Legal Mechanism of Counteracting Information Aggression in Social Networks: from Theory to Practice

Andriy Peleschyshyn[1][0000-0002-5022-0410], Tetiana Klynina[2][0000-0002-0334-9852], and Sergiy Gnatyuk[2] [0000-0003-4992-0564]

[1] Lviv Polytechnic National University, Lviv, Ukraine
[2] National Aviation University, Kyiv, Ukraine
apele@ridne.net, tklynina@gmail.com, s.gnatyuk@nau.edu.ua

Abstract. An open public discourse is one of the basic conditions of democracy, because this is how citizens can discuss their common matters, form political opinions and ultimately reach a decision for themselves. To have a lively and rational discourse, media freedom, individual freedom of expression and the right to receive information are equally needed. Today's media environment gives individuals the chance to express their ideas at every possible instance – in this respect, the pluralism of ideas is overwhelming. This overwhelming volume of information makes navigation and access to trustworthy information a hard task. Today social networks created a new public space that can be flexibly utilized to get any message to selected parts of the audience. It has no national boundaries, a feature that can be used not only for good purposes, but often for bad ones such such as slander. The article is noted that social networks act as a separate sphere for the emergence, change or termination of civil legal relations, therefore the urgent question is to clarify the application of the legal mechanism in the fight against information aggression, which includes the following components: the discovery of inaccurate information, which is not just an appraisal judgments, but frankly slander outlining the range of probable defendants; making an application to the court in accordance with the requirements of national legislation; proving the fact of unreliability by providing evidence.

Keywords: Social Networks, Informational Aggression, Legal Mechanism, Network laws.

1 Introduction

The process of informatization in the late XX - early XXI century was marked by the emergence of an innovative social phenomenon - social networks, which at the stage of its formation were used primarily for communication and entertainment. However, now we see that social networks have become not only a complete tool for doing business, but also a means of popularizing and representing state authorities, educational institutions, enterprises, public figures, etc., due to the presence of a target audience in networks that is often highlighted today aggression in it. Every day mil-

lions of Internet users leave aggressive on-line comments on social networks such as Facebook, Twitter, YouTube, etc., to voice public criticism, personal indignation or simply release pairs.
In many cases, these comments include rough remarks and addressed to companies, public and state figures, ordinary people, adolescents and others. The forms of such verbal information aggression are diverse and different from expressions of disgust and contempt to defamation, insults and hatred. In relationships that arise in social networks are governed primarily by local acts of these networks, which establish the basic rules for their use.
The social networks themselves are usually not responsible for violating the rights of others, as they are explicitly mentioned in user agreements during registration. In this regard, the question often arises: should react and respond to aggression and how to do it correctly? And since social networks today act as a separate sphere for the emergence, change or termination of civil legal relations, therefore the question becomes the construction of an algorithm of action within the legal field.

2 Related Works

Social networks as a phenomenon of modern society were investigated by foreign scholars such as D. Bell, M. Castells, A. Toffler, A. The problems of the formation of social networks, their main provisions and the principles of their use are devoted to the works of D. Westerman, B. van der Heide, C. Tonga, L. Langwell, J. Kim, J. Antony.
A number of Ukrainian scholars have studied the issues of communication, communicative environment and dialogue in social networks. In particular, A.M. Peleshchyshyn, R.O. Korzh, O.V. Markovets, etc., in their previous studies proposed a classification of mechanisms for protecting the reputation of information media entities in social networks from deliberate targeted compromise, in particular for institutions of higher education.
We do not see any fundamental restrictions on extending the scope of this classification to a wider range of entities, such as public organi-zations, government agencies, commercial entities and private individuals in particular.
However, unfortunately, the specified work does not detail the tools of each class and does not define clear rules and scenarios for its application. That is why the specific possible tools of each class will be explored, the conditions of their application, and the indicative schemes of scenario layout between them. Let's now detail the legal tools.
According to Article 3 of the Constitution of Ukraine, a person, his life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value, which in itself enshrines the duty of everyone not to encroach upon the honor and dignity of other people [20].
Also, according to Art. 201 of the Civil Code of Ukraine (hereinafter - CCU) honor, dignity and business reputation relate to personal non-property benefits, are intact and subject to judicial protection, which is regulated by Art. 297 CCU [19].

Thus, an individual who has suffered as a result of the distribution of inaccurate information, within the legal field has the right to reply, as well as to refute such information.
However, the following differences should be taken into account:

a) when refuted, distributed information is considered to be inaccurate, and in the exercise of the right to reply - a person has the right to cover his or her own point of view regarding the widespread information and circumstances of violation of personal non-property rights without acknowledging it to be unreliable;
b) falsifies the person who disseminated it inaccurate information, and the answer is given by the person in respect of which the information is disseminated [20].

3 Legal Mechanism Of Counteracting Information Aggression In Social Networks

The legal mechanism of counteracting information aggression in social networks is based on the use of the legal framework of the state, legal acts regulating the spheres of information activity and the Internet. A typical example of such an instrument is the appeal to law enforcement agencies regarding the detention of slander in social networks.
However, it should be noted that direct access to such law enforcement agencies as the police or the prosecutor's office, in most cases, will not result in any of the desirable ones for the applicant. This is due to the fact that after the cessation of the validity of the Criminal Code of Ukraine of 1960, which was replaced by the Criminal Code of Ukraine in 2001, from the criminal law, such a crime as defamation has disappeared, since it was not included in the new code that, in essence, made him more progressive and guaranteed the right to freedom of expression guaranteed by the Constitution [13].
In addition, in Ukraine today there is practically no legislative framework to deal with certain threats spreading in social networks, which weakens the possibility of attracting legal instruments. Thus, in the text of the key law in this area "On the main principles of providing cyber security of Ukraine", directly in the text (item 3 of Article 2) excluded from the objects of attraction of the law (hereinafter quoted) «social networks, private electronic information resources on the Internet (including blog platforms, video hosts, and other web resources)» [3].
However, the very term "slander" has been preserved in other legislative acts, in particular in the Law of Ukraine "On Information" (defined by the notion of appraisal judgment) [1] and in the Constitution of Ukraine (Part 1, Article 80), which gives grounds for appeal to the court [23].
However, in order to go to court, it is first necessary to find out whether the legal structure of the offense, in the presence of which your claim will be satisfied, in other words, to understand whether the information is false only evaluative judgments, that is, the thought or assumption of a person who is not can be a subject for refutation.

If it was found that false information is still a slander, we move on to the second stage, where it is necessary to clearly identify who will be the defendant in the case. Since we are talking about material as information that is posted on the social network and treated by us as a slander, insult, cybersquatting, humiliating our honor and dignity, etc., there may be some problems with the defendant's definition.

Defendants in a case concerning the defense of dignity, honor, or business reputation are natural or legal persons who have disseminated inaccurate information, as well as the author of this information. All would be nothing, if the author or distributor of defamation, he is also a potential defendant, a person is known. But we are talking about social networks, where the "creator" of inaccurate information can hide under the pseudonym, or may not be indicated at all.

But, for example, in accordance with the Facebook Terms of Service, the user undertakes not to place inaccurate information in the account; in addition, there is a direct obligation to specify accurate information and to constantly update it. However, in reality, service providers do not have time to monitor compliance with these provisions, which again provides a field for maneuvers from the side of users.

If the author of the information is unknown or his identity and / or place of residence (location) cannot be established, and when the information is anonymous and access to the network is free, the proper respondent in this case becomes the owner of the social network or the website where the specified informational material, since it created the technological opportunity and conditions for the distribution of inaccurate information. To bring the owner of the network accountable, it must be proved that the controversial information was disseminated precisely on this network [20].

Today, however, social networking owners are trying to limit their responsibility for the information that is posted on the network. In addition, social networks often point out at the same time that they refuse to be liable in such cases.

For example, in the already mentioned Facebook Terms of Service, which, before the registration, according to the general rules, the user must read and accept, the (further quotation) states ("the quotation) that" we do not control the actions and statements of people and others, we do not direct them and we do not bear responsibility for their actions and behavior (on the Internet and outside the Internet) and any content they share (including offensive, inappropriate, obscene, illegal or illegitimate for other reasons)» [8].

The situation with the responsibility of the website owner is even more interesting. If the owner of the website is unknown, the data on him may be requested by the administrator of the system of registration and registration of domain names and addresses of the Ukrainian segment of the Internet.

However, all this is possible if the domain is registered in Ukraine and there is access to information about the owner of the website. In case if the domain is registered not in Ukraine and there is no access to the information about the owner, the injured person may apply to the court in a separate proceeding with a statement on the establishment of the fact of inaccurate information.

But, this option has several drawbacks: first, the burden of proof from the defendant is automatically translated into the applicant, that is, the non-distributor of inaccurate information has to prove the truthfulness of the information; on the contrary, the

plaintiff must prove that the information disclosed about him is defamatory; and secondly, it bears the costs of refuting this information; thirdly, the mere fact that the information is unreliable cannot solve the problem of its dissemination and will not automatically lead to the deletion of this information.

But in a situation where the anonymous material is published, the domain name is registered in another country to a private individual, or it may even be on the wagon, which is not possible to set, this is probably the only way out.

The next step in implementing the legal method is to file a lawsuit in a court that must meet certain requirements. Such an application must contain, in particular, information on how the information that violates the personal non-proprietary rights of the plaintiff (the applicant) is disseminated, which information is distributed by the defendant (respondents), indicating the time, method and persons to whom such information has been communicated.

Other circumstances of a legal significance, references to evidence to support each of these circumstances, as well as indication of the method of protection in which the plaintiff wishes to protect his or her violated right.

However, directly in the courtroom, during the hearing on the merits, the plaintiff will have to prove that this information has become known to at least one third person. It does not matter how the person received the indicated information (read, saw or heard).

Secondly, you will need to prove that this information relates to you. In order for the information to have a relationship with a particular person, it does not necessarily have to be given her last name - it is enough that this information contains certain signs, from which it becomes obvious who it concerns.

Thirdly, it will be necessary to prove that the information given is false and violates your personal non-proprietary rights. It is the providence of the latter fact that is the main reason for the satisfaction of the claim, as it happens when the court refuses to satisfy the claims, because it does not see the violation of the right to respect for honor and dignity, because of the fact that valuation judgments, except for insult or slander is not subject to judicial protection.

However, to prove that the disseminated information is unreliable, certain evidence needs to be provided. In accordance with clause 5 of Art. 177 of the Civil Procedure Code of Ukraine, the plaintiff is obliged to add to the statement of claim all evidence available to him that confirms the circumstances on which the claims are based (if the plaintiff can file written or electronic evidence, he may add a copy of the relevant evidence to the claim statement) [19].

Previously, information that was posted on the social network was submitted to the court most often in paper form (printouts of the user's page or screenshot) and was one of the types of written evidence.

However, this issue was followed by a lack of unity among judges. Some courts accepted this evidence, investigated, evaluated and taken into account when making a decision.

Others did not accept the printed content of the pages in social networks as valid and admissible evidence, explaining that the printouts of pages from the Internet do not prove the fact of the placement of the relevant information, and most importantly, the

person who placed the information. That is, the special attention in this case caused the possibility of identifying the person who created and published the information (post, comment, letter, etc.).
This was due to the fact that social networks can register any person and under any name, and therefore the given name or login does not allow identification of the person. That is why the court, for the most part, came to the conclusion that such evidence is inappropriate and permissible, since it does not include identification of individuals. However, with the adoption of new legislation, and the emergence of a new type of evidence-electronic, it would seem that the problem of the correct use of this evidence in the trial should have disappeared, but in practice this had the opposite effect. Of course, Art. 100 of the Civil Code of Ukraine states that electronic evidence is information in an electronic (digital) form that contains the circumstances relevant to the case, in particular:

- electronic documents (including text documents, graphic images, plans, photographs, video and audio recordings, etc.),
- websites (pages),
- text,
- multimedia
- voice messages,
- metadata,
- databases,
- other data in electronic form.

Such data may be stored, for example, on portable devices (memory cards, mobile phones, etc.), servers, back-up systems, and other places of data storage in electronic form (including the Internet) [22].
However, the courts continue to make collisional decisions, noting that such evidence does not have the requisites, which confirms their integrity. However, some materials of the judicial practice indicate the recognition of such evidence, provided that there are no objections from other persons involved in the case [12].
The next gap relates to the problem of defining the concept of "original" and "copy" of electronic evidence, which are still undisclosed. In addition, paper copies of electronic evidence must be certified in the manner prescribed by law.
In Art. 75 of the Law "On Notary" there is a norm which grants the right to notaries and officials of local self-government bodies who carry out notarial acts to certify the authenticity of copies of documents [4]. But is there a web-screenshot of this kind of document? In the opinion of many scholars, a webpage cannot be identified with such a document, since such documents must contain the name of the business entity, the date, the signature of the authorized person, and in some cases the seal. In addition, the web page does not always contain a link to the subject that uses the website [12].
Accordingly, Ukrainian notaries are denied the implementation of the web-site review protocol because of the lack of such a notarial act in the Law "On Notary" and in the Procedure for Notarial Acts by Notaries of Ukraine [4; 14].

Also, problems may arise when submitting copies of electronic evidence, such as photographs, since the courts do not accept such evidence in connection with the violation of their requirements.
If the plaintiff decides to use his legitimate right to protect himself from compromised information, he should pay attention to all of it advantages and disadvantages (see Table 1).

Table 1. Advantages and disadvantages of the legal mechanism.

Advantages of the legal mechanism	Disadvantages of the legal mechanism
– obligatory performance of the obtained results and the quality of their reliability; – application of legal and force resources of the state, including punitive possibilities (civil and criminal liability of the aggressor); – lack of notion of limitation, which makes it possible to seek protection of their non-new rights at any time after the discovery of aggression; – informally constructed social image of "a person, institution or organization that is dangerous to attack"; – an international tendency to increase the responsibility of the community administration for the aggressive actions of individual participants.	– high cost of application (lawyers' services, etc.); – the statement of unreliability of the information will not solve the problem of its dissemination and will not automatically lead to the deletion of this information; – the lack of a clear legal definition between the notion of "judicious judgment" and "false information", which allows the law to be used arbitrarily; – frequent ambiguity of interpretation of results and low efficiency in the conditions of anonymity – the statement of unreliability of the information will not solve the problem of its dissemination and will not automatically lead to the deletion of this information; – complexity in implementation in the distributed environment, which is regulated by the legislation of different countries; – slow deployment and implementation – the fact that the destruction of information on the network in the future makes it impossible to prove the fact of the offense.

However, more effective in this case will be the focus not on the advantages or disadvantages, but on compliance with the rules and the algorithm of the application of the legal mechanism.
Taking into account the correct observance of the proposed algorithm of action (see Table 2), a court may compel a person who disseminated false information to refute

them within a month from the date of the decision. In other words, in our case, if such information was distributed on a page in the social network, its refutation should be placed in the same way.

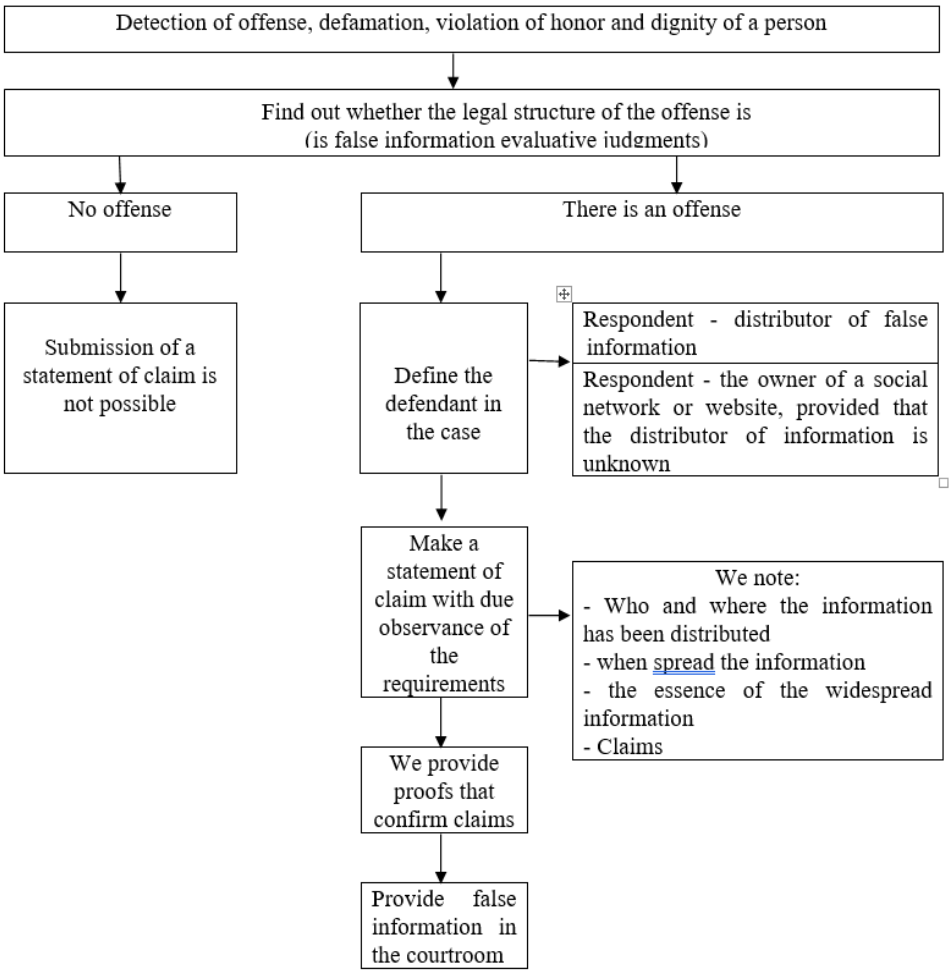

Fig. 1. Algorithm for the application of the legal mechanism.

4 Conclusions

The right to protection is a constitutional right of a person. The exercise of the right to protection at its discretion means that the right-holder has the opportunity to choose the type of conduct - to exercise or not to exercise his right to protection, to choose the forms and methods of protection of the violated right. Civil legal relations in social networks have their own peculiarities, which are connected with the specific vir-

tual sphere of their occurrence and peculiar subjective composition. This is due to the complexity of legal regulation of various types of civil relations that exist in the field of social networks. The common problem is that each network currently has its own terms of use, which usually protects service owners from liability for violating rights, freedoms and legitimate interests in this area. However, despite this, offensive speeches should not be left out of the attention of the person they are concerned and need to be addressed by appropriate legal means, which in turn may become a deterrent to the person being subjected to further dissemination of offensive information character.

References

1. About information: The Law of Ukraine, http://zakon0.rada.gov.ua/laws/show/2657-12, last accessed 2019/05/01.
2. Al-Mhabis, N., Cunningham, H.: Socio-political perspectives on surveillance and censorship: Implications for on-line privacy in the age of cloud computing. In: Proceedings of Computing Conference, pp. 208–213. London (2017).
3. About the basic principles of ensuring cyber security in Ukraine: the Law of Ukraine, http://zakon3.rada.gov.ua/laws/show/2163-19, last accessed 2019/05/01.
4. About the notary: The Law of Ukraine, https://zakon.rada.gov.ua/laws/show/3425-12, last accessed 2019/05/05.
5. Chip Stewart, D.R.: Social media and the law: A guidebook for communication students and professionals. In: Social Media and the Law: A Guidebook for Communication Students and Professionals, pp. 1–234. Taylor & Francis (2013).
6. Eltgroth, D.: Best Evidence and the Wayback Machine: Toward a Workable Authentication Standard for Archived Internet Evidence. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4467&context=flr, last accessed 2019/05/08.
7. Eltgrowth, D. R.: Best evidence and the Wayback Machine: toward a workable authentication standard for archived Internet evidence. Fordham L. Rev. 78, 181 (2009).
8. Facebook Terms Service, https://www.facebook.com/terms.php, last accessed 2019/05/08.
9. Gathegi, J.N.: Social media networking literacy: Rebalancing sharing, privacy, and legal observance. Springer, Cham (2014).
10. Henderson, M., de Zwart, M., Lindsay, D., Phillips, M.: Legal risks and social networking: Removing the blinkers on cyber safety. In: From Cyber Bullying to Cyber Safety: Issues and Approaches in Educational Contexts, pp. 133–148. Nova Science Publishers Inc, New York (2013).
11. Korzh, R., Peleshchyshyn, A., Fedushko, S., Syerov, Y.: Protection of University Information Image from Focused Aggressive Actions. In: Szewczyk, R., Kaliczynsra, M. (eds.) Advances in Intelligent Systems and Computing: Recent Advances in Systems, Control and Information Technology, SCIT 2016, vol. 543, pp. 104–110. Springer, Poland (2017). DOI: 10.1007/978-3-319-48923-0_14.
12. Marits, D.: Legal regulation of the fixing of legal facts in the information sphere. Informational Law 6, 231–237 (2018).
13. Mudra, I.: Social networking on the Internet as a tool for promotion “infected” information. TV and radio journalism 14, 210–213 (2015).

14. On Approval of the Procedure for the Performance of Notarial Acts by Notaries of Ukraine: Order of the Ministry of Justice of Ukraine, https://zakon.rada.gov.ua/laws/show/z0282-12, last accessed 2019/05/08.
15. Ookita, Y., Fujita, S.: Effective suppression of false rumors in social network service. In: The 5th IEEE International Symposium on Computing and Networking, pp. 243. Aomori, Japan (2017).
16. Peleshchyshyn, A., Vus V., Markovets O., Albota S.: Identifying Specific Roles of Users of Social Networks and Their Influence Methods. In: Proceedings of the 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2018, pp. 39–42. Lviv (2018). DOI: 10.1109/STC-CSIT.2018.8526635.
17. Resolution of the Supreme Court of Ukraine "On Judicial Practice in cases concerning the protection of the dignity and honor of an individual, as well as the business reputation of a natural person and a legal entity", https://zakon.rada.gov.ua/laws/show/v_001700-09, last accessed 2019/05/01.
18. Song, M., Zhu, Z., Liu, S., Fan, H., Zhu, T., Zhang, L.: Effects of aggressive traits on cyberbullying: Mediated moderation or moderated mediation? Computers in Human Behavior 97, 167–178 (2019).
19. The Civil Code of Ukraine, https://zakon.rada.gov.ua/laws/show/435-15, last accessed 2019/05/07.
20. The Constitution of Ukraine, https://zakon.rada.gov.ua/laws/show/254%D0%BA/9%D0%B2%D1%80.
    The EU Code of conduct on countering illegal hate speech, https://ec.europa.eu/info/policies/justice-and-fundamental-rights .
21. Korobiichuk, I., Fedushko, S., Juś, A., Syerov, Y.: Methods of Determining Information Support of Web Community User Personal Data Verification System. In: Szewczyk R., Zieliński C., Kaliczyńska M. (eds) Automation 2017. Advances in Intelligent Systems and Computing, vol. 550, pp 144–150. Springer (2017). DOI: 10.1007/978-3-319-54042-9_13.
22. Korzh, R., Peleschyshyn, A., Syerov, Yu., Fedushko, S.: The cataloging of virtual communities of educational thematic. Webology 11 (1), article 117 (2014).
23. Korzh, R., Fedushko, S., Peleschyshyn, A.: Methods for forming an informational image of a higher education institution. Webology 12(2), article 140 (2015).