DOI https://doi.org/10.36059/978-966-397-142-1/159-175

PROBLEMS OF LEGAL REGULATION OF RELATIONS ON THE INTERNET

Mazurenko S. V.

INTRODUCTION

In today's context, there is a rapid growth of the global and Ukrainian segment of the global Internet information network, both in quantitative (number of operators and users) and qualitative (expansion of the range of services provided) in relation.

In Ukraine, the formation of a separate branch of legislation governing Internet relations is only just beginning. Existing jurisprudence relating to the use of the Internet cannot be called great, as long as the law enforcement activity of public authorities in this area is low.

Similar to the legal systems of other countries, including the United States and European Union countries, Ukrainian special legislation on the Internet is at its very beginning. However, it is largely possible to speak about the absence of an effective regulatory framework in this area, despite the existence of general rules of constitutional, civil and administrative law and a number of other legislative acts. The reasons for this are both insufficient theoretical elaboration of some fundamental regulations and subjective precautionary treatment of the Internet by law enforcement agencies.

However, the lack of legislation on the Internet, as well as the possibility of their effective application, adversely affects the development of public relations (for example, in the area of citizens' rights to information, prevention of dissemination of information that affects the honor and dignity of citizens, protection of intellectual property objects property, in other spheres of social and political life) not only in Ukraine but also abroad.

In this regard, the urgency of the issues chosen is that, having appeared more than fifty years ago, the Internet is still considered a "white spot" from the point of view of law. The constant increase in the number of subscribers, the increasing importance of information exchange through the Network, attract the attention of the public to the problems of regulation, elaboration of rules of fair, legal functioning of the Internet from the state side.

Today it is difficult to imagine the existence of human civilization without a world wide web. The Internet is the largest repository of publicly available data, the most up-to-date media, the territory of many e-shops, interest clubs and more.

The Internet has become a virtual space in which millions of network users enter into different relationships every day, unaware of it. The types of social relationships that emerge and develop on the Internet are as diverse as they are in the ordinary physical world. This situation makes it necessary to pay more attention to Internet relations.

Today in the scientific literature it is quite common to find the terms "Internet relations", "Internet legal relations", "legal relations on the Internet", "legal relations in the electronic sphere", "information legal relations on the Internet", etc. We believe that the most appropriate term is the term "Internet relations".

Public relations arising from the use of global computer networks are special informational relations aimed at organizing the movement of information in the society. Internet relations are conditioned by the information nature of communications in the information society, which can only be accessed through a computer connected to a computer network. The peculiarity of these relationships is also the presence of a technical component, information content, special subject composition. Internet relations are public relations that exist in electronic and digital form in cyberspace. It should also be noted that the subjects of these relations may be located in different countries, and their activities are governed by the laws of different countries. Internet relationships cannot exist without the use of information and telecommunications technologies and networks. These relationships are informative, that is, they are about information on the Internet.

1. The problem of identifying users on the Internet

With the development of the Internet and Internet relations, one of the most pressing problems has been the problem of identifying users on the Internet. This problem is multidimensional and has many manifestations.

The task of user identification does not lose its relevance due to the constant race of information security technologies and technologies of unauthorized access to information. The urgency of this task for the Internet is increasing through the use of unsecured data channels.

First of all, it should be noted that the issue of identification already arises at the stage of connection to the Internet. It is associated with a number of basic terms that characterize network relationships at the technical level and subsequently flow into the legal plane: account (an account usually contains the information required to identify the user when connected to the system, authorization and accounting information); domain (a means of identifying a resource area on the Internet); domain name (the name that identifies the computer or computers on the Internet); identifier (a unique combination of a user name and password to ensure his / her identification process); identification (matching the recognized object to its image) and the like[1].

The problem of identification on the Internet is not only a technical dimension, but also a social and legal dimension. D. Afanasiev focuses on the social dimension of such identification. According to the author with the spread of broadband networks and the advent of Web 2.0 technology, which is a modern concept of Internet development on the basis of collective content creation by any user of the network, the number of Internet users has increased and the software supporting group interactions has increased. The emergence of social networks on the Internet – that is, communities of people related to a common interest or business existing on the Internet, using specialized software services, websites, and portals to engage people in a group or group. Accordingly, there was a need to identify users of social networks[2]. However, without going into the specifics of such identification, it can be argued that the scientist speaks about the various social roles that users of the Internet and social networks can acquire (for example, a man can portray himself as a woman, a humane person chooses a mask of a cruel being, etc.). However, for the law, the complexities are quite different – the problem becomes relevant only when the rights of others or the law are violated. For example, when an account was stolen on a social network and the information is being distributed on behalf of that user that violates the rights of others. However, the owner (real) of this account does not know about it.

[1] Базові поняття і терміни веб-технологій / [А.В. Кільченко, О.І. Поповський, О.В. Тебенко, О.В. Тебенко, Н.М. Матросова]; Упорядник: Кільченко А.В. – К. : ІІТЗН НАПН України, 2014. – С. 21.

[2] Афанасьєв Д. Особливості ідентифікації суб'єкта інтернет-мережевих спільнот / Д. Афанасьєв // Науковий вісник Ужгородського національного університету. Серія : Педагогіка. Соціальна робота. – 2012. – Вип. 24. – С. 16.

For example, an identification problem may arise in the event of a breach of a contract concluded via the Internet. Thus, according to S.M. Zhutova, today the questions of the possibility of identification of the parties to a contract concluded electronically remain unresolved. It is possible to determine that the contract signed by those persons who have identified themselves on the Internet is possible only by means of an electronic-digital signature, which in modern conditions can also be forged[3].

Particularly urgent problem of identification of users on the Internet becomes in case of copyright infringement. The relative anonymity of Internet users is twofold. On the one hand, such activity contributes in some way to copyright infringement and other infringements. On the other hand, the question of the anonymity of Internet users must be considered in the light of the principle of proportionality between intellectual property rights and the right to freedom of expression, the right to respect for privacy and family life. In addition, the anonymity of connections does not interfere with publicly useful activities (such as the legitimate distribution of works).

A.S. Ogarkov notes in this context that "the most common ways of controlling access are powerless against sufficiently experienced users who easily find methods of circumventing such systems. Moreover, there are special services to help users hack into these controls and access resources that are not accessible to them[4]".

K.A. Zerov claims that the process of identification of a person who has committed copyright infringement for works published on the Internet has been divided into three scientific stages in foreign scientific literature.

The first stage involves the right holder (his representative) acting to identify and collect IPs and other information that will help identify the offender. To determine and collect the IP address of a copyright infringer in the field of P2P networks, copyright holders use the following methods:

1. indirect identification of users, which relies on a set of data on the money returned from the torrent tracker;

2. The direct definition is to connect via torrent tracker to users who distribute certain files and then share files with them.

---

[3] Жутова С.М. Особливості укладання угод через мережу інтернет / С.М. Жутова // Молодий вчений. – 2017. – № 11. – С. 877.

[4] Огарков А.С. Примусова авторизація в мережі інтернет / А.С. Огарков // / Вісн. Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна. – Дніпропетровськ, 2011. – Вип. 36. – С. 189.

The second stage is to match the IP address to the designated subscribers (users) of individual Internet intermediaries. For example, in 2010, the Law on Telecommunications was amended in Ukraine, in particular to Part 2 of Art. 39: "Operators, telecommunication providers shall store and provide information about the connection of their subscriber in the manner prescribed by law [5]".

The third stage consists in informing or forwarding the claims to the persons about their copyright infringement and the possibility of filing (or filing directly) against them. This stage is the most difficult because it requires two components to be proven, namely: to establish a connection between the person to whom a particular IP address is delegated and the violation; Proof that the IP address was actually used in unauthorized distribution of works[6].

An important practical problem of identification of the offender is indicated by N. Razigraev. This problem is related to the definition of defendant in online disputes[7].

Thus, according to paragraph 13 of the Information Letter of the Supreme Economic Court of Ukraine "On some issues of the practice of application by the economic courts of information legislation" of March 28, 2007 No. 01-8 / 184, information about the owner of the website may be required from the Limited Liability Company Hostmaster, which currently administers the domain name registration and registration system and the address of the Ukrainian segment of the Internet. Following the implementation of measures related to the delegation of administrative rights, these functions should be performed by the Association of Enterprises of the Ukrainian Network Information Center "(hereinafter referred to as" UMIC")[8].

---

[5] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

[6] Зеров К.О. Ідентифікація особи, що здійснила порушення авторських прав на твори, що розміщені в мережі інтернет за допомогою p2P – мереж / К.О. Зеров [Електронний ресурс]. – Режим доступу: https://www.pdaa.edu.ua/sites/default/files/node/2793/identyfikaciyapoltavazerov.pdf.

[7] Разиграєва Н. Сучасний стан та новели захисту прав у мережі Інтернет / Н. Разиграєва [Електронний ресурс]. – Режим доступу: https://blog.liga.net/user/nrazigraeva/article/22013.

[8] Про деякі питання практики застосування господарськими судами законодавства про інформацію: Інформаційний лист Вищого господарського суду України від 28 березня 2007 року № 01-8/184 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/v_184600-07.

According to Article 56, paragraph 3 of the Law of Ukraine "On Telecommunications", the administration of the Internet address space in the UA domain is carried out by a non-governmental organization formed by self-governing organizations of Internet operators / providers and registered in accordance with international requirements[9].

According to the decree of the Cabinet of Ministers of Ukraine of July 22, 2003 No. 447-p "On domain administration". UA", authority to manage the address space of the Ukrainian segment of the Internet, maintenance and administration of the system registry and system of top-level domain names". UA" carried out by OP "UMIC"[10].

In practice, a person who believes that his or her rights have been violated attempts to obtain information on the domain name registrant (proper defendant) through the WHOIS service. However, such information is often hidden in accordance with the Law of Ukraine "On Personal Data Protection[11]". Also, such persons independently attempt to send appropriate requests to OP "UMIC", and in return may also receive information that the relevant data are hidden domain name registrant in accordance with the Law of Ukraine "On Protection of Personal Data".

Therefore, persons interested in filing a lawsuit apply to the court for a statement of evidence and a statement of precautionary measures (requiring evidence). In addition, the party has the right after filing a claim to request the seizure of evidence.

Even more difficult is the problem of proving a crime through the Internet. Thus, according to V.A. One of the problems that a law enforcement officer faces in investigating crimes committed through the Internet is identifying a computer user of a network from whom criminal activity (cybercrime) was committed. IP-based identification errors (until recently, accounting was the primary method of identification) consist of transmission errors and computer usage errors. For example, when users work through the root server, the entire subnet behind it will, in most cases, have a single IP address. On the other hand, when working through

[9] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

[10] Про адміністрування домену «.UA»: Розпорядження Кабінету Міністрів України від 22 липня 2003 року № 447-р [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/447-2003-%D1%80.

[11] Про захист персональних даних: Закон України від 01.06.2010№ 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

a dial-up connection, the user will receive a new IP address, etc., each time the connection is made[12].

The task of identifying a device is usually solved using unique codes such as MAC or IP addresses on Ethernet networks or IMEIs in GSM networks. However, using a unique code answers the same question or not, but does not tell the exact type of device and how it is used by a specific user. In addition to identifiers, it may be possible to use additional information that is required when processing indirect features, based on the information received from the sensors of the device and as a result of the software running on the device. In this case, it means determining the type of user activity according to global positioning and gyro systems, as well as applying dynamic and static biometrics, such as, vein drawing on the palm, fingerprint, iris, geometry of the hand or face, 3B- skull projection, keyboard handwriting, ear shape, voice and any other distinctive feature can serve to identify a person with a biometric system.

The notion of the imprint of the device should be used in relation to the information remaining on the servers and other devices of registration, and the concept of the imprint of the person in the device to the information that indirectly characterizes the person by the information remaining in the device used by them. An example of a device's fingerprint is the entry in the server's log file, and the person's fingerprint information about the programs used, the time and duration of the programs, a set of used files and other resources.

A special place among the software in terms of the task of identifying the device is the browser, as a program through which the user accesses the majority of Internet-cookies. Cookies are used to identify cookies and installed fonts and plugins. When solving the problem of identifying using indirect attributes, the speed of changing the configurations of the hardware and software used by the user, as well as the biological rhythms to which the person is predisposed, should be considered. Dynamic human biometric characteristics change within six months. Static biometric features persist throughout life.

A file system footprint refers to information about the structure of the file system, not to obtain a mathematical convolution of data in the file system. Particular attention is paid to files older than a month that have not

[12] Світличний В.А. Від ідентифікації комп’ютера до ідентифікації користувача у мережі інтернет / В.А. Світличний // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності. – 2014. – № 3. – С. 151.

been modified during this time. They have sufficient stability to become an identifying feature for a while. It is suggested to use the file name, location, size, creation date and editing date to create a file system imprint.

User information consists of: days of the week, time of use, duration of software activity; recurring typographical errors, parasite words, typing errors; mouse or keyboard events.

The ultimate goal of the study of the task of identifying humans and devices is to build a recognizable, capable of satisfactorily accurate identification. The peculiarity of this device is a constant set of input values, which should be reflected in its internal structure.

Thus, one of the most difficult problems in Internet law is the problem of identifying a user of the Internet. It is of paramount importance when it comes to identifying the offender (not the place where the offense was committed). This identification alone is not enough through the use of an IP address, so additional evidence must be used to establish a causal link between the person to whom a particular IP address is delegated and the infringement.

2. The problem of legal liability of Internet service providers

Since the introduction of broadband Internet in Ukraine, the number of providers providing access to the network has increased hundreds of times. Each user needs a computer, a browser (web browser) and an Internet service provider to connect to the Internet.

An Internet service provider is a company that provides Internet access or an Internet service provider. One of the biggest problems with internet law is one of the biggest problems with internet law – the problem of liability. This responsibility can be diverse. [13]

For example, civil liability arises in the event of a breach of the Internet Service Provider Agreement. For example, SO Yemelyanchyk provides such a definition of liability in an Internet service contract as an obligation to pay a penalty or indemnification of damages and non-pecuniary moral damage or other measures of liability provided for by the contract or civil law, which are entrusted to the parties by Internet service contract for failure or improper fulfillment of its terms[14].

[13] Базові поняття і терміни веб-технологій / [А.В. Кільченко, О.І. Поповський, О.В. Тебенко, О.В. Тебенко, Н.М. Матросова]; Упорядник: Кільченко А.В. – К. : ІІТЗН НАПН України, 2014. – С. 25.

[14] Ємельянчик С.О. Договірне регулювання наданя послуг доступу в Інтернет: автореф. на здобуття наук. ступеня канд. юрид. наук: спец.12.00.03 / Сергій Олександрович Ємельянчик. – Х., 2013. – С. 13.

However, even here the problem is with the types of providers, because the provider can be a regular intermediary – which only provides access to the network, including end-user Internet connection, and can be a provider of information resources belonging to a third party and making them accessible (hosting – provider, content – provider). In addition, there is a so-called cache provider, which provides automatic interim temporary storage of material on the system or the Internet, controlled or managed by the provider[15].

Thus, the Internet access provider (Internet Service Provider) provides a technical base for accessing the Internet (cables, equipment, etc.), that is, creates a data transmission environment, and content providers provide the information content of the Internet (use content that contains objects copyright and related rights). The ISPs have nothing to do with the content process of filling electronic resources online and cannot monitor the extremely large amount of content generated by content providers.

The Law on Telecommunications of Ukraine uses the following terms: a telecommunications provider – an entity that has the right to carry out activities in the field of telecommunications without the right to maintain and operate telecommunications networks and to provide telecommunication channels. The right to such service is granted to a telecommunications operator – an entity that is entitled to carry out activities in the field of telecommunications with the right to maintain and operate telecommunications networks.

The question arises – in which case the provider – the owner of the information resource and information system is responsible for the actions of the persons who used the resources and systems specified?

There are three main approaches to this:

1. the provider is responsible for all user actions, regardless of whether he or she has the right to have knowledge of the actions taken,

2. the provider is not responsible for the users, if he fulfills certain conditions related to the nature of the provision of services and interaction with the subjects of information exchange and persons whose rights are violated by the actions of the users,

3. the provider is not responsible for user actions.

[15] Зеров К.О. Особливості відповідальності інтернет-посередників за порушення авторських прав на твори, розміщені в мережі Інтернет [Електронний ресурс]. – Режим доступу: http://aphd.ua/publication-159/.

According to T.V. Konnov, there are three types of responsibility of Internet providers in the world practice:

1. Strict liability for which the provider is responsible for all user actions, regardless of whether or not he knew of their actions. This approach is mostly applied in countries with authoritarian regimes where the Internet is subject to severe censorship (China, Belarus). An interesting aspect of such responsibility is the need to register (notarize) the creation of sites, the provision of services. A similar but somewhat different approach has been applied in the UK, which, according to the Defamation Bill, provides for providers to commit themselves to "effective control", and when they undertake such a commitment, they are strictly liability for copyright infringement by third parties. The disadvantages of such responsibility are the positive responsibility that the Internet service provider has to check the data with which it deals, and given the speed and volume of data transmission, it is almost impossible. In addition, it violates the privacy of individuals, and may be contrary to the basic principles of the rule of law, to be a tool for imposing censorship.

2. Differentiated liability for which providers are responsible for copyright infringement by third parties only if, after receiving information (complaint / appeal) about such infringement, within the timeframe specified by the law, they have not taken measures to remove such information from such resources. This approach is practiced, for example, in Sweden (Act on Responsibility for Electroinic Bulletin Boards). The problem with the use of such liability is that, at the request of individuals, providers, as practice shows, do not check completely remove legal content, not wanting to be responsible. In addition, the question arises as to how the author of a work (copyright object) can track every infringement that occurs on the Internet. And how much more realistic is it to protect a person's rights when it takes an average of seven days to delete a person's copyright infringement over which that information can be copied and misused many times over?

3. Establishing immunities for providers (essentially not a liability). When providers operate as "free harbors" according to OCILLA (The On-Line Copyright Infringement Liability Limitation Act). They are recognized as such provided that the information is not provided on their own initiative. And they are liable only in the aggregate of the following conditions: if they have received significant benefits from copyright infringement by third parties (significant benefit is an appraisal concept and is determined by the court in each case); if the providers knew, or

could have known about the commission of such violation (here, in essence, we again have the so-called "responsibility without fault", which places on the person). These categories are purely evaluative and often lead to abuse, given that providers are solely responsible for copyright infringement, such rules can be misused to protect their reputation, honor, dignity, etc. (in most countries of the world) the provision that any negative information is considered to be inaccurate unless the person who refers to it proves otherwise – is not valid). In particular, this type of liability can be effective only in countries with a precedent system, since the legislative enabling of such liability allows the courts to evaluate each individual case and, depending on the circumstances, determine its compliance with the criteria of liability[16].

In Ukraine, changes were recently made to Art. 40 of the Law on Telecommunications. According to her operator, the telecommunications provider bears the following property liability to consumers for failure to provide or improper provision of telecommunication services:

1) for not providing paid telecommunication services or providing them in the amount less than paid;

2) for the delay of transmission of the telegram, which led to its non-delivery or late delivery;

3) for unreasonable shutdown of final equipment;

4). for unreasonable reduction or change of the list of services;

5) in other cases – in the amounts stipulated by the contract for the provision of telecommunication services;

6) in case of failure within one day from the fixed moment of submission by the subscriber of a claim for damage to the telecommunication network, which made it impossible for the consumer to access the service or reduced to unacceptable values the quality of the telecommunication service, the subscription fee for the entire period of damage is not charged, and the telecommunication operator damage within five days from the fixed moment of submission by the subscriber of the relevant application pays the consumer a fine of 25 percent of the daily subscription fee for each day of exceeding this term, but not more than three months[17].

---

[16] Коннова Т. Відповідальність інтернет-провайдерів за порушення авторських прав третіми особами / Т. Кононова // Актуальні проблеми міжнародних відносин. – 2011. – Випуск 98. – С. 175.

[17] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

O. Matskevich draws attention to the problem of legal liability of providers for infringement of copyright and related rights on the Internet. The scientist draws attention to the fact that in determining the responsibility of the provider, one must proceed from the subjective composition of the offense:

1. violation committed by the provider;

2. The violation is committed by a user who has been granted access to the network.

In the first case, consider the following:

the violation is intentionally committed, and therefore the provider itself becomes the offender and must bear the statutory liability; violation committed accidentally (technical failure, error). In such a case, it may be compensation or other compensation for the damage caused by the contract. [18]

In the second case it is necessary to proceed from the following:

the provider was unaware of the breach and therefore cannot be held responsible for the commission of the other person; the provider knew about the violation but did not correct it. In determining the liability in this case, the existence or absence of a useful purpose and form of guilt should be considered.

If information that is detrimental to the business reputation of a business entity has been distributed on the Internet site (even if not registered as a media) and the court finds that such information is untrue, then according to the court decision, it must be denied on the same site in accordance with the requirements of the press law.

If the relevant information is disseminated in the form of messages not by the owner of the site, which is freely accessible, but by third parties, who are anonymous, then responsibility for such dissemination of information and damage to the business reputation of the entity has it is the owner of the site who is responsible for the fact that his activity created technological opportunities and conditions for dissemination of negative information that is untrue and violates the rights and legitimate interests of the person.

Due to the fact that the legislation does not clearly resolve the issue, the practice comes to the opposite conclusion. This situation leads to the

[18] Мацкевич О. Загальні підходи до визначення юридичної відповідальності провайдерів за порушення авторських і суміжних прав у мережі Інтернет / О. Мацкевич. // Теорія і практика інтелектуальної власності. – 2012. – №1. – С. 57.

need for a contractual settlement of issues of liability of the provider. However, contracts often state that the access provider is not responsible for the content transmitted by its networks and does not control the transmitted information; the access provider has the right to disconnect the subscriber from the network in cases where the provision of services may endanger the security of the network and/or third parties, or in the case of unlawful actions by the subscriber, as well as in case of non-compliance with the contract or violation of the current legislation of Ukraine. On the other hand, there is a problem with whether providers have the power to prevent an offense. In other words, whether there are grounds for granting the provider the right to disconnect the user, provided that the terms of the contract are violated or the grounds for such actions may be a court decision. Not resolved at the legislative level is the ability of the provider to restrict user access to the network in the case of receiving applications from third parties or in the case of self-detection of violations, as well as what should be understood as access restrictions.

Thus, the problem of provider liability is related to variations of this category of subjects of Internet law. Today there are three approaches to such responsibility: the provider is responsible for all user actions; the provider shall not be liable for the users if it fulfills certain conditions related to the nature of the provision of services and interaction with the subjects of information exchange and persons whose rights are violated by the users; the provider is not responsible for user actions. We believe that the Internet Service Provider, as a company providing access to the Internet, should not be responsible for the content of information contained on the Internet. In doing so, he is legally responsible for the quality of network access. Another situation is with the provider who owns the hosting, Internet resource. In Ukraine it is necessary to use the experience of foreign countries, where the responsibility of the provider is divided into strict, differentiated and immunities.

CONCLUSIONS

The fastest growing industries in the world include electronics, communications, communications, electronic media. This process is so rapid that sometimes the rules of law do not catch up with it. In particular, the legal relations between the processes of human interaction through electronic means of communication, when many actions are carried out not in the real world but in the virtual, are insufficiently developed. Very

often, these actions are outside the legal field: it can be argued that relationships on the Internet today are characterized by a set of loopholes in jurisprudence.

When transferring existing formed relationships governed by the rules of law to the Internet, they are transformed in such a way that the rules that governed them remain, at best, unnecessary due to the impossibility of their practical use.

The Internet needs specially designed legal frameworks that take into account the specifics of real legal relationships in the virtual world. The rules governing Internet relations, owing to the almost ten-year advance of the mass introduction of the Internet into everyday life, have already been largely drafted, however, attempts to directly transpose Western legal norms are inappropriate, because Western common law norms differ greatly from national norms. However, it is worth noting that the Ukrainian rulemaking in this area is quite active, a new kind of law has emerged – information law, several journals are published, theses are defended.

Today, there is no unity of scholars in defining the Internet. It is possible to distinguish a purely technical approach, according to which the Internet is a collection of networks; an information approach whereby the Internet is an information space, and others. We believe that today there is a need to integrate different approaches to the Internet and formulate a comprehensive definition of it. When doing so, it is imperative to consider its legal nature. The attributes of the Internet include mass, accessibility, openness, communicativeness, out-of-space, timelessness, regulatory and more.

Under internet relationships, we suggest understanding the relationships that are associated with the operation of the Internet. Internet – Legal relationships can be defined as public relations that are related to the functioning of the Internet, and members of which are linked by mutual legal rights and obligations protected by the state. The characteristics of Internet relations include the following: digital form, the distance of the subjects, the presence of entities that provide organizational and technical possibility of relations, the use of software, technical standards and protocols, self-regulation, technological complexity, technical, cultural and educational qualification. The subjects of Internet relations are Internet access service providers, information providers, users. The objects of Internet relations are any phenomena that are influenced by the subjects on the Internet. At present, there is no unity in isolating the

varieties of Internet relations. Subjects and objects can be selected as criteria. Highlight the general; organizational (managerial); informational; subject internet relationships.

SUMMARY

The article deals with the peculiarities of legal regulations on the Internet. One of the most difficult problems in Internet law is the problem of identifying a user of the Internet.

It is of paramount importance when it comes to identifying the offender (not the place where the offense was committed). In this case, identifying solely through the use of an IP address is not enough, so additional evidence must be used) to establish a causal link between the person to whom a particular IP address is delegated and the violation of rights.

Internet Service Provider have to do with variations of this category of Internet law entities. Today there are three approaches to such responsibility: the provider is responsible for all user actions; the provider shall not be liable for the users if it fulfills certain conditions related to the nature of the provision of services and interaction with the subjects of information exchange and persons whose rights are violated by the users; the provider is not responsible for user actions.

The Internet Service Provider, as a company providing access to the Internet, should not be held responsible for the content of information contained on the Internet. In doing so, he is legally responsible for the quality of network access. Another situation is with the provider who owns the hosting, Internet resource. In Ukraine it is necessary to use the experience of foreign countries, where the responsibility of the provider is divided into strict, differentiated and immunities.

REFERENCES

1. Базові поняття і терміни веб-технологій / [А.В. Кільченко, О.І. Поповський, О.В. Тебенко, О.В. Тебенко, Н.М. Матросова]; Упорядник: Кільченко А.В. – К. : ІІТЗН НАПН України, 2014. С. 21.

2. Афанасьєв Д. Особливості ідентифікації суб’єкта інтернет-мережевих спільнот // Науковий вісник Ужгородського національного університету. Серія : Педагогіка. Соціальна робота. 2012. Вип. 24. С. 16

3. Жутова С.М. Особливості укладання угод через мережу інтернет // Молодий вчений. 2017. № 11. С. 877.

4. Огарков А.С. Примусова авторизація в мережі інтернет // Вісн. Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна. – Дніпропетровськ, 2011. Вип. 36. С. 189.

5. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. 2004. № 12. Ст. 155.

6. Зеров К.О. Ідентифікація особи, що здійснила порушення авторських прав на твори, що розміщені в мережі інтернет за допомогою p2P – мереж / https://www.pdaa.edu.ua/sites/default/files/node/2793/identyfikaciyapoltavazerov.pdf

7. Разиграєва Н. Сучасний стан та новели захисту прав у мережі Інтернет / https://blog.liga.net/user/nrazigraeva/article/22013.

8. Про деякі питання практики застосування господарськими судами законодавства про інформацію: Інформаційний лист Вищого господарського суду України від 28 березня 2007 року № 01-8/184 // http://zakon.rada.gov.ua/laws/show/v_184600-07.

9. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. 2004. № 12. Ст. 155.

10. Про адміністрування домену «.UA»: Розпорядження Кабінету Міністрів України від 22 липня 2003 року № 447-р // http://zakon.rada.gov.ua/laws/show/447-2003-%D1%80.

11. Про захист персональних даних: Закон України від 01.06.2010№ 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

12. Світличний В.А. Від ідентифікації комп'ютера до ідентифікації користувача у мережі інтернет // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності. 2014. № 3. С. 151.

13. Базові поняття і терміни веб-технологій / [А.В. Кільченко, О.І. Поповський, О.В. Тебенко, О.В. Тебенко, Н.М. Матросова]; Упорядник: Кільченко А.В. – К. : ІІТЗН НАПН України, 2014. С. 25.

14. Ємельянчик С.О. Договірне регулювання наданя послуг доступу в Інтернет: автореф. на здобуття наук. ступеня канд. юрид. наук: спец.12.00.03 / Сергій Олександрович Ємельянчик. Х., 2013. С. 13.

15. Зеров К.О. Особливості відповідальності інтернет-посередників за порушення авторських прав на твори, розміщені в мережі Інтернет // http://aphd.ua/publication-159.

16. Коннова Т. Відповідальність інтернет-провайдерів за порушення авторських прав третіми особами // Актуальні проблеми міжнародних відносин. 2011. Випуск 98. С. 175.

17. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. 2004. № 12. Ст. 155.

18. Мацкевич О. Загальні підходи до визначення юридичної відповідальності провайдерів за порушення авторських і суміжних прав у мережі Інтернет // Теорія і практика інтелектуальної власності. 2012. № 1. С. 57.

Information about the author:
Mazurenko S. V.
PhD in Law, Associated Professor
at the Department of Intellectual Property Law,
National University “Odessa Law Academy”
2, Academychna str., Odessa, 65009, Ukraine