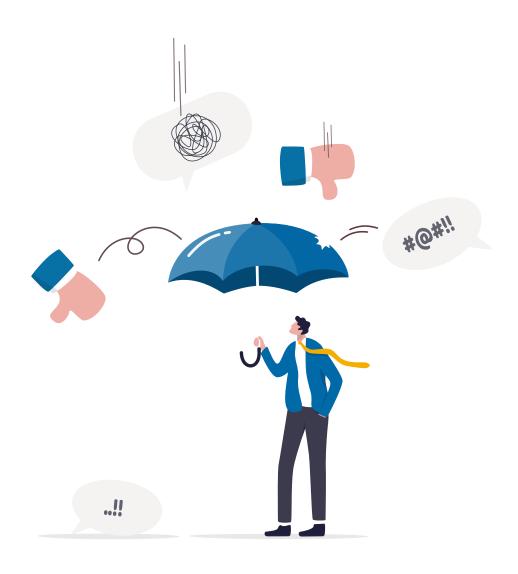
DIGITAL HARASSMENT

Perpetrators of digital violence are usually very determined to stay in control; and technology is one of many tools they use to do just that. If the perpetrator seems to know a lot about you, he/she may be collecting this information by tracking your devices, accessing your online accounts, monitoring your location or collecting online data about you.

Becoming an online target may make you feel as if things are getting out of control. There are, however, protective measures you can take without blaming yourself. Here are some of them:

- Gather data to identify the perpetrator and document what happened. Documenting a series
 of events may demonstrate to the police or the court that there is a pattern of stalking or
 harassment. The documents can also help you see an increase in activity and plan your security
 accordingly.
- Get a screenshot. Screenshots are very fundamental and useful tools to store information you gather on the internet.
- You can report the irritating online behavior to the website or app it happened on. If the behavior
 is in violation of the service terms of the platform, that content can be removed or the person
 can be banned. It is important to know that the report content can be totally removed; therefore,
 evidence should be documented before reporting.
- You may want to reveal the perpetrator on Twitter and other social media accounts. #tacizvar #tacizesesver #sendeanlat #susmabitsin
- Share your experience with people you trust, get support from a women's consultation center.

- Consult lawyers specializing in this area to learn about the legal processes. Talk to Women's Consultancy Centers of the Bar Organizations.
- You can file a complaint with the nearest police precinct or the prosecutor's office. Also, if
 urgent intervention is required, you should demand a restraint order regulated in Act 6284. It is
 also possible to file a lawsuit for punitive damages.
- You can demand that the content be removed according to Act 5651. If the related content is
 not considered critical, and if it is not based on a real decision, the person who does not want to
 be associated with this content can still demand its removal as part of their right to be ignored.
 If the right conditions for legal counselling have emerged, a lawyer can be demanded.
- In any case, it is vital for the victim to know their rights in the eyes of the law and raise their awareness about the legal process as well as knowing what constitutes a crime.
- You can complain about acts of lynching, sexist rhetoric, and digital violence against other people, too. This way, you can help the accounts of the perpetrators get terminated.
- You can organize online and offline campaigns to raise awareness about the fight against gender-based digital violence; create an agenda; and engage in digital activism to get both internet companies and politicians to come up with solutions.





4. LEGAL ASPECTS OF DIGITAL VIOLENCE IN TURKEY

Digital Violence Action	Under the scope of which crime/law	What are the possible sanctions?
Persistent tracking: Sending messages or calling continuously, forcing to report location or send photos. Insisting on establishing communication even though he/she states that he/she does not want or respond.	Deterioration of peace and order of people Turkish Penal Code Article 123 Calling another person insistently or making noise with the intention of deteriorating peace and order or executing any other unlawful act for this purpose.	Upon the complaint of the victim, the perpetrator is sentenced to imprisonment from three months to one year.
Disclosure of private correspondence and images	Violation of Communicational Secrecy Turkish Penal Code Article 132	
	Violation of secrecy of communication between persons.	- One to three years of imprisonment
	Secrecy is violated by by recording contents of communication between persons	- The sentence is increased by one half.
	Unlawful disclosure of contents of communication between himself and others without obtaining their consent.	- Two to five years of imprisonment
	Unlawful and public disclosure of the content of communication with himself without obtaining the consent of the other party	- One to three years of imprisonment
	Disclosure of data through press and broadcast	- One to three years of imprisonment
	Tapping and recording of conversations between individuals Turkish Penal Code Article 133	- Two to five years of imprisonment
	Any non-general conversations between the individuals listened to through a device without obtaining the consent of any of the parties or recording these conversations by use of a recorder	- Six months to two years of imprisonment or punitive fine

	Recording a conversation not open to public with a recorder without the consent of the participants Disclosing unlawfully the data obtained by recording conversations not open to public between persons Disclosure of data through press and broadcast Other crimes such as violation of privacy and violation of personal data may occur at the same time.	 Two to five years of imprisonment and punitive fine up to four thousand days Two to five years of imprisonment and punitive fine up to four thousand days
Cyber exploitation / Sexual blackmail: Shooting intimate images of a person and threatening by sharing them and/or sharing them with others on the Internet, social networks or private messaging	Violation of Privacy Turkish Penal Code Article 134 Violating secrecy of private life Privacy violation by use of audio-visual recording Unlawful disclosure of images or sounds of one's private life Disclosure of data through press and broadcast Disclosure of personal data is also possible.	 Imprisonment from one to three years The penalty to be imposed is increased by one half Two to five years of imprisonment Two to five years of imprisonment
	Threat – Turkish Penal Code Article 106 Threatening another person by saying that he intents to kill himself or one of his relatives, or to violate corporal or sexual immunity of others Threatening by causing a great property loss or other misconduct	 Six months to two years of imprisonment Up to six months of imprisonment or punitive fine

Threatening; a) with a gun, b) by unsigned letter or use of special signs concealing one's identity, c) by more than one person, d) by taking advantage of the terror actions of existing or potential organized groups,

- Two to five years of imprisonment

In case of commission of defense by threat resulting from felonious homicide, felonious injury or damage to property - Additional punishment from these offenses.

If threatening statements are directed to a person through social media, the same crime will be considered as committed. Together with the offense of insult and in connection with the same action, this crime is also committed.

Defamation Turkish Penal Code Article 125

Any person who attacks with the intention to harm the honor, reputation or dignity of another person through concrete performance or giving impression of intent

In order to punish the offense committed in absentia of the victim, the act should be committed in presence of at least three persons.

The commission of offense in writing or by use of audio and visual means directed to the aggrieved party.

In case of commission of offense with defamatory intent a) against a public officer b) due to disclosure, change or attempt to spread religious, political, social and philosophical belief, opinions and convictions and to obey the orders and the restriction of one's religion; c) by mentioning sacred values in view of the religion with which a person is connected,

- Three months to two years of imprisonment or punitive fine

- Three months to two years of imprisonment or punitive fine
- The minimum limit of the punishment to be imposed may not be less than a year.

Open Defamation In case of public officers The punishment to be working as a committee to imposed is increased by one perform a duty, then the sixth. offence is considered to have committed against the members forming the committee. In this case, the provisions of the article relating to successive offense applies. Sexual harassment Cyber Harassment: Sending Article 105 a person messages and/ or messages or images with sexual content without his/her If a person is subject to sexual - Three months to two years harassment by another person consent of imprisonment or punitive - Commission of the offense - Six months to three years of against a child imprisonment - a) by taking advantage of the - The punishment to be convenience of public office or imposed according to the service relationship or family above paragraph is increased relationship; by one half. b) by persons who offer services as guardian, educator, instructor, caregiver, foster family or healthcare or persons with the obligation of protection, care and supervision c) benefiting from the convenience of working in the same workplace, d) benefiting from the convenience offered by post or electronic communication tools, e) by exposure - The punishment to be imposed may not be less than The victim is obliged to leave a year. the business place, school or house for this reason

Privacy violation: Retrieving the person's e-mail and/or social media passwords and accessing their accounts, checking the information on their devices without permission

Recording of personal data Turkish Penal Code Article 135

Recording of personal data unlawfully

Recording the political, philosophical or religious concepts of individuals, or recording unlawfully personal information relating to their sexual origins, ethical tendencies, health conditions or connections with syndicates

- One to three years of imprisonment

- The punishment to be imposed in accordance with the first paragraph shall be increased by half.

Giving or acquiring data unlawfully Turkish Penal Code Article 136

Giving, disseminating or acquiring personal data unlawfully

The subject of the offense shall be the statements and images recorded in accordance with paragraphs 236 / 5-6 of the Turkish Penal Code

- Two to four years of imprisonment
- The punishment to be imposed is increased by one half.

Qualified forms of offense Turkish Penal Code Article 137

In case of commission of the offenses defined in above articles; a) by a public officer or due influence based on public office, b) by exploiting the advantages of a performed profession and art,

Destruction of data Turkish Penal Code Article 138

Failure to fulfill the duties of those responsible for destroying the data within the system despite the expiry of the legally prescribed period

If the subject of the offense is data that need to be eliminated or destroyed according to the provisions of the Code of Criminal Procedure.

- The punishment to be imposed is increased by one half.

- One to two years of imprisonment
- The punishment to be imposed is increased by one half.

Accessing the data processing system Turkish Penal Code Article 243

Accessing a part or whole of the data processing system and remaining there unlawfully

Committing the abovementioned offenses which involve systems which are benefited against charge

Deletion or alteration of data within the content of the system due to this offense

Monitoring illegally the data transmissions that occur in an information system itself or between the information systems without entering the system by means of technical tools

Hindrance or destruction of the system, deletion or alteration of data Turkish Penal Code Article 244

Hindering or destroying operation of a data processing system

Garbling, deleting, changing or preventing access to data, or installing data in the system or sending available data to other places

Committing these offenses on the data processing systems of a bank or credit institution or a public institution or corporation

Execution of the abovementioned acts not constituting any other offense apart from unjust benefit secured by a person for himself or others

- Up to one year of imprisonment or punitive fine
- The punishment to be imposed is increased up by one half.
- Six months to two years of imprisonment
- One to three years of imprisonment

- One to five years of imprisonment
- Six months to three years of imprisonment
- The punishment to be imposed is increased by one half.
- Two to six years of imprisonment and up to five thousand days of punitive fine

Improper Use of Bank or Credit Cards Turkish Penal Code Article 245

Any person who acquires or holds bank or credit cards of another person(s) whatever the reason is, or uses these cards without consent of the card holder or the receiver of the card, or secures benefit for himself or third parties by allowing use of the same by others

- Three to six years of imprisonment and up to five thousand days of punitive fine

Producing, selling, transferring, purchasing or accepting counterfeit bank or credit cards by linking them with the bank accounts of others

- Three to seven years of imprisonment and up to ten thousand of punitive fine

Any person who secures benefit for himself or others by using a counterfeit or falsified bank or credit card (unless the act constitutes an offense that requires a more severe punishment) -Four to eight years of imprisonment and up to five thousand years of punitive fine

If the offense in the first paragraph is committed to the detriment of

- No punishment is imposed on the relative

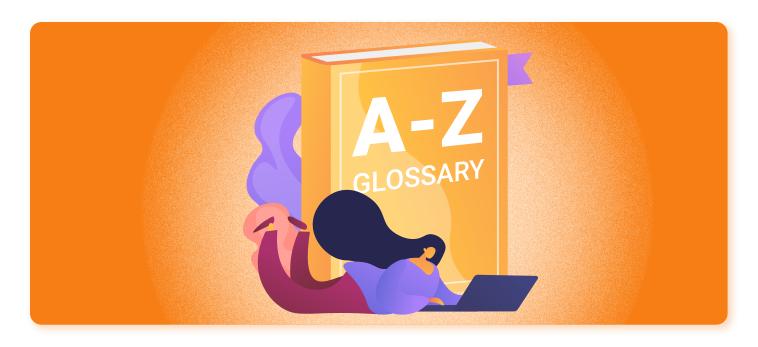
- a) one of the spouses whose separation decision has not been made,
- b) lineal kinship or one of such a brother-in-law or adopted,
- c) one of the siblings living together in the same dwelling.

The effective remorse provisions relating to crimes against the assets of this Law shall apply to the acts falling within the scope of the first paragraph.

Opening fake accounts on Unlawful delivery or acquisition The punishments are the internet on behalf of the of data explained above. person and sharing posts Turkish Penal Code Article 136 In addition, through these accounts, the insult crime may occur, or secrecy of private life may be violated. Or a person's memory may be insulted. Such an offense may also be committed against legal persons. Defamation Turkish Penal Code Hate speech: Sharing The punishments are described above. humiliating, insulting, sexist Article 125 messages on the Internet, social media, digital games, Determination of the aggrieved messaging applications, party Turkish Penal Code Article targeting people and exposing 126 them to virtual lynch Even if the name of the Regulated by Article 126 of the Turkish Penal Code, targeting aggrieved party is not clearly a person or a member of indicated or the accusation is a group through media or implicitly expressed, both the through conventional means name of the aggrieved party of media is a criminal offense and the act of defamation is assumed to have been declared provided that there is clear indication of defamation of a person's character based on the quality of the offense. Provoking people to be rancorous and hostile Article 216/2 - Six months to one year of Any person who openly provokes a group of people imprisonment belonging to different social class, religion, race, sect, or coming from another origin, to be rancorous or hostile against another group - Six months to one year of Openly disrespecting the religious belief of group. imprisonment (If this act is conducive to disrupt public peace)

Doxxing: To collect detailed information about the person on the internet and to disseminate and use this information to cause harm to the person.	Unlawful delivery or acquisition of data Turkish Penal Code Article 136	The punishments are explained above.
Defamation: Sharing posts in a way that damages a person's commercial reputation, revealing trade secrets	Compensation for violation of personal rights Civil Code Article 24 Turkish Commercial Code Article 56 Unfair Competition	The compensation provisions specified in the relevant laws shall apply.
	Infringement of trademark right, Provisions of the Law No. 6769	Compensation and penal provisions specified in the relevant law shall apply.
	Provisions of the Law Number 5651	Blocking access and removing content.
Checking: Checking a person's social media posts, trying to limit social media communication	Prevention of communication Turkish Penal Code Article 124	
	Unlawful prevention of communication among persons	- Six months to two years of imprisonment or punitive fine
	Unlawful prevention of communication among the public institutions	- One to five years of imprisonment
	Unlawful prevention of broadcasts or announcements of all kinds of press and publication organs.	- Punishable according to paragraph two.
	In addition, violation of constitutional rights such as freedom of expression, the right to receive information and the right to information could also be possible.	The relevant penal provisions and compensation provisions of the Turkish Penal Code and other laws shall apply according to the relevant act.

Threat / Blackmail: Using digital means to threaten and blackmail with death, sexual assault and physical violence	Threat Turkish Penal Code Article 106 Blackmail Turkish Penal Code Article 107 Any person who forces a person to perform an act contrary to the law; or to execute or not to execute a duty beyond his responsibility; or to derive unjust benefit from a thing by declaring his will to perform or not to perform an obligation which he is entitled to do so Threatening to reveal or charge with issues that may harm the dignity or prestige of a person to derive benefit for himself or others	 Punishment is explained above. One year to three years of imprisonment and up to five thousand days of punitive fine Punishable according to paragraph one.
Disclosure of personal data: disclosing personal data of persons	Recording personal data Unlawful delivery or acquisition of data Turkish Penal Code Articles 135, 136, 137, 138 Law No. 6698 for the Protection of Personal Data ARTICLE 18. Misdemeanors Failure to comply with the obligations of disclosure and data security.	- Punishment is explained above. - Punitive fine of up to 5000 to 1,000,000 Turkish Lira



5. GLOSSARY OF DIGITAL VIOLENCE

Body Shaming:

Making negative remarks about a person's body, making fun of one's appearance; offending, scorning, demeaning a person due to their bodily features. Body shaming is practiced both online and offline. It may target a person's height, weight, certain parts of their body (Schlüter, Kraag and Schmidt, 2021, p. 8).

Catfishing:

Imitating another person's online identity in order to act like that particular person on digital platforms. The perpetrator opens a new account by using another person's social media images and information and acts like them on social media. The fictional identity aims at damaging this person's prestige and social status and forming relationships that would harm them (Cybersmile. org)

Character Assassination:

Reputation assassination is spreading faulty news and rumours about a person or group with the aim of making them lose reputation and credibility. In today's world social media channels are often used for assassinating people's reputation.

Creepshot:

Shooting women's photos or images without their consent and publishing them unbeknown (European Women Lobby).

Cyber Bullying:

Exhibition of hostile behavior in an intentional and repetitive manner by a person or group, aiming at harming other people by taking advantage of electronic communication technologies, under

the disguise of preparing questionnaires, sending mobile phone messages, e-mails or instant messages. (Küçük, İnanıcı and Ziyalar, 2017). Having widened its scope with digital communication media, cyber bullying may be defined as a wider version of peer violence among children and teens, and includes: use of bad language, insults, threatening messages, reading others' emails without their consent, theft of passwords, sending demeaning messages, sending of insulting images of a person on the net without their consent (Baker and Kavşut, 2017).

Cyber Flashing:

The perpetrator's sending their own inappropriate images (usually of the genitals), abruptly in public spaces via end-to-end wi-fi channels such as Bluetooth, Airdrop, etc. Cyber flashing include sexual images sent through digital channels without consent, and is a form of "sexual abuse backed up by technology ". Sexual abuse backed up by technology, including cyber flashing, may restrict "women's safety and security in public places" (Freeman, 2020).

Cyber-Mob Attack:

A high number of abusers' collective assault onto one specific target individual, with threats, insults, and abusive tactics (PEN).

Deadnaming:

Naming an individual by their dead name (assigned at birth) despite the individual's decision to be called by another name they chose on their own. In other words, deadnaming is calling a person by his/her ex-name after they began to use a new name by having made an amendment via official means. This type of violence is especially resorted against LGBTIQ+ individuals who, for a variety of reasons, rejected the name assigned at birth (Women Media Center). Deadnaming may be both intentional or accidental, and aims at making a person's identity invalid, or misgendering this individual (Lieurance et al., 2022, pp.341-342).

Deep Fake Porn:

The production and spread of a person's fake images by the use of artificial intelligence technologies without their consent.

Digital Sex Trafficking:

Carrying out acts of smuggling, prostitution and sexual trade. Perpetrator(s) make use of the global and anonymous quality of the internet; gain information on the ones they target and force them to become sex workers. (European Women Lobby).

Doxing:

Having access to and spreading personal data belonging to a particular person on the internet. Personal data may include home address, e-mail, telephone numbers, identity, images, etc. The term "doxing" derives from hacker culture, originally meaning, "accessing the files" (Anderson and Wood, 2021, p.205). Doxing generally aims at harming the targeted individual. Doxing usually appears in connection to other types of online abuse, and leads to a person is being targeted both in online and offline platforms (Eckert and Metzger-Riftkin, 2020, p.1).

Gasligthing:

Gaslighting may be defined as an effort to make another person doubt themselves, by manupilating their opinions and psychological well-being. Gaslighting is a type of emotional abuse causing a person to question their own feelings, memories of specific events, and perception of reality (Porter and Standing, 2020). Either unintentionally or on purpose, the agent who resorts to gaslighting tries to make the other party feel that the reality they perceived, events they recall and/or what they believe in are wrong. The gaslighting agent may go so far in as much that s/he blames the other person for having lost their minds (Abramson, 2014, p. 2). Gaslighting may take place in any relationship (romance, family, friendship, business, etc.), on both face to face and online platforms.

Ghosting:

Cutting the communication with a person that one is regularly in contact with, in an abrupt manner with no explanation. In ghosting incidents, one of the partners in a relationship begins to stop answering text messages, calls, etc. with no explanation. 'Ghosting' includes instances when the perpetrator leaves the other party in pure silence in a punishing manner, totally disappears, blocks the other person on social media platforms or ignores the other person's efforts to maintain contact. (Navarro et.al, 2020, cit. Biolcati et al. 2021, Pancani et al. 2021).

Love Bombing:

Love bombing may be defined as the perpetrator's expression of over attention and over affection towards the other party usually at the beginning of a romantic relationship. The perpetrator in such a relationship is insistent on being continuously in contact, and is eager to communicate with his/her partner throughout the day via texts, e-mails, mobile phone or social media. Love bombing is a type of abuse. The perpetrator who exhibits narcissistic behavior may seem unproblematic at first, but may tun into a pain in the neck as time goes by. The narcissistic perpetrator, either intentionally or unintentionally, tries to make sure s/he is holding the center stage in the other person's life (Strutzenberg, 2016). Buying expensive gifts, trying to spend time unceasingly, overdose compliments, uneasiness about the other party's setting up limits may be signs of love bombing. The person who is subjected to such treatment may become addicted to the relationship and may find it difficult to give up.

Multi-Platform Abuse:

The perpetrators' targeting the individual(s) not only via a single digital platform but a series of platforms in coordination. In other words, multi-platform abuse means individual(s)' being subjected to digital violence via e.g. Twitter, Facebook, e-mailing, or Instagram at the same time. This type of abuse includes threats, insults or other types of contact via social media accounts, e-mail accounts, blogs, online/offline business communities or telephone (Matias et al., 2015, p.19). Multi-platform abuse makes use of the fact that each digital platform needs to control their own safety measures, therefore leaving the victim at a more difficult position (Women Media Center).

Online Economic Violence:

Economic violence has taken new forms due to the advance of digital media. The perpetrator may make use of digital media with the purpose of putting up economic pressure on the victim. Methods such as theft of identity, the blockage of access to online accounts, manipulation of credit information are all under the title of online economic violence (Women Media Center).

⁸ In EIGE text, the term cyber abuse is being used; however, due to the use of online abuse in addition to cyber abuse, both terms have been used in this study.

Online Grooming:

Online "grooming" is a form of sexual abuse aiming at children on digital media platforms. It is carried out through perpetrator's attempt to have sexual intercourse with a child or to abuse the child sexually. The perpetrator pretends to be a child or adolescent/teenager on the sites frequented by children, gains their trust, and then asks for the child's personal and intimate data (such as images with sexual content) to further blackmail the child later on (ChildSafeNet). According to Gunawan et al. online grooming is made up of 6 stages: 1- Making friends: The perpetrator gets the child's personal information at this stage. 2- Forming bonds: The perpetrator and the child begin to communicate about the school the child is going to, their hobbies and interests, and the perpetrator makes the child believe that they have formed a bonding relationship. 3- Risk assessment: The perpetrator asks the child to be alone while in contact and avoid making others see the messages they exchange. 4- Making it special: The perpetrator has now gained full trust of the child and abused their love and attention. 5- Sexual contact: At this stage, both sides begin to exchange messages on sexual activity and sexual phantasies. 6- Final stage: At this final stage, the perpetrator has persuaded the child for face-to-face contact. The frequency in which these stages occur, their order and content may change from one case to another. (Gunawan et al., 2016, p.1).

Online Hate Speech:

Using a hateful discourse on online platforms, scorning, threatening and targeting others (based on their race, ethnic community, gender, sexual tendencies, age and disability, etc.) The hate speech already existing on offline platforms have become more prevalent especially with the use of social media, which made it easier for perpetrators to resort to hate crime and violence acts targeting certain groups. Although it is not directly accepted as hate crime, expressions that constitute hate discourse, both before and after a certain crime is committed, would eventually serve as strong evidence to prove the presence of 'motivational bias'" (İnceoğlu, 2012, p. 107). When viewed from the perspective of motivational bias, being involved in hate discourse is a crime (Özarslan and Yıldız, 2021).

Online Stalking:

Online stalking may be defined as following a specific person insistently and peering at their life systematically by use of e-mailing, texting, social media apps, apps indicating geographical locations and their digital footprints. Stalking weakens the party subjected to this sort of violence due to the recurrence of events - whether they are directly or indirectly harmful to the subject- and brings them to a state of anxiety, fear, even alarm. Online insistent following is sometimes referred to as 'stalking (secretly peering)'. The follower in this case may be named as a 'stalker'. Cyber stalking, is a term used to define certain behaviors that causes an individual to feel frightened or doubtful regarding their safety, through online communication channels, mounting up to recurrent threats and/or harassment.

Online/Cyber Abuse:

Online or cyber abuse may be defined as contacting a person against their own will or forcing them to be contacted despite their lack of consent to do so. Online abuse may be in the form of a variety of ways: e-mails with unwanted sexual content, online texting or sending of texts; inappropriate or aggressive acts taking place in social websites or chat rooms; threatening others to use physical or sexual violence via e-mails, texts or online messages; use of hateful language/discourse scorning, insulting, threatening behavior shown towards an individual targeting their identities (gender) or other features (such as sexual preferences or disability) (EIGE)⁸.

Revenge Porn (Cyber Exploitation):

Online spread of a person's photos, images and/or videos including sexual content without their consent. In addition, this type of digital violence also includes threatening that person by spreading their images online. The perpetrator is usually an ex-partner or spouse who reached access to images and videos of sexual content during their relationship, and makes use of these images either to end the relationship or to take revenge for any kind of grudge, by making the other party feel intimidated and insulted. That being said, the perpetrators may neither always be ex partners or spouses whom a person had previous relationship with, nor the act is always a revengeful one. The images may have been achieved by hacking the person's social media accounts, mobile phone or PC, and may aim at damaging their life in 'offline world'.

Sexting:

Sending another person various messages, photos, images and voice mails with sexual content. "Sexting" initially used to mean sending messages including sexual content via texting; however, in today's world, its scope has been widened due to widespread images and videos being shared (Van Ouytsel et al., 2019). When it is practiced without the other party's consent or permission, sexting is categorized as digital violence (stopcybersexisme.com).

Sextortion:

The perpetrator's threatening and/or blackmailing the targeted individual with nude or sex images in order to get him/her do what they want.

Slut-Shaming:

Naming/labeling women and girls with adjectives such as "slut", and/or criticizing their sexual acts or sexual behavior, no matter if that particular behavior is real or assumed to be so by the perpetrators. Perpetrator(s) label(s) women and girls on the grounds that they do not obey sexual norms (Karaian, 2014). Widespread use of sexual media has led to a higher number of incidents in which users are bitterly "sealed as sluts". The roots of this type of violence are the double-standards imposed by men onto women and girls; since women are punished for the same type of behaviors that men are rewarded and praised for (Van Royen vd., 2018). Women who exhibit behaviors outside the box of conventional gender roles attributed to women by the society are labeled as "slut" or other similar adjectives. This labeling is observed on media and social media platforms.

Upskirting:

Shooting and spreading of others' photos or videos via mobile phones or cameras, aiming at their bodily parts below their skirts. The perpetrator(s) may occasionally shoot upskirt images of women in public spaces, toilets, during opendoor activities or on the street.

Victim Blaming:

In any kind of violence practiced against a victim, putting the blame on the very person subjected to the violence for a variety of reasons, thus freeing the perpetrator from being the agent of the crime (Cinsel Şiddetle Mücadele Derneği). On the internet, especially on social media, victim blaming is prevalent. For instance, when a woman is sexually attacked, the social media users may practice incidents of victim blaming when commenting on the issue on social media.

REFERENCES

Abramson, K. (2014). Turning up the lights on gaslighting. Philosophical Perspectives, 28(1), 1–30. doi:10.1111/phpe.12046

Anderson, B. ve Wood, M. (2021). Doxxing: A scoping review and typology. The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 205–226. doi:10.1108/978-1-83982-848-520211015

Avrupa Kadın Lobisi (2017). #KadınınHakkıKadınınİnterneti. https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf Erişim tarihi: 08.04.2022.

Biolcati, R., Pupi, V. ve Mancini, G. (2021). Cyber dating abuse and ghosting behaviors: personality and gender roles in romantic relationships. Current Issues in Personality Psychology. doi:10.5114/cipp.2021.108289.

ChildSafeNet(2022). Cyber Grooming. https://www.childsafenet.org/new-page-15. Erişim tarihi: 10.04.2022.

Cinsel Şiddetle Mücadele Derneği (2019). Kavramlar Sözlüğü. cinselsiddetlemucadele.org. Erişim tarihi: 03.04.2022

Cybersmile (2021). Catfishing. https://www.cybersmile.org/what-we-do/advice-help/catfishing Erişim tarihi: 10.04.2022.

Eckert, S. ve Metzger-Riftkin, J.(2020). Doxing. The International Encyclopedia of Gender, Media, and Communication. (ed.) K.Ross, I. Bachmann, V. Cardo, S. Moorti ve M. Scarcelli. John Wiley & Sons, Inc. DOI: 10.1002/9781119429128.iegmc009

EIGE. (2017). Cyber Violence Against Women and Girls. http://eige.europa.eu/rdc/ 6 eige-publications/cyber-violence-against-women-and-girls Erişim tarihi: 03.04.2022

Erdur-Baker, O. ve Kavşut, F. (2007). Akran Zorbalığının Yeni Yüzü: Siber Zorbalık Cyber Bullying: A New Face of Peer Bullying. Eurasian Journal of Educational Research, 27, s.31-42.

Freeman, V. (2020) "Cyber Flashing: Unwanted and Non-Consensual Lewd Photographs as Technology Enhanced Sexual Harassment". Student Works. 1090. https://scholarship.shu.edu/student_scholarship/1090

Gunawan, F.E. vd. (2016). Detecting online child grooming conversation. 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS). Yogyakarta, Endonezya.

İnceoğlu, A. A. (2012). Nefret Suçu Kavramı ve Türk Ceza Mevzuatı Açısından Değerlendirilmesi, Nefret Söylemi ve/veya Nefret Suçları içinde (s.103-120), Yasemin İnceoğlu (Der.) İstanbul: Ayrıntı Yayınları.

Karaian, L. (2014). Policing "sexting": Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. Theoretical Criminology. 18, 282–299. doi:10.1177/1362480613504331

Van Ouytsel, J., Walrave, M., Ponnet, K. and Temple, J.R. (2018). Sexting. In The International Encyclopedia of Media Literacy (eds R. Hobbs and P. Mihailidis). https://doi.org/10.1002/9781118978238.ieml0219

Küçük S, İnanıcı, M. A, Ziyalar, N. (2017). Siber Zorbalık Ölçeği Türkçe Uyarlaması. Adli Tıp Bülteni, 22(3), 172 - 176.

Leitão R. (2019). Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. Human—Computer Interaction, DOI: 10.1080/07370024.2019.1685883

Lieurance, D et. al. (2022). Words matter: how to increase gender and LGBTQIA + inclusivity at Biological Invasions. Biol Invasions 24, 341–344. https://doi.org/10.1007/s10530-021-02665-7

Matias, J. N., Johnson, A., Boesel, W. E., Keegan, B., Friedman, J.,ve DeTar, C. (2015). Reporting, Reviewing, and Responding to Harassment on Twitter. Women, Action, and the Media. May 13, 2015. http://womenactionmedia.org/twitter-report

Özarslan, Z. ve Yıldız, F. (2021). Nefret söylemi araştırmalarında yöntem üzerine bir analiz. Proceedings of the 18th International Symposium Communication in the Millenium, 26-27 Ekim 2021.603-616. Pdf file, E-Book. ISBN: 978-625-7960-45-8.

PEN(2022). Online Harassment Field Manual.

https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/ Erişim tarihi: 03.04. 2022

Pancani L, Mazzoni D, Aureli N, Riva P.(2021). Ghosting and orbiting: An analysis of victims' experiences. Journal of Social and Personal Relationships.;38(7):1987-2007. doi:10.1177/02654075211000417

Porter, J. ve Standing K. (2020) Love Island and Relationship Education. Frontiers in Sociology, 4 (79). doi: 10.3389/fsoc.2019.00079

Stop Cyber Sexisme (2022). Sexting. https://www.stop-cybersexisme.com/le-dico-ducybersexisme. Erişim tarihi: 03.04.2022

Schlüter, C., Kraag, G. ve Schmidt, J. (2021). Body Shaming: an Exploratory Study on its Definition and Classification. International Journal of Bullying Prevention https://doi.org/10.1007/s42380-021-00109-3

Strutzenberg, Claire, "Love-Bombing: A Narcissistic Approach to Relationship Formation" (2016). Human Development, Family Sciences and Rural Sociology Undergraduate Honors Theses. 1.http://scholarworks.uark.edu/hdfsrsuht/1

Van Royen K., Poels K., Vandebosch H., Walrave M. (2018) Slut-Shaming 2.0. In: Walrave M., Van Ouytsel J., Ponnet K., Temple J. (eds) Sexting. Palgrave Studies in Cyberpsychology. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-71882-8_6

Women Media Center. https://womensmediacenter.com/speech-project/online-abuse-101#crossPlatformHarassment Erişim tarihi: 03.04.2022







görüşlerini yansıtmamaktadır."