# DIGITAL LAW AND DIGITAL HYGIENE

Javlon Zoilboev
Teacher of Administrative and financial
law department, Tashkent State University of law,
j.zoilboyev@tsul.uz
+998946796649

https://doi.org/10.5281/zenodo.7722748

Abstract.
This article explore new concepts law which emerging and becoming popular in jurisprudence. This is literally “digital law”, and “digital hygiene”. This article will discuss the problems and shortcomings of cybersecurity, digital law and digital hygiene, as well as the problems and obstacles that the world's media currently face.

Keywords: digital law, digital hygiene, safety, privacy

“Digitizing information” [1,11p] means representing information as a sequence of zeroes and ones. Digital data can be easily edited, stored, and transferred between computers. Given the high power of modern computers and their Global Internet, this means that large amounts of data can be processed, stored, and transmitted in real-time. This means the digitalization of data. So, the concept of “digital” is the representation of information in the form of numbers. In this way, usually confidential information is encrypted and kept from public knowledge. Now, if we come to the concept of law, the concepts that have been formed for many years help to understand and interpret the law. The law as a means of control [2, 6p] has been forming and maintaining its internal structure since the 18th century. Law is also defined as: “a system of rules by which a particular country or community regulates the actions of its members and enforces them through punishment”.

It is also appropriate to mention that “the law is an enterprise of subordinating human behavior to the management of rules [3, 5p]”. In addition, the law is defined as “a process that aims to shape behavior, resolve conflicts, secure rights, and freedoms, and even hope for justice [4, 122p]”. It follows from this that the law is a social process that determines the order of behavior in society and acquires a special feature when it is developed and protected by the state authorities. There are also different approaches to the study of law, and under the influence of these approaches and views, law families are divided into such huge types as “common law” and “continental law”. However, it would not be an exaggeration to say that the digital right we are talking about has united the above two families.

Since the beginning of humanity and individuals began to live as a community, the members of the community have determined certain actions to be performed by them as a rule. With the passage of time and the introduction of modern technology into our lives, the implementation and application of law are changing and expanding. In particular, in today's digital world, the concept of "digital law" has entered our lives, and at the moment, the development of "Digital Law" is entering the digital battlefield as the most alternative solution to "cybercrimes", online offenses. What is digital right? How is it different from common law? Digital law is emerging as a modern concept of electronic responsibility for ethical or unethical behavior. At the same time, digital law is defined as electronic responsibility for actions and actions[5]. To put it another way, digital law refers to what is allowed and what is prohibited while using the internet. Also, according to the ethical criterion of using the Internet, two types are distinguished: ethical use includes all activities on the Internet that comply with the laws of society. Unethical use covers all activities on the Internet that do not conform to the laws of society. As mentioned earlier, cyber security plays an important role in the continuous development of information technologies and Internet services. Making the Internet safer (protecting Internet users) and developing new services is becoming an integral part of government policy. Cybersecurity strategies—for example, developing technical protection systems or educating users to prevent becoming a victim of cybercrime—can help reduce the risk of cybercrime. Digital law is the most important of these tools. If the main actions of the state and international organizations are reflected in constitutions, laws, international agreements, and legal documents, digital law is a form of these rights that are implemented in modern techniques and technologies and the Internet, without denying these sources of law.

International economic organizations such as the Organization for Economic Co-operation and Development (OECD)[6], the Forum for Asia-Pacific Economic Cooperation (APEC)[7], and the African Union (AU)[8] have their data privacy policies related to cross-border transfers of personal data. These guidelines help create an international privacy and data protection standard to promote international trade, but these norms are weaker than the domestic laws of some participating countries. One of the most important of these standards is the "General Rules for the Protection of Personal Data" adopted by the European Union in 2016[9]. In ordinary social relations, the personal rights of a person regulate the social relations that occur in everyday material life with the provisions stipulated in the Constitution, laws, legal documents, and international agreements. In digital law, as well as in the Constitution, laws, regulations, and international agreements, the rules, and procedures for the implementation, and management of actions carried out on the Internet are determined. For example, Article 97 of the Criminal Code of the Republic of Uzbekistan stipulates that if "intentional murder" is a crime against a person, disclosure of information about a person without his permission, as well as preparation, storage, and distribution of religious materials, is also considered a crime[10]. These norms are considered material law norms. Digital law, as a new field of law, is a set of legal norms aimed at regulating social relations related to modern techniques and technologies. As a rule, it should be said that digital law is a set of rules of conduct aimed at regulating social relations arising through digital technologies, determining the level of responsibility of Internet users for their actions[11].

As an example of digital law, let's consider the digital legal norms of the Facebook[12] social network, which is used by approximately 2 billion 936 million people[13] of the world's population. According to https://transparency.fb.com, users of the Facebook social network will have to follow the legal norms in the following areas:

- *Authenticity;*
- *Security;*
- *Confidentiality;*
- *Dignity.*

Authenticity.

Facebook wants to make sure that the content you see on it is authentic and will try to ensure that it is. Also, given that authentication is a good environment for information sharing, Facebook does not support hacking information about who users are or what they are doing on Facebook.

Safety.

Facebook is a safe network, and content that could harm the physical safety of users is removed. Any information that threatens people can intimidate, humiliate, or insult others will be deleted from the network.

Confidentiality.

Facebook ensures the privacy of its users and the confidentiality of information. Privacy allows users to make independent decisions about when and what information to share and what information not to share on Facebook.

Dignity.

Every user using Facebook is guaranteed the same dignity and rights and freedoms. Each user shall also take steps to ensure that the dignity of others is respected.

The above are the terms of use of the Facebook social network. In addition, there are important digital rules that every user should follow. In particular, users are prohibited from posting the following materials:

- Materials promoting violence and violence;
- Materials promoting cruelty and religious discrimination;
- Content that spreads international incitement and threatens humanity.

We can conclude that digital law is a form of material law applied to modern technologies. In this, the main focus should be on determining responsibility for any crime or other socially dangerous act committed through digital technologies, as in traditional law. In particular, any damage caused to the dignity of a person through mass media and social networks should be strictly punished. In addition, it is appropriate to protect any form of copyright.

What is digital hygiene and can it prevent cybercrime?

As soon as we hear the term hygiene, we think of a set of actions such as getting up in the morning, washing our hands, brushing our teeth, and dressing neatly. These actions serve as the main protector of a person's health. At the moment, before going to work or study, we go to our profiles on social networks through the mobile communication tool in our hands: we get acquainted with what's new in it, the messages directed to us and sent to us. Now think about it, do you follow your hygiene on your mobile device and social networks?

Digital hygiene. We cannot imagine our daily life without social networks and electronic devices, as well as procedures for safe use of the Internet. From a scientific perspective, “digital hygiene is a tool to encourage people to engage in regular digital practices to minimize cyber risks”. The term was first used by Suzanne Sontag in a lecture at the James Institute in October 1977[14], and unlike “cybersecurity” used in military or combat operations, “digital security” is concerned with the health of the individual. In 2014, the entire scientific and theoretical aspects of the term “digital hygiene” were covered by scientists from the Institute of Network Culture(INC). According to him, in a text called “Digital transcoding”, Marianne interpreted the concept of “digital practice” as a serial set of everyday practices that involve manipulating, modifying and designing digital symbolic objects of social importance[15].

So, with the origins of “digital hygiene” dating back to the recent past, what do we need to do to ensure our safety on social media?

Firstly, It is necessary to form the ability to follow the principle of "I hear, and forget. I see, and I remember. I do, and I understand". The reason is that each of us uses social networks in our daily life. Let's say you have Facebook, Instagram, or just a Telegram messenger, and you run your business through them. To keep your personal information, files, and your leisure time safe in the Telegram messenger, you will need to implement a multi-step algorithm. This algorithm is called "two-step verification" [16, 134p]. You should test this protection system yourself to make sure your personal information is protected. Only then, your data will be stored safely, and the security system created with the help of any second person will create a danger to that second person.

Secondly, it is advisable for you to thoroughly familiarize yourself with the consequences of not keeping your personal information safe. And this in itself forms the idea of what "digital hygiene" is and the ability to follow it. What are the consequences of not following the rules of security in the cyber environment and not protecting personal information?

Failure of a computer, phone-"gadget" in general; There is a risk that viruses can easily transfer from other devices and damage your device to the extent of turning it into a worthless item; Neglecting the device and even worse, it can lead to the loss of files that are very important to you; Cause irreparable damage or loss of necessary information; Disclosure, dissemination, disclosure of personal information, resulting in violation of the "right to privacy"; Poisoning of the young generation, especially your child, with inappropriate information; Violation of financial security and increase of risks affecting a person's activity, etc.

"Digital hygiene" teaches that to ensure data security, it is necessary to establish several levels of control. Risk prevention is better than its elimination.

*Here are some of the best tools and techniques:*

*1. Make sure that the device is secure;*

*2. It is important to always use secure systems, such as knowing that unsecured Wi-Fi is not safe.*

*3. Before entering the site, check that the sites you are visiting are not harmful.*

*4. Take security measures when downloading files on the Internet.*

*5. Avoid downloading any "free" programs provided on the Internet, always remembering that they are not without the possibility of being a source of viruses.*

*6. In any case, check the given external memory devices for antivirus.*

*7. Understand the need to be careful of pop-up ads and announcements;*

*8. Using official applications that ensure device security.*

*9. Imagining the social network as real life, forming the skill to leave that factor if a suspicious factor appears.*
*10. Regular cleaning of files.*

It is important to note that those who pose a threat to your personal information are first of all persons who have perfect knowledge of technology. They are also educated and more precise. A clear example of this is a young man named Scotsman. In 2002, he carried out "the largest military hack of all time". At the same time, Scotsman was able to break into 97 computer systems (this system belonged to the US and NATO military forces) [17, 138p].

In general, in today's fast-moving digital world, the safety of the person and data depends on the scale and impact of the measures being implemented. As noted and analyzed above, cybercrime is becoming one of the most dangerous enemies of society and the state. In the fight against it, it is required to introduce the most effective systems, put them into practice, and strengthen integration. Another important aspect is the need of the hour to form cyber security, digital rights and digital hygiene, making them an integral part of everyday life..

## References:

1. Eric Hilgendorf, Jochen Feldle. 2018. Digitization and the Law. Wurzburg: Nomos.
2.Waldron, J, E.N. Zalta. 2020. The Stanford Encyclopedia of Philosophy. Stanford: Stanford University.
3.Austin, John. 1955. The Province of Jurisprudence Determined. Cambridge : Cambridge University Press.
4.Katsh, M. Ethan. 1995. Law in a digital world. London: Oxford University Press.
5.Digital Citizenship by Stephanie Miller is licensed under a Creative Commons Attribution NonCommercial-NoDerivs 3.0 Unported License.
6.https://www.oecd.org (Organization for Economic Cooperation and Development)
7.https://www.apec.org (Asia-Pacific Economic Cooperation)
8.https://au.int
9.General Data Protection Regulation. 2016. Online: https://gdpr-info.eu/
10.Criminal code of Uzbekistan: https://lex.uz/docs/-111453
11.Author
12.Facebook©. A social platform created by Mark Zuckerberg in 2004. To date, Meta Platforms Inc. - an American multinational holding company that owns a technology conglomerate and is based in Menlo Park, California. Facebook, Instagram, WhatsApp and Oculus are integrated networks.
13.https://datareportal.com/essential-facebook-stats#:~:text=Here's%20what%20the%20latest%20data,)%3A%202.936%20billion%20(April%202022)&text=Number%20of%20people%20who%20use,)%3A%201.960%20billion%20(April%202022)
14.https://www.youtube.com/watch?v=6WC5ncbR0zQ
15.https://networkcultures.org/blog/2021/05/12/digital-hygiene/

16.Gelbstein, Eduardo. 2015. Good digital hygiene:a guide to staying secure in cyberspace. Bookboon.