DOI: 10.33498/louu-2021-09-144

Alizadeh Huseyn Oktay

PhD Doctorate,
Baku State University
(Baku, Azerbaijan)
huseyn.alizade.95@bk.ru

УДК 342.92

THEORETICAL AND LEGAL APPROACHES TO THE CLASSIFICATION OF INFORMATION-LEGAL VIOLATIONS

Abstract. The current legislation is characterized by the lack of a unified approach to the assessment of violations in the field of information technology, the unity of the conceptual apparatus used and the application of inappropriate and unsystematic changes that do not yield the expected results. In addition, the imperfection of the legislation governing the application and use of the achievements of scientific and technological progress, the division of the regulatory framework in approaches to the legal regulation of various aspects of technological progress remain a common legal problem.

Due to the fact that the global network covers all countries, the states dealing with information violations must develop a common legal language in order to carry out effective cooperation. It is important to standardize international norms on the basis of this legal language, so that the states of the world must implement their legal regulations in accordance with these international rules. In most cases, international norms are accepted as a "standard" and implemented in national law. However, the necessity of modern times confirms the obsolescence and change of many international norms. The article proposes to make various edits on such international documents related to information violations. In our opinion, since national law is often based on international law, such edits and changes can also contribute to domestic law.

As noted in the article, in many cases, violations in the field of information do not constitute an error or a crime, but only temporary "user concerns". However, the practical examples we present once again confirm that a simple crack can eventually lead to loss of life. Therefore, law enforcement agencies should not be indifferent to complaints about the use of such computers and the Internet, and take preventive measures to prevent them.

Keywords: information-legal violation; classification; cybercrime; cyberspace; Budapest Convention.

The study of information-legal violations as an urgent problem began after the formation of the information society. In this society, which was expected to achieve successful results in its early days, it was inevitable that there would be various negative situations. As early as the 1950s, Norbert Wiener, the founder of information theory, who defined information as information obtained in the process of adapting ourselves and our senses to the environment, posed problems with automation and the dangers of ICT. Over time, these threats, which Wiener mentioned, became widespread as information-legal violations.

Today, the Internet has penetrated all areas in accordance with the needs of everyday life and connected people from all over the world. This connection allows people to shop and communicate, transfer information, and even globalize in a free environment. Today, even states are forced to use information technology to carry out their activities. With the Internet connection, the activities of the legislative, executive or judicial bodies of the state are organized in such a way that, unlike the classical system of governance, the instructions are transmitted more quickly between government agencies in electronic form. The use of information systems in key infrastructure sectors such as energy, communications, agriculture, health, transport, education and finance has highlighted the importance of the concept of cyber security, which is thought to be equivalent to national security. In the modern world, which is interconnected by a single global network, the existence of cyberspace, along with the risk of losing the sovereignty of states, as well as the existence of specific borders has become a controversial fact. Because in this area where there is no central government, it is very difficult to prevent or combat abuses, and the regulation of one state is not enough. Therefore, the prevention of violations of information rights is important not only in one direction, but also in other human rights.

The article's objective is to analyze theoretical and historical approaches to information-legal violations, to identify the main and different features of these violations and to make legal proposals in this regard.

Bringing into the focus only the criminal-legal aspect of information-law violations is not sufficient to reveal the essence of the issue. Therefore, it is more appropriate to consider these violations as misdemeanour, civil tort and crime. In the digital society, there are many information security violations that undermine civil law relations. Thus, on social media, which has a database of billions of users, such violations have become very widespread. The development of social media as a means of communication in recent years has confirmed that cyberspace is a significant area for strategic communication and information dissemination. Hereby, one can even assert that organizations founded with the aim to prevent the spread of negative information in cyberspace operate and promote the activities of states in a positive direction. For instance, the WikiLeaks network reveals several high-profile cases of

ПРАВО УКРАЇНИ • 2021 • № 9 • 144-154

corporate and government corruption, "Troll Farms"[1] create fake social media profiles, and websites to support troll operations. Troll farm employees not only write messages, but also respond to comments and participate in online discussions. They can simulate controversy to increase the impression of the trustworthy of the fake profiles they spread by creating content.

Conversely, there are social media sites and platforms that are engaged in conveying the policy of a state in a positive direction. For instance, Israel's Hasbara press is used to promote the government's policies in a positive light in response to criticism and negative feedback. Moreover, Hasbara put its efforts to foster Israel's reputation. Hasbara is considered a euphemism for propaganda.

It should be noted that no matter how much this type of false information is combated, its impact on misleading people is enormous. Nowadays, social media has become a major player in the hybrid warfare, and the concept of spam is not only interpreted from a technical point of view, but also applies to false information shared on social media[2].

Spear phishing and cyber espionage should be mentioned among the information-related violations related to social media. Victims of phishing attacks usually were engaged in an action that involves clicking on a malicious link or opening an email application that is loaded with malware. Both actions can lead to fake websites that require victims' login information. Cyber-espionage accounts for 24 % of phishing violations including abuse of state secrecy[3]. The main motivation is to extract sensitive government information that can be misappropriated for several malicious purposes. By way of illustration, one can mention the case with the email accounts of Hillary Clinton's campaign manager John Podesta and former US Secretary of State Colin Powell which have been hacked allegedly by Russian-backed spear attacks and the information has been leaked to the public with the purpose of defamation or in order to negatively impact the campaign. Intellectual property theft, such as robbing military plans or technological innovations, can

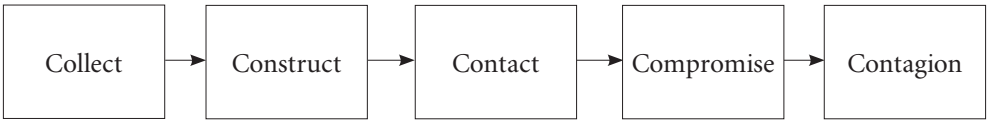
[1] The term "troll factory" started to emerge on a wider scale in media reports in 2015. At that time, journalists revealed the existence in St. Petersburg of a troll factory employing 300 people. The entity officially operated as the Internet Research Agency, managed by an oligarch, Yevgeny Prigozhin. The duties of the employees included publishing on the Internet, mainly in social media, posts praising Russian President Vladimir Putin, and criticizing countries not supporting Russia. The operation of this troll factory was initially associated with the annexation of Crimea and then with the presidential election in the United States ('Troll factories' *(deepportal.hq.nato.int)* <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal2-troll-factories.pdf> (accessed: 16.09.2021)).

[2] Benjamin Duranske, 'Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life' (*Virtual Law,* 24.04.2007) <http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life> (accessed: 16.09.2021).

[3] '2021 Data Breach Investigations Report (DBIR)' <https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf> (accessed: 16.09.2021).

be used to achieve strategic geopolitical goals. Furthermore, obtaining trade or production data can provide a tactical advantage in trade negotiations[4].

As with email, most phishing attacks on social media are financially motivated cybercrimes. The implementation of spear phishing on social media is interpreted in five stages[5]:



The first step is to collect information about the intended target. Social media platforms provide a lot of information that is accessible to everyone, and this information can then be used to create fake accounts that suit the target's personal or professional interests. During the data collection, research is done first. Because even if the offender knows which object will be phishing, he may not know the exact range of people to whom all the phishing will be directed. In addition to identifying Internet connections, criminals can collect identifying information, such as email addresses, phone numbers, work history, education, or interests. The attacker can track the target's previous online connections, especially on open platforms such as Twitter and LinkedIn. On the eve of the French elections in 2017, Facebook revealed about twenty fake accounts that were spying on the Emmanuel Macron's presidential campaign who was then himself a presidential candidate. The accounts, linked to the Russian hacker group Fancy Bear, which was responsible for the US Democratic National Committee's email attacks were involved in this event; 'the spying campaign included Russian agents posing as friends of friends of Macron associates and trying to glean personal information from them'[6].

After gathering information, criminals create fake social media profiles to interact with the target. The created profile may include fake information, such as working for the same organization or studying at the same university. As the case with the Russian Internet Research Agency which created Facebook pages such as "The United Muslims of America" and Blacktivist shows, established accounts can even mimic or fabricate organizations.

As a matter of fact, in most cases, photos of attractive women are used in the form of profiles. This method is known as the Robin Sage Experiment. Robin Sage is a fictional American cyber threat analyst. It was created in December 2009 by two controversial security experts and hackers from New York City,

[4] Levent Kurt, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması* (Seçkin Yayınları 2005) 98.

[5] A-M Huhtinen, J Rantapelkonen, 'Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere' [2016] 15 (4) Journal of Information Warfare 50–67.

[6] Joan Goodchild, 'The Robin Sage experiment: Fake profile fools security pros' (*NETWORKWORLD,* 08.07.2010) <https://www.networkworld.com/article/2213486/the-robin-sage-experiment--fake-profile-fools-security-pros.html> (accessed: 16.09.2021).

Robin Casey and Thomas Ryan. The name is derived from the training of the Special Forces of the United States Army. Introducing herself as a beautiful 25-year-old woman on social media, Ryan made contact with men and women of all ages in a short period of time from December 2009 to January 2010. Almost all of them served in the US military and relevant government agencies. Using these connections, Ryan learned the location of secret military units based on Facebook photos of soldiers, contacts between different people and organizations, as well as access to email addresses and bank accounts[7]. This practice was later repeated several times in different countries. For instance, an Iranian hacker carried out the Robin Sage experiment by seizing secret data of the Middle Eastern industries and governments and creating a fake Mia Ash profile[8].

The next step in spear phishing is to make contact. The most common method of communication is to communicate with the target through any account. For example, making friends on Facebook, connecting on LinkedIn, following on Twitter and Instagram. Another way to connect is with platform-specific chat services such as Facebook Messenger, LinkedIn InMail or Twitter Direct Message. The third method is advertising campaigns. Although social media companies hire human moderators to validate paid ads, there are documented cases of malicious software connections that go beyond this verification process.

95% of phishing violations are software downloads to the target device, which is usually obtained when a user downloads an email attachment with a malicious software load. Therefore, this is the stage of compromise. After the malware is installed, criminals use a dangerous device to steal information by browsing the network. It is often unknown that the target devices are affected, and the attackers cannot be detected in a network for years.

The latest stage that is the stage of contagion could increase the scale of the cyber-attack. Contagion is especially dangerous because hackers can target vulnerable victims and reach larger targets.

Some researchers, who give an overly broad interpretation of information-law violations, refer to these violations as illegal actions that can be committed in the field of information security, which is a special field of human activity and which includes searching, creating, processing, transmitting, receiving, storing, protecting and using all kinds of information. At the same time, they include violations in other areas of human activity in the information environment, that is using information tools and technologies to work with information, regardless of its form[9].

[7] Huhtinen, Rantapelkonen (n 5).
[8] F B Nacar, *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları* (Yüksek Lisans Tezi 2010).
[9] Michael Bossetta, 'The weaponization of social media: spear phishing and cyberattacks on democracy' [2018] 71 (1.5, Special Issue) Journal of International Affairs 97–106.

Fatma Burju Najar classifies information-legal violations depending on the object[10]. In our opinion, this classification can be considered more pertinent. Information-law violations can be explained in more detail not only within the context of cybercrime, but also based on the author's classification. However, the biggest shortcoming of the author's position is to almost equate information-legal violations to cybercrime, and in some cases to identify one with the other. One must also bear in mind that in any case, information security violations infringe on information or data. Moreover, even illegal access to the network can lead in the end to such negative consequences as the change, destruction, etc. of the data. Therefore, it is better to classify information-legal violations according to the method of committing a crime.

Some researchers classify information security violations as the following:

1. Violations of the data:

– Data interference can take the form of unlawful interference, alteration, or access to information.

– Data capturing is carried out in the form of removal of information from the location in order to harm the owner of the information or others, or to gain an illegal advantage over by the offender himself or by others.

– Data alteration involves compromising, damaging, or altering the security of information in information systems.

2. Violations of information networks:

– network blocking prevents the user from accessing the entire network or part of it;

– network sabotage aims to change an information system or network as a result of physical damage;

– illegal access is defined as access to an information system without the owner's permission;

– the spread of a virus is the activation of malware to damage the system or data. Viruses damage systems, data, and programs. The spread of viruses is not a separate crime, but a crime depending on the result obtained[11].

Verison's 2021 Report refers to the terms "incident" and "breach" in relation to information security violations. If the incident involves a security incident that violates the integrity, confidentiality and accessibility of the information asset, the breach consists of actions that result in the disclosure of the data to an unauthorized party, however the process consists only of possibilities of potential disclosure[12]. The report, which assesses violations more dangerously, notes that violations have occurred over time compared to previous years, and

[10] Bossetta (n 9).

[11] Joseph Menn, 'Exclusive: Russia used Facebook to try to spy on Macron campaign – sources' (*News. Yahoo,* 27.07.2017) <https://uk.news.yahoo.com/exclusive-russia-used-facebook-try-spy-macron-campaign-050414445--finance.html> (accessed: 16.09.2021).

[12] 2021 Data Breach Investigations Report (DBIR) (n 3).

based on the generalizations made, the following specific violations have been identified[13]:

Social Enineering	Psychological compromise of a person, which alters their behavior into taking an action or breaching confidentiality
Basic Web Application Attacks	Simple web application attacks with a small number of steps/additional actions after the initial web application compromise
System Intrusion	System Intrusion captures the complex attacks that leverage Malware and/or Hacking to achieve their objectives including deploying ransomware
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which is grouped with theft instead.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges.
Lost and Stolen Assets	Any incident where an information asset went missing, whether through misplacement or malice.
Denial of Service	Attacks intended to compromise the availability of networks and systems. Includes both network and application layer attacks.
Everything Else	This last "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns.

Thus, the increase of the incidents happened according to last example is absolutely true. This is due to the fact that the methods of committing information-legal violations are changing day by day. However, the approach is not considered successful within our research topic. Interpreting information rights violations in terms of actions rather than in the context of events might be significant in preventing those violations. One of the main classifications of information-legal violations is related to open and closed information. The problem is that a lot of confidential information is protected under different rights. For example, confidential personal information is protected by the right to privacy. However, in our opinion, the violation of the rules related to the protection of confidential information, as well as the provision of various information, namely the implementation of the information request, etc., and failure to comply with such rules and regulation is a direct information-legal violation. As it is evident, information is divided by law into open and closed (restricted access) information. Confidential information is protected under

[13] 2021 Data Breach Investigations Report (DBIR) (n 3).

the name of "secret" and violation of the legal regime of this information, both in electronic and non-electronic form, will result in appropriate liability. Such violations, which are formalized as a minor administrative offense and fall within the scope of Chapter 32 of the Criminal Procedure Code, are more serious than the relevant articles of the Criminal Code (Articles 155, 156, 202, 284).

To sum up, it should be emphasized that information-legal violations should be classified from civil, administrative and criminal-legal aspects. Violations of information law, which take the form of civil tort, in many cases lead to litigation. As early as 2007, a complaint was received in Belgium about the cyberbullying in the "Second Life" virutal environment and an investigation was launched correspondingly. As a result, it was reported that in Second Life, avatars may have virtual aggression against each other. However, the consent of the other player is required. That is to say, you can be raped only upon your consent[14].

Information-legal violations should not be strictly limited to cybercrime. Definitely, cybercrime is a major illegal act that undermines the completeness, confidentiality and accessibility of information. However, as information relations are more extensive, information-legal violations must also have a broader content. For instance, if certain computer information becomes the object of an attack by obtaining information about a person's private life, it is also plausible to violate that person's rights by insulting that person in cyberspace. In this regard, the boundaries of the information infringement are somewhat wider. Perhaps that is why the classification of cybercrimes in the Budapest Convention is made in this context.

Conclusions. Thus, in most literature review, "information infringement" refers only to cybercrime. The issue is that in the case of violations in the field of information, in most cases there is a need to apply criminal law. This is due to the fact that the Criminal Code does not provide for a lighter form of criminalized cybercrime in the Code of Administrative Offenses (CAO). Thus, while there are cases where ordinary theft is classified as a crime or an offense, depending on the value of the object of the conspiracy, the legislature has not provided any alternative to the circumstances in which acts committed in cyberspace against information systems and data bring minor consequences. It is expected that there will be difficulties in the implementation of the CAO, which identifies a common error (Article 371 of the Code of Criminal Procedure of the Republic of Azerbaijan), such as "violation of the rules of use of information resources". At the same time, another problem is related to the fact that for most cybercrimes, a special subject is perceived as a constituent element. In our digital world, it is not uncommon for ordinary people to seize information using ICT. We believe that the formal provisions of the Criminal Code need to be included in the Code of Criminal Procedure as an

[14] Duranske (n 2).

administrative offense. Moreover, the execution of these acts by all persons regardless the status of a subject, should be held accountable. In this regard, there is a need to analyze the experience of foreign countries.

It should also be borne in mind that illegal actions related to the use of ICT data, in many cases, do not cause serious consequences, but bring up certain concerns for different people. For instance, one can note that malware and virus e-mails content are sent via e-mail. If the user does not open the received email, there is no negative consequence. However, there are concerns caused. For instance, temporarily blocking a website (chat, discussion forum, etc.) that a person often uses by administrators might be an example for the case. Although it doesn not legally constitute a crime, it is possible to solve the problem by imposing liability as an administrative offense. There is even the experience of foreign countries on complaints about the damage caused in the virtual space. Concerns that do not lead to these serious consequences may create administrative liability.

The essential issue is that the term "cybercrime" is not clarified in international norms. Therefore, in the national laws of different countries, such acts are called differently (electronic crimes, computer crimes, crimes in the field of computer information, high-tech crimes, etc.). Also, cybercrime is widely interpreted in most sources, namely all violations committed in cyberspace are considered cybercrime. This is the approach of the Budapest Convention. However, in our opinion, such an approach may eventually lead to the criminalization of all criminal acts. This is due to the fact that digitalization also creates great opportunities for the criminal world. For example, insults or slander in the traditional form are almost non-existent. Since crimes must be classified depending on the object of intent, it is not correct to consider these acts as cybercrime. Therefore, a broad interpretation of cybercrime is not acceptable. In this regard, it is more expedient to amend the Budapest Convention itself. Although the Convention is broadly based on an analytical approach, many acts committed using ICT (such as public incitement to terrorism) remain unregulated.

REFERENCES

Bibliography

Authored books

1. Levent K, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması* (Seçkin Yayınları 2005) (in Turkish).

Journal articles

2. Bossetta M, 'The weaponization of social media: spear phishing and cyberattacks on democracy' [2018] 71 (1.5, Special Issue) Journal of International Affairs 97–106 (in English).

3. Huhtinen A-M, Rantapelkonen J, 'Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere' [2016] 15 (4) Journal of Information Warfare (in English).

Theses

4. Nacar F B, 'Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları' (Yüksek Lisans Tezi 2010) (in Turkish).

Websites

5. '2021 Data Breach Investigations Report (DBIR)' <https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf> (accessed: 16.09.2021) (in English).
6. 'Troll factories' (deepportal.hq.nato.int) <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal2-troll-factories.pdf> (accessed: 16.09.2021) (in English).
7. Duranske Benjamin, 'Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life' (*Virtual Law,* 24.04.2007) <http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life> (accessed: 16.09.2021) (in English).
8. Goodchild Joan, 'The Robin Sage experiment: Fake profile fools security pros' (*NETWORKWORLD,* 08.07.2010) <https://www.networkworld.com/article/2213486/the-robin-sage-experiment--fake-profile-fools-security-pros.html> (accessed: 16.09.2021) (in English).
9. Menn Joseph, 'Exclusive: Russia used Facebook to try to spy on Macron campaign – sources' (*News.Yahoo,* 27.07.2017) <https://uk.news.yahoo.com/exclusive-russia-used-facebook-try-spy-macron-campaign-050414445--finance.html> (accessed: 16.09.2021) (in English).

Алізаде Гусейн Октай

ТЕОРЕТИЧНІ ТА ПРАВОВІ ПІДХОДИ ДО КЛАСИФІКАЦІЇ ІНФОРМАЦІЙНИХ ПОРУШЕНЬ

Анотація. Чинне законодавство характеризується відсутністю єдиного підходу до оцінки порушень у сфері інформаційних технологій, єдністю понятійного апарату який використовується та застосуванням неналежних і несистематичних змін, які не дають очікуваних результатів. Крім того, поширеною правовою проблемою залишаються недосконаліть законодавства, що регулює застосування і використання досягнень науково-технічного прогресу, поділ нормативно-правової бази у підходах до правового регулювання різних аспектів технічного прогресу.

У зв'язку з тим, що глобальна мережа охоплює всі країни, для ефективної співпраці держави, які займаються інформаційними порушеннями, повинні виробити спільну правову мову. Важливо стандартизувати міжнародні норми на основі цієї правової мови, щоб держави світу реалізовували свої правові норми відповідно до цих міжнародних правил. У більшості випадків міжнародні норми приймаються як "стандарт" й імплементуються у національне законодавство. Однак нагальна потреба сучасності підтверджує застарілість і зміну багатьох міжнародних норм.

У статті пропонується внести різноманітні правки до таких міжнародних документів, пов'язаних із інформаційними правопорушеннями. На нашу думку, оскільки національне законодавство часто базується на міжнародному праві, такі правки та зміни також можуть сприяти внутрішньому праву.

Як зазначається, у багатьох випадках порушення в інформаційній сфері не є проступком чи злочином, а лише тимчасовими "занепокоєннями користувачів". Проте практичні приклади, які ми наведемо, ще раз підтверджують, що просте порушення у підсумку може призвести до загибелі людей. Тому правоохоронні органи не повинні бути байдужими до скарг на використання таких комп'ютерів та інтернету й вживати превентивних заходів для їх запобігання.

Ключові слова: інформаційне правопорушення; класифікація; кіберзлочинність; кіберпростір; Будапештська конвенція.