Krakowskie Studia Małopolskie
2021, nr 2 (30)

Alla Bezhevets[1]

Legal Liability for Various Offenses on the Internet

1. Introduction

Almost any relationship that arises in a society involving many persons should be governed by the rule of law. However, the relationship on the Internet is almost unregulated at all, which gave push to a favorable environment for a number of offenses on the Internet.

However, the problem for optimizing the relationship on the Internet is not only the lack of legal regulation, but also the technical problems of identifying the appropriate subject of liability and cross-border transmission of information, which creates serious difficulties in regulating these relationships at the national level.

The purpose of the study is to define ways to find the subjects of legal liability for various offenses on the Internet and to disclosure technical and legal obstacles to such investigations, as well as ways to regulate methods to prosecute offenders in the cross-border nature of crimes on the Internet. To this end, a profound study of the structure of the Internet and possible types of offenses that may be committed there, the legal provisions, as well as scientific works in this area are studied.

[1] Senior Lecturer, National Technical University of Ukraine „Igor Sikorsky Kyiv Polytechnic Institute", ursluzhba@ukr.net, https://orcid.org/0000-0001-5434-3883.

2. The main text

There are many protocols for various online transactions that are approved by private companies, so the law does not regulate the technical aspects related to the placement and dissemination of various information. On the other hand, despite the common belief that entities that provide technical access to information are not legally liable for the content of this network, there are opposing views, including court decisions regarding it. In particular, the European Court of Human Rights and the highest courts of Ukraine have already made decisions to hold the web site owner liable for providing him with the technical ability to disseminate inaccurate information or information that degrades the author's honor, dignity and business reputation[2].

Website owners usually publish the rules for using their sites, indicating, in particular, that the authors of the comments are liable for their comments. At the same time, web site administrators can delete comments themselves, which, for example, contain obscene language (this can be done automatically), offensive address comments and so on. In addition, web sites usually also have a feedback system that allows a person to notify the site administrator of incorrect comments. On the other hand, web sites may have neither feedback nor a system for removing incorrect posts. That is why, there is a question of the need to establish a legal obligation for the site owner to create such security systems on his web site, which has not yet been implemented.

It is very important what kind of web site it is, if it is a social network, than the rules should be of one kind, and for commercial sites – of the other. For commercial sites that sell certain goods and services, there may be issues regarding compliance with the law on advertising, not violating the means of individualization of participants in civil circulations and not misleading consumers (in particular, by artificial responses to their own goods and services). If we are talking about social networks,

[2] Tarnavska M.I. (2015). Spory pro poshyrennia vidomostei u merezhi Internet: superechnosti sudovoi praktyky [Trials on Information Dissemination on the Internet: Contradictions of Case Law]. Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: Yurydychni nauky. № 813. P. 343–349. [in Ukrainian].

then there are two conflicting rights: 1) the right to freedom of expression and 2) the right to protection from libel, dissemination of inaccurate, harmful information and personal data leakage without the permission of their owner. Taking into account that social networks acquire the features of the media, their legal regulation should be similar to the legal regulation of the functioning of the media.

The media are legally liable for the content of the information, and even if there are live calls for the overthrow of the constitutional order or incitement to interracial or interfaith hatred, etc., this may justify applying of certain sanctions to the channel. In addition, TV channels can operate only after the issuance of the appropriate license. There are no such burdens on social networks yet. However, it becomes clear that they need to be gently filtered with content. In the EU, a Rapid Alert System was created in 2019 to combat misinformation and destructive information on the Internet[3]. The concept of destructive (harmful) information, which is unacceptable on social networks, on news sites, etc., requires a coordinated approach at the international level, which can be set out in EU directives. A positive example of attempts to resolve this issue is the Model Law «On Protection of Children from Information Harmful to Their Health and Development», adopted on December 3, 2009 by the Interparliamentary Assembly of the CIS member states[4].

If we consider commercial sites such as e-shops, then, in our opinion, should oblige hosting service providers when creating and indexing the site to require from web site owners duly certified documents on the status of the business entity, verified contact information *due to protect rights of consumers when purchasing goods and services through such web sites*. That is, so that consumers can return or exchange the goods within the period prescribed by law, return low-quality goods and demand compensation for damage, if any, which is almost impossible when

[3] Muzhanova T.M., Yakymenko Yu. M. (2019) Dosvid Yevropeiskoho Soiuzu z protydii destruktyvnii informatsiinii diialnosti v merezhi Internet [The Experience of the European Union in Combating Destructive Information Activities on the Internet]. Suchasnyi zakhyst informatsii. № 2 (38). P. 37–41. [in Ukrainian].

[4] Pro zakhyst ditei vid informatsii, shcho zavdaie shkodu yikh zdoroviu ta rozvytku: Modelnyi zakon, 2009 [On Protection of Children from Information Harmful to Their Health and Development: Model Law, 2009]. URL: http://jurconsult.net.ua/zakony-stran-sng.

the web site owner is unknown or the data provided is not valid. The WHOIS database aims to protect domain names and their uniqueness, and not to verify the authenticity of data provided about the person who registers this domain.

There are other risks on the Internet, such as electronic non-banking payment systems. The fact is that non-bank payment systems can be created by legal entities with the status of financial institutions after obtaining the appropriate license of the National Bank. Only licensed Internet banks can also be created, with the exception of, for example, Monobank, which does not have a banking license, it only provides an online service that gives access to banking services, and banking operations are carried out by Universal Bank[5]. However, there are electronic payment systems that perform settlement operations without obtaining a license from the National Bank, which operate with electronic (rather than non-cash) money. Ukrainian companies cannot be issuers of electronic money[6]. Therefore, in Ukraine, as in other countries where such a ban applies, there are many foreign companies engaged in electronic payments and are issuers of electronic money (MAXI, MoneXy, etc.), not all of which have agreed the rules of their activities with the National banks of the respective countries.

In such cases, there is always a risk of using a non-accredited payment system from their variety, the operator of the electronic payment system may be questionable, or some of the foreign payment systems may be sanctioned, such as Russian payment systems: ЮMoney, QIWI, etc. therefore, funds in the wallets of these payment systems remain frozen. In addition, it is possible to register a domain name, similar to the web page of a well-known Internet bank with a copy of its design in order to steal passwords and funds from the accounts of clients of real

[5] Hovorova K. I. (2020). Mistse sudovo-ekonomichnoi ekspertyzy u protydii shakhraistva z nadannia posluh u nebankivskii sferi cherez Internet [Place of Forensic Economic Expertise in Combating Fraud in the Provision of Services in the Non-banking Sector via the Internet]. Teoriia i praktyka sudovoi ekspertyzy i kryminalistyky. № 22, pp. 461–470. [in Ukrainian].

[6] Polozhennia pro elektronni hroshi v Ukraini, zatverdzhene postanovoiu Kabinetu Ministriv Ukrainy vid 4 hrudnia 2010 roku № 484 [Regulations on Electronic Money, approved by the Cabinet of Ministers of Ukraine of December 4, 2010 # 484]. URL: https://zakon.rada.gov.ua/laws/show/z1336–10#Text.

Internet banks. Finding a person who has registered under someone else's name may not be so easy, and the ability to use VPN technology facilitates anonymity.

The use of cryptocurrencies as funds issued by private persons and not tied to banks or non-bank payment systems that are partially controlled by banks creates risks of excessive fluctuations in cryptocurrencies[7] and even the possibility of stopping their conversion into real currency. Blockchain creates a reliable mechanism for tracking all transactions, but it does not protect against dishonesty of web site owners and the problem of verification of these owners. On the other hand, cryptocurrency provides the possibility of no-commission payments and lack of control by the tax authorities, the latter is a concern, in particular, through the simplification of anonymous financing of terrorist groups.

VPN technology allows you to access different web sites by changing your IP address, which in turn creates even more problems in identifying the person responsible for any, including more serious than economic, crimes. Currently, there are many types of offenses on the Internet that are related to human life and health. It would seem that there is no physical contact between the participants of the Internet communication, so the danger is also virtual. However, the main risk is *in the psychological impact and leakage of personal data.*

In particular, such virtually coordinated games as "Blue Whale", "Run or Die", "Red Owl", "Momo" have collected more than a hundred very real deaths of teenagers, as their ultimate goal is the suicide of a person playing this game. Of course, as a rule, it is the psychological unhappiness in the family, the feeling of loneliness and uselessness that contributes to such victim behavior of teenagers, but leading to suicide is a criminal offense. Finding the subject or subjects who deliberately created and distributed such games is a very difficult task, as they mostly use social networks (Vkontakte, Tick-talk, etc.) under other people's names and avatars, often use Internet cafes, someone else's Wi-Fi coverage and VPN protection.

---

[7] Maramy`gin M. S., Prokof`eva E. N., Markova A. A. (2015). E`konomicheskaya priroda i problemy` ispol`zovaniya virtual`nix deneg (kriptovalyut) [Economic Nature and Problems of Using Virtual Money (Cryptocurrency)]. Izvestiya UrGE`U. № 2 (58), pp. 37–42. [in Russian].

Even mentally balanced adults can suffer from posting their own personal information, because if a person reports a vacation, one can be robbed at that time. By becoming a public figure, bloggers run the risk of falling into the field of view of aggressive opponents of the views they express and becoming the object of both virtual and real persecution.

Bullying, child pornography and child involvement in it, recruitment to sects, distribution of videos of real crimes created solely for the purpose of gaining more views (this is a threatening feature of mass psychological perversions) and other offenses, plenty of which qualify as criminal offenses.

Some types of offenses on the Internet include the creation of viruses to capture personal data, damage to gadgets, etc. It is extremely difficult to find the primary subject who created a certain virus and to prove its guilt. Even more dangerous are cyberattacks aimed at banking institutions, government agencies and, most dangerously, at special regime facilities, such as nuclear power plants.

Nowadays, the concept of theft of virtual property, for which very real money is paid, has appeared. In particular, Valve, the developer of the computer game World of Tanks, sells virtual tanks and other virtual equipment for a considerable amount of money, which can total be hundreds of thousands of dollars per person. Players can sell such a right to permanent use of virtual equipment only with an account. You can top up your wallet on your account in many supermarkets using the Ibox service. At the same time, there are cases of account theft together with the accumulated amounts of funds.

More common offenses on the Internet include hacking other people's e-mail boxes, unauthorized downloading of various intellectual property, gambling through the network, including accepting bets on various sports and other events. In some countries, spam is also prohibited, ie mass mailing of unsolicited (unsubscribed) advertising, or propaganda etc.

A separate type of offense is the use of robotic agents that catch up with clicks on banner advertising, which is paid for by customers of such advertising. The advertising customers transfer a certain amount of money to the account of the advertising executor, and for each event of a potential consumer entering an ads banner, a certain amount of money is charged from the client. However, the use of such robotic

agents leads to the collection of funds from the account of the customer of advertising without entering his ads real people. Such an offense is not recognized as a separate crime in the legislation of most countries, it can be attributed to a type of fraud. In this case, this type of offense is committed with the use of specially equipped computers, which may not be in the person's home, so to track them and bring the offender to justice is a very complicated case. In addition, the use of such computers is not a separate offense without proving that the offenders have received funds for such activities.

There are two main problems in prosecuting offenders online:

1) The difficulty of identifying a subject of liability who may use VPN, Tor, I2P or even when determining the IP address of the offender one can not always identify which of the users of the server committed illegal acts (because the subject of liability – an individual, not family members or employer);
2) A person who is physically in one country may commit a crime in another country and will not be subject to the jurisdiction of that country.

There are scientific proposals to decide problem of cross-border offences on the Internet. One of the most interesting solutions is the creation of a non-governmental international court on the Internet[8]. Of course, the sanctions of such a court will concern the blocking of the violator's activity on the Internet. Therefore, in our opinion, in relation to criminally punishable offenses, it is worth establishing cooperation between the Internet court and state or international courts, which may apply sanctions in the form of imprisonment, etc. However, various organizations operating under certain technical network protocols can assist the court in identifying the person-offender and his locating. An intergovernmental agreements can regulate the extradition of offenders from one country to another or the obligation to bring a person to justice in their own country.

It should be noted that if we talk about crimes on the Internet, the number of such crimes committed through web sites indexed in Google and other search engines is much smaller than via the so-called Dark

[8] Xiabing Li, Yongfeng Qin (2018), Research on Criminal Jurisdiction of Computer Cybercrime. Elsevier. Procedia Computer Science. 131, pp. 793–799.

Web, which is hidden from indexing in search engines. It is there that drug, arms trafficking, murder orders, child pornography are distributed, terrorism is financed and human trafficking takes place. For example, Silk Road is one of the most powerful organized drug trafficking markets operating on the Dark Internet. All payments are made using cryptocurrencies, so it is extremely difficult to identify people who are buyers or sellers of illegal goods, as they act under other people's names, without identification from non-indexed web sites and do not leave other physical traces, such as fingerprints, image capture and more.

In this case, the cyberpolice and the regular police must work together to carry out, in the first instance, investigative actions with the information they can obtain from victims of such crimes and try to act undercover as potential customers of illegal services and goods through links that are thrown into some social networks. With such painstaking work, it is sometimes possible to find the e-mail addresses of criminals or even their fingerprints on drug packages.

3. Conclusions

To solve the problem of liability of offenders on the Internet it should be required by law that hosting providers and other organizations that provide domain names must request information about the owners, along with certified copies of passport documents or registration documents of legal entities – owners of relevant web sites, establishing the procedure for transferring rights to web site to other persons. This will make it easier to identify those liable for online violations that come from web sites that are indexed by search engines. The possibility of creating a non-state international court on the Internet seems to be a fairly natural solution for regulating relations, which due to its cross-border nature cannot be resolved in any other way. Along with technical protocols should be created the integrity protocols of the network, which such a court will be governed with when making appropriate decisions. It is now almost impossible to track crimes on the so-called Dark Internet, where sites are not indexed by search engines, which raises legal questions about its ban and finding ways to technically implement such a solution.

References

Hovorova K.I. (2020), Mistse sudovo-ekonomichnoi ekspertyzy u protydii shakhraistva z nadannia posluh u nebankivskii sferi cherez Internet [Place of Forensic Economic Expertise in Combating Fraud in the Provision of Services in the Non-banking Sector via the Internet]. Teoriia i praktyka sudovoi ekspertyzy i kryminalistyky. [in Ukrainian].

Maramy'gin M.S., Prokof'eva E.N., Markova A.A. (2015), E'konomicheskaya priroda i problemy` ispol`zovaniya virtual`nix deneg (kriptovalyut) [Economic Nature and Problems of Using Virtual Money (Cryptocurrency)]. Izvestiya UrGE`U. [in Russian].

Muzhanova T.M., Yakymenko Yu. M. (2019), Dosvid Yevropeiskoho Soiuzu z protydii destruktyvnii informatsiinii diialnosti v merezhi Internet [The Experience of the European Union in Combating Destructive Information Activities on the Internet]. Suchasnyi zakhyst informatsii.

Pro elektronni hroshi v Ukraini: Polozhennia, zatverdzhene postanovoiu Kabinetu Ministriv Ukrainy vid 4 hrudnia 2010 roku № 484 [Regulations on Electronic Money, approved by the Cabinet of Ministers of Ukraine of December 4, 2010 # 484]. URL: https://zakon.rada.gov.ua/laws/show/z1336–10#Text

Pro zakhyst ditei vid informatsii, shcho zavdaie shkodu yikh zdoroviu ta rozvytku: Modelnyi zakon, 2009 [On Protection of Children from Information Harmful to Their Health and Development: Model Law, 2009]. URL: http://jurconsult.net.ua/zakony-stran-sng

Tarnavska M.I. (2015), Spory pro poshyrennia vidomostei u merezhi Internet: superechnosti sudovoi praktyky [Trials on Information Dissemination on the Internet: Contradictions of Case Law]. Visnyk Natsionalnoho universytetu „Lvivska politekhnika". Seriia: Yurydychni nauky. [in Ukrainian].

Xiabing Li, Yongfeng Qin (2018), Research on Criminal Jurisdiction of Computer Cybercrime. Elsevier. Procedia Computer Science.

Summary

The article examines the main types of possible offenses on the Internet and the existing problems in identifying those liable for these offenses. At the same time, the cross-border nature of offenses in the network and ways to solve problems with bringing individuals to justice for such crimes are taken into

account. The issues of liability of web site owners, administrators of social networks, operators of non-bank electronic payment systems, distributors of virtually coordinated dangerous games and other subjects are considered. In addition, the article analyzes the difficulties in identifying the subject of liability for offenses in the network when they use VPN technology, private network Tor, non-indexed sites that are part of the Dark Internet.

Also, the offenses that arose with the advent of the Internet, such as theft of virtual property, fraudulent enrichment on clicks by robotic agents, and others are investigated. The proposal to create a non-governmental international court on the Internet to block the violator's activity in network is being considered.

Keywords: liability of web site owners; social networks; electronic payment systems; virtually coordinated games; theft of virtual property; Internet court; Dark Internet