UDC 343.6.343.9
DOI: 10.32518/sals1.2024.202

Соціально-правові студії. 2024. Т. 7, № 1
Social & Legal Studios. 2024. Vol. 7, No. 1

Practice-based methods of bringing to legal liability for anonymous defamation on the Internet and in the media

Liana Spytska*
Doctor of Psychological Sciences, PhD in Law, Professor
Kyiv International University
03179, 49 Lvivska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-9004-727X

Abstract. As of 2024, the need to coordinate generally accepted standards on legal liability for anonymous defamation in the virtual space of the Internet and the media is becoming more relevant in the context of rapid technological development and digital transformation. Therefore, the study aims to identify the most common and effective approaches to bringing liability for the dissemination of false information in the virtual space of the Internet and the media. A variety of scientific and legal methods were used to achieve this goal, in particular comparison, forecasting, generalisation, system analysis, formal legal, formal logical and other methods. The author analyses the controversial aspects related to the protection of individual dignity, honour and commercial reputation of individuals in the context of the Internet, covering the basis for the emergence of legal relations in this area and the practical challenges faced by individuals seeking to protect their rights to dignity and commercial reputation violated by the dissemination of information on the Internet which is considered to be biased or inaccurate. The study shows that most national courts today reject claims aimed at protecting privacy on the Internet and do not recognise the information disseminated through this channel as unreliable, without requiring its refutation. Recommendations that can be implemented in practice to bring individuals to legal liability for false information disseminated anonymously on the Internet and in the media are developed and justified in this study. The author suggests practical ways that can be used to exert legal influence on persons who commit anonymous defamation on the Internet and the media

Keywords: dissemination of false information; humiliation of honour and dignity; protection of business reputation; disinformation on the Internet; reliability of information

Introduction

The fundamental rights of an individual in the digital space include not only the freedom to create, collect, store and disseminate information but also the right to receive complete, timely and reliable information about events and phenomena. Thus, according to Articles 2 and 3 of the Constitution of Ukraine (1996), as well as Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), everyone has the right to freedom of expression. Therefore, it is necessary to devote particular attention to the legal regulation of the dissemination of reliable information in this digital environment.

This issue has already been addressed by many scholars and researchers. For instance, S. Bevz and O. Samchynska (2021) analysed the provisions of Article 173-1 of the Code of Ukraine on Administrative Offences, which relates to liability for spreading false rumours, and identified several shortcomings in its application in modern conditions. In analysing this problem, this problem was found relevant due to a discrepancy in determining the objective side of the violation due to the presence of various subjective assessment categories, such as "unconfirmed rumours", "panic" and "public disorder".

M. Blikhar (2023) addresses the legal framework for the protection of personal data on the Internet in his research. He points out that despite the existing legal framework, recipients of personal data do not always comply with legal requirements in full or selectively. Thus, the problem of personal data protection on the Internet remains relevant for all parties interested in this issue: data subjects, recipients and the state. The low level of digital literacy among Internet users is the main reason for this problem. Many individuals are not sufficiently familiar even with the basic principles of legal and technical means of protecting their data, which are necessary to prevent their illegal use without their proper consent. The role of the state in this context is to create and ensure the effective functioning of the legal and regulatory framework for the protection of personal data on the Internet.

Suggested Citation **Article's History**: Received: 23.11.2023 Revised: 26.02.2024 Accepted: 28.03.2024

Spytska, L. (2024). Practice-based methods of bringing to legal liability for anonymous defamation on the Internet and in the media. *Social & Legal Studios*, 7(1), 202-209. doi: 10.32518/sals1.2024.202.

*Corresponding author

O.M. Kukh and A.M. Kukh (2021) address topical issues of court practice in cases of dissemination of false information. Thus, the author outlines the existing trends in case law in this category. The author proposes to improve liability for dissemination of false information, considering the case law, by: reasonable enforcement of court decisions for each method of legal protection of subjects (refutation of inaccurate information, removal of websites from it, publication of a full court decision along with refuted information or use of several of these measures); a clear definition of the concept of "false information" in the legislation; proceedings under Article 173-1 Code of Ukraine on Administrative Offenses (1984).

Awareness of the basic algorithm of actions in case of dissemination of false information will help protect rights and restore reputation more efficiently. M. Pakhnin (2023) conducted a study analysing the legal aspects of journalists' activities, in particular the criminalisation of defamation. One possible way to address this problem is to establish criminal liability for defamation. However, in the current Ukrainian context, there is a lack of effective application of the law, which does not meet the standards of protection of human rights and freedoms. Such conditions may lead to the use of defamation legislation to restrict freedom of speech, and a similar reason may be found in other articles of the Criminal Code of Ukraine.

V. Romanova *et al.* (2021) argue that public opinion of active social groups in modern society is formed upon subjective rather than critical analysis of the information received. The process of development and implementation of new legislative acts aimed at regulating the status of subjects of information relations on the Internet and establishing the grounds for their liability is also the subject of the study. The problem of dissemination of inaccurate information through the media and the Internet is addressed by the laws of Ukraine regulating public relations in the field of information dissemination, following the Civil Code of Ukraine.

S. Onyshchenko *et al.* (2023) addressed the possibilities of developing and implementing new legal norms aimed at regulating the status of subjects of information relations in the online environment and establishing the grounds for their legal liability. The results of the analysis show that enhancing personal data protection in times of crisis requires an integrated approach that includes regulatory, organisational and communication measures. For instance, it is necessary to improve data protection legislation in the context of modern technological dynamics, as well as to introduce mechanisms of international cooperation to effectively address this issue and support education and awareness raising of citizens and organisations on data protection.

L. Arbatman and J. Villasenor (2022) conducted a detailed analysis of the current legal framework governing personal data protection, focusing on its relevance in the context of technological progress and digital transformation. This approach identified key aspects of legal regulation in this area and established the need for further legislative initiatives or improvements.

Despite the widespread interest in this topic among legal researchers, there is a need for further scientific research on this phenomenon. Thus, it is possible to argue that the dissemination of false information about a person, including through the media and the Internet, is becoming increasingly relevant both in practice and among academic groups. Therefore, the study aims to examine and identify effective strategies for bringing individuals to legal liability for spreading anonymous accusations, through the media and the Internet.

Materials and methods

A wide range of different methods was used to establish practical ways of bringing to legal liability for anonymous defamation on the Internet and in the media, including comparison, forecasting, generalisation, system analysis, formal legal, formal logical and other methods. Thus, the comparative method was used to analyse the experience of the United States of America and Germany in regulating and resolving disputes related to defamation on the Internet and in the media. This method was used to identify similarities and differences in legislation, judicial practice and approaches to solving the problem in two different countries.

The systematic analysis method was also used to compile different approaches to understanding defamation and to expand the classification of threats to personal data security, especially in martial law, to analyse them more deeply, their origin and types. This method was also used to identify the factors that determine the specifics of protecting a person who has been the subject of false information on the Internet or in the media and to identify factors that affect the protection of a person who has been the subject of defamation or false information on the Internet or in the media. The overall objective of this method is to improve knowledge of the nature of defamation and threats to personal data security, especially in conflict situations, and to develop more effective strategies for protecting this data.

The formal legal method was used to systematise the key provisions of the legal acts regulating the functioning of the legal mechanism for personal data protection. This method was used to assess the current state of the problem and identify opportunities for improving practical measures to bring justice for disseminating false information about a person on the Internet or in the media. The formal logical method was used to formulate key conclusions and recommendations for improving the effectiveness of the existing methods of legal liability for anonymous accusations on the Internet and in the media.

The forecasting method was used to explore various approaches to the protection of personal data on the Internet and to identify relevant areas for improving the legal mechanism aimed at protecting personal information under martial law in Ukraine. By applying the method of generalisation, the study identified the main problems and gaps that impede the effective implementation of legal measures to establish liability for anonymous accusations on the Internet and in the media. This method was used to identify the lack of a clear mechanism for identifying persons who disseminate false information and the insufficient legal framework as the main factors that complicate the legal regulation of this issue.

Regulations of various legal sources were used in the study to fully understand and substantiate the issue, in particular: the Constitution of Ukraine (1996), Convention for the Protection of Human Rights and Fundamental Freedoms (1950), Resolution of the Plenum of the Supreme Court of Ukraine No. 1 "On Judicial Practice in Cases on Protection of Dignity and Honour of an Individual and Business Reputation of an Individual and Legal Entity" (2009), Decision of the Zvenyhorod District Court of Cherkasy Region (2023),

Decision of the Frankivsk District Court of Lviv (2023) and Decision of the Sviatoshynskyi District Court of Kyiv (2023). Moreover, a Department for Digital, Culture, Media & Sport of the UK (2022) report and other related materials were used in the study.

Results

Before studying the relevant aspects of judicial protection against defamation on the Internet, the essence and characteristics of defamation should be determined. According to the definition given in Resolution of the Plenum of the Supreme Court of Ukraine No. 1 (2009), information is considered false if it does not correspond to objective reality or is presented with a mistake. This means that it contains information about events or phenomena that did not exist at all or did exist, but the information provided does not reflect the real state of affairs, whether due to fragmentation or distortion. Such information may be disseminated through a variety of media channels, including the press, radio, television, and Internet resources, or through other means of mass communication and telecommunication, including profiles, statements, letters addressed to other persons, as well as public speeches and electronic networks, regardless of the form, which is intended to be directed at least one person.

Thus, it is worth noting that one of the key conditions for the dissemination of information is its reliability. The understanding of this term is subjective, as each person may consider it depending on their ideas. In addition, there is no official definition of "reliability" in the current legislation of Ukraine. Therefore, credibility can be viewed as the communication of truthful information under any circumstances or through oral explanations. Importantly, the concept of credibility should be objective and not be influenced by the perception of the information by a particular person or the method of its dissemination.

The analysis of publications on the political platform www.openpetition.de, which took place as part of the study, showed that users of this platform and the cultural community associated with it influence the spread and nature of offensive content. In addition, the study examined the impact of social norms on the theory of "online storms", which describes collective online aggression against subjects of public interest. These social norms can influence the expression of public dissent (Department for Digital, Culture, Media & Sport, 2022).

An experiment conducted on Reddit, a community dedicated to discussing scientific research with 13.5 million subscribers, included a proposal to moderators to post community rules in the comments at the top of some threads (Department for Digital, Culture, Media & Sport, 2022). This initiative resulted in a decrease in the number of users posting messages that violated the rules. The experiment confirmed that moderators' intervention can influence social norms and shape online behaviour, which supports the idea that the culture of a platform has a significant impact on the level of abuse. For example, a report by the UK Department for Digital, Culture, Media and Sport highlights anonymity-related abuses and identifies three main types of abuse: abuse, which includes discrediting individuals through false information they post or disseminate on anonymous networks; using anonymity to carry out cyberbullying and online threats; violation of the privacy and intimacy of individuals through anonymity on the Internet.

The overall conclusion from the research is that platforms can implement measures to change their culture to reduce the attractiveness of abuse to users by making such behaviour less attractive and discouraging. One possible measure is to limit the creation of multiple accounts for a single user, which can avoid the "longevity" of negative consequences. In today's environment, when a user is locked out of one account, they can often easily create another and continue the inappropriate behaviour.

Under Ukrainian law, there are various forms of legal liability for disseminating false information. For example, civil liability may be imposed for the dissemination of false information that violates the honour, dignity and reputation of an individual or legal entity. Thus, if the information disseminated by an unknown person is untrue and violates the rights of an individual, the latter has the right to apply to the court to recognise this information as untrue and refute it. This is provided for in paragraph three of part four of Article 277 of the Civil Code of Ukraine (2003). Given that the judicial procedure for resolving disputes is the most effective, let consider possible options for bringing a person to justice in court.

To establish the fact of a violation of a person's rights as a result of a defamatory statement, the legal elements of the offence must be present. Only the existence of such legal elements can serve as a basis for satisfying a claim. This implies the following circumstances: disclosure of information about a known person in any form; this information must relate to a specific individual or legal entity, i.e. the plaintiff; the information disseminated must be improper, i.e. not true; such information may violate personal non-property rights, causing damage to the relevant personal benefits or preventing a person from fully and timely exercising personal non-property rights.

In case of defamation of a person on the Internet, to bring the perpetrators to civil liability, it is necessary to identify the author who disseminated such false information and file a claim with the relevant court. There are many cases in court practice related to the protection of honour, dignity, business reputation and compensation for non-pecuniary damage as a result of the dissemination of false information about a person, including on the Internet. For example, in case No. 694/1379/22 (Decision of the Zvenyhorod…, 2023), the plaintiff states that on 27 July 2022 at 08:29 a.m. and on 03 August 2022 at 18:18 a.m., the defendant posted a text message about him on her personal Facebook page, which alleged the fact of the plaintiff's unlawful and socially unacceptable behaviour, which was negative, unreliable and violated his right to respect for honour and dignity, and humiliated his honour and dignity. The materials of another case show that in 2022, the defendant systematically terrorised the plaintiff with phone calls and messages that were threatening and unacceptable. Later, she received calls and messages from unknown persons who claimed to have found her phone number on the Internet. The circumstances described above have severely undermined her physical and mental state. She claims that she stopped sleeping and eating normally, stopped communicating with her family, and started taking sedatives (Decision of the Frankivsk…, 2023).

In the context of false information about a person being disseminated on the Internet, the violation of the rights of such persons results in appropriate actions requiring the removal of false data from the network. One of the most

effective remedies is to post information on the same platform that refutes the false information, as in the event of a court case, the court may order the person concerned to take such action. For example, the Decision of the Sviatoshynskyi District Court of Kyiv (2023), in the framework of the lawsuit, obliged the defendant to refute the information disseminated on the Internet on its website by publishing a refutation on the social network Facebook. An analysis of court practice shows that this method of protecting rights is considered to be the most effective, since in cases where it is impossible to identify the owner of a social media account, national courts dismiss claims based on the lack of a response (identification of a specific defendant). There is also the issue of disseminating false information on "fake accounts", where a web page is created under the guise of a name without reflecting the author's real identity. In such cases, an effective method of protection is to contact the social network administrator with a complaint about a violation of the company's policy. Administrators often respond to users' comments and can block those who violate the rights of others by publishing false information.

Given the accumulated experience of Ukrainian court verdicts, victims of defamation violations are advised to clearly define in their claim the nature of the information that they believe to be unreliable. In addition, it is necessary to provide evidence that this information relates to their person and has become known to other persons, considering the time, method and identification of the persons to whom this information was transmitted. It is also necessary to submit legal documents confirming that the social media account belongs to a specific person (defendant) in real life, as well as to indicate the copyright holder of the website where this information is disseminated. Therefore, the statement of claim should be accompanied by all available evidence confirming the circumstances on which the claim is based. In cases involving the protection of dignity, honour and business reputation, it is important to remember that plaintiffs must prove that the disseminated information adversely affects the person's honour, dignity and business reputation and violates their non-property rights.

Online platform providers, website moderators and bloggers should be careful when engaging in the dissemination of offensive speech, while journalists should be careful in their coverage of events and news to avoid publishing content that could be classified as defamatory. Even if truth is an absolute defence to defamation, it is often an extremely difficult or costly process to establish truthfulness.

One potential option would be to limit the jurisdiction of defamation cases to countries with which there is a "real and meaningful connection". For example, Germany has achieved quite a successful legitimate regulation of combating copyright infringement through torrent technologies. An agency cooperating with the copyright owner monitors attempts to distribute content on known trackers, obtaining information about the IP addresses of those who download and distribute content. Then, using the IP addresses, the provider identifies the infringer, who is sent a request for identification. This technology functions quite effectively (even if there are ways to circumvent it), but there are obvious difficulties in scaling: the availability of data transmission and the ease of identifying IP addresses, which are unique to torrent technologies (Civil Code of Ukraine, 2003).

In the United States, the Communications Act (1934) is often characterised by inconsistency. In a well-known decision, it was determined that an online service provider (considered as a conduit or disseminator) is liable for defamatory acts in publications of third parties on their platform. Thus, in the Stratton Oakmont case, the court found convincing evidence that the online service provider Prodigy acted more like a publisher than a distributor by installing moderators to control content, using filtering software and considering itself a family-oriented (another sign of content control) network access provider (Stratton Oakmont v. Prodigy, 1995).

Understanding such cases is key for institutions to formulate appropriate responses to requests for information from third parties or to address their involvement in the perception of harmful and anonymous speech when the institution itself is the target of such actions and seeks to identify the anonymous speaker. Thus, in the case of a person spreading false information, it is important to identify this person properly, which will significantly increase the chances of refuting such allegations. In such a situation, it may be useful to try to resolve the issue through out-of-court settlement, as the judicial system is overloaded, and the number of judges is limited. Therefore, before filing a lawsuit, it is prudent to consider all available options for resolving the situation outside the court system.

Bringing anonymous defamation to legal accounts on the Internet and in the media can be challenging due to the anonymity and global nature of the Internet. However, certain practical ways can be used to bring legal action:

- contacting law enforcement agencies. Law enforcement agencies may attempt to identify the person hiding behind anonymity through an IP address, but this requires a court order and cooperation with Internet service providers;
- contacting platform administrators. Administrators may be responsible for removing content or providing information about a user in the event of defamation being posted on a particular platform;
- involvement of civil society organisations and initiative groups. The active role of civil society organisations, in cooperation with legal experts and information technology experts, can help identify and document cases of anonymous defamation. These organisations can create mechanisms to collect evidence of disinformation and facilitate its transfer to law enforcement agencies for further investigation and prosecution of those who disseminate false information online. This approach will engage more third-party forces in the fight against anonymous defamation and ensure more effective control over its spread.

Discussion

A review of the legal mechanism for ensuring the security of personal data on the Internet requires a comprehensive analysis. Discussions on the effectiveness of this mechanism in ensuring the protection of private information on the Internet have caused a wide resonance in the scientific community. The position emphasising the importance of the control function in the legal mechanism of protection against defamation on the Internet and in the media is voiced by K. Akrami *et al.* (2021). While the above studies highlight the importance of analysing the legal framework for personal data protection in the context of technological advances, they do not fully consider the dynamics and complexity of the modern digital environment. These studies may be limited

in the context of constant changes in technology and data protection strategies. In addition, the positions of the above authors emphasise the control function in the legal mechanism of protection against defamation on the Internet and in the media, which may not consider the risks of restricting freedom of speech and privacy in the digital space.

Proponents of the introduction of liability for defamation G. Lee and A. Soonah (2022) point to the ineffectiveness of civil law defence, which, moreover, does not play any preventive role. According to D.T. Indriasari and K. Karman (2023), freedom of speech in Ukraine is increasingly associated with the unrestricted dissemination of unverified, sometimes even inaccurate, information facts. In addition, criminal liability for disseminating certain types of information is not something exceptional in the current legislation (Al-Zoubi, 2023). Thus, it is difficult to balance between protection against defamation and ensuring freedom of speech, which requires careful consideration and resolution by legislators. The diversity of approaches to the problem of defamation and freedom of speech reflects the complexity of the issue itself and the different perspectives of researchers on this subject. On the one hand, there is a need for effective protection against defamation and other forms of disinformation that may damage the reputation of individuals or organisations and disrupt public order. On the other hand, it is important to ensure freedom of speech and access to information, which are one of the main components of a democratic society. The balance between these two aspects is key to creating a fair and functional legal environment. It should be borne in mind that too much protection against defamation can lead to censorship and restrictions on freedom of speech, while insufficient control can lead to the spread of disinformation and harm society and individual rights. Therefore, addressing this issue requires in-depth analysis and discussion by lawmakers, researchers and the public to develop rational and effective legal mechanisms that will protect against defamation while not restricting freedom of speech and access to information.

According to N. Chaudhary (2023), the current diversity of case law lacks consistency, provides insufficient guidance and often fails to adequately address the rights of an anonymous person to express their views in the online space. For this reason, an approach is proposed that considers the overwhelming burden of proof for the person requesting disclosure of identity but also develops a specific balancing test that includes factors such as: form of anonymous expression; participation of the speaker in the main trial; extent and harm that could be caused to the parties if the wrong disclosure decision is made. While this approach is valid, it is worth elaborating that such a framework favours flexibility and adaptability, avoiding an attempt to create a one-size-fits-all standard that is likely to be inadequate given the huge variety of factual circumstances that arise in disclosure cases. This approach treats each disclosure case individually, considering all contextual factors affecting it. This may include the specifics of the case, the type and sensitivity of the information, privacy requirements and other circumstances. This approach ensures maximum adaptability and efficiency in dealing with specific situations.

I.D. Kurniawan and K. Kristiyadi (2022) emphasise that the actions of persons who knowingly disclose someone's name, whether they do so in public or via the Internet/media, can be stopped and punished by detention and compensation for the proposed activity. Public authorities, as guarantors of protection for those who are the subject of criticism, do not remain silent, protect victims, and appropriate rewards as a solution to minimise damage to their image. This is indeed the case, as the actions of the offenders cause significant damage to the victim, as they spoil their reputation, and in the worst case, may even lead to the victim's exclusion from society. Therefore, the practical methods proposed earlier that can be used to exert legal influence will allow for more effective prosecution of those responsible for committing defamation.

Following H. Shimizu (2023), the right to request disclosure of the sender is an established substantive law. Thus, the victim, who is the owner of the right, can exercise this right without going to court. In the case of publications that are not of general interest, ordinary actions of citizens in everyday life are emphasized. While partially agreeing with this thesis, it should be specified that in cases where the absence of public interest is found, the circumstances considered are such as a clear indication in the information of other motives, such as revenge, persecution or personal attacks, and the absence of signs that would indicate the presence of public interest. This is obvious from an analysis of the context. Furthermore, in cases where the same person systematically and persistently makes statements that deny the right to personal identity for ordinary private citizens, this goes beyond what is permissible under accepted norms and is considered an open violation of personal dignity and feelings.

According to L. Wang (2022), improving the civil law protection of the right to online privacy requires attention to two aspects: strengthening the legal framework to ensure adequate protection of the privacy of Internet users and raising public awareness of online privacy protection. In full support of this view, it is worth adding that the improvement of online privacy protection contributes to the formation of an effective civil law system and reflects the development of a socialist country, considering its peculiarities following Chinese specifics.

A.K. Jain *et al.* (2021) state that privacy breaches during interaction and presentation are becoming a significant future threat due to the relevant mechanisms of interaction with smart devices and systems that are constantly evolving. Interaction with smart devices and systems can undoubtedly be a source of privacy threats. However, it can also be a contributing factor in ensuring security and efficiency. Modern technology can be used to develop advanced authentication and encryption methods that protect personal data. In addition, innovative developments in cybersecurity can help to detect and prevent potential privacy breaches. Therefore, while there are threats associated with interacting with smart devices, the availability of these technologies can also provide new opportunities to improve data security and protection.

Some experts, in particular R. Qu (2023) and K. Lincoln *et al.* (2022), argue that anonymity creates a favourable environment for extremism and social degradation. On the other hand, A.O. Banjo and O.O. Dokunmu (2023), A.K. Čelofiga and T. Tomažič (2023) argue that the violation of online privacy is too high a price to pay for an uncertain increase in security. At the same time, it should be understood and borne in mind that the precise legal distinction between protecting the right to legitimate use of anonymity and intervening to prevent abuse remains a hotly debated

issue worldwide. Complicating factors such as differences in jurisdictions, technological workarounds, and conflicts between cultural values related to privacy make it difficult to create consistent global standards that are universal.

Given the above, researchers consider a variety of practical measures to prevent and respond to defamation, such as establishing a reasonable burden of proof, effectively combating false information, developing mechanisms for transnational cooperation, and strengthening the oversight and cooperation of social media platforms. A variety of measures, such as legislation, technology and education, aim to create a cyberspace that not only ensures freedom of expression but also promotes fairness and respect, making it a platform for communication, cooperation and inclusion.

The gradual or unpredictable introduction of regulation may undermine regulatory objectives and create uncertainty about legal obligations and liabilities, making it difficult for organisations and individuals to develop best practices in the use of online content. From a practical perspective, the global nature of online content also raises regulatory challenges: there is likely to be an incentive to harmonise standards and practices across jurisdictions, particularly on the major digital platforms, but a specific regime based on defamation law could create a risk of significant divergence between markets such as the European Union.

The most essential component of avoiding defamation lawsuits is the awareness and education of people, including active users of social media, regarding the use of these platforms for communication and dissemination of information. Internet/media users must exercise caution and prudence to avoid liability for their statements, comments and postings through the various social media platforms available. In today's fast-moving world, where technology enhances communication, traditional principles of defamation, while still relevant, are becoming more complex and are actively influenced by the social media era.

Conclusions

The issue of protecting honour, dignity and business reputation on the Internet and in the media is important in the modern world. With the growing popularity of social media, citizens are becoming more vulnerable to the flow of unverified information that finds its way online.

Particular attention is devoted to the following key aspects that are important for persons seeking protection in court for violations of their online image: confirmation of the publication of information on the Internet, which, according to the complainant, damages personal rights; identification of the parties to the case; analysis of the context and form of information to determine its reliability. These aspects are carefully considered by the courts when resolving cases related to the protection of honour, dignity and business reputation in the online environment.

A review of the current situation and legislative context in the fight against negative content demonstrates that the strategy of this battle cannot be limited to technical means of removing information, as provided for by the legislation of any country. As the amount of information is constantly growing, the identification and classification of potentially dangerous content, its legal regulation and the protection of citizens from it are becoming extremely difficult tasks in many cases.

Ukraine currently lacks a special law that would control the dissemination of information online. Therefore, when a person is faced with the dissemination of confidential or unknown information on the Internet, personal rights are to be protected in court, based on the general rules established in the procedural law, the Civil Code of Ukraine and the decisions of the Plenum of the Supreme Court of Ukraine No. 1, as well as the protection of the business reputation of individuals and legal entities. The procedure for reviewing relevant cases has a well-established algorithm, especially in cases where unverified information is disseminated through the print media (newspapers or magazines) or on the Internet.

When considering cases on the protection of personal data on the Internet and in the media, certain criteria of evidence are applied, which are quite stable. However, sometimes there are difficulties in identifying the owner of the website, the person who owns it and the defendant, as well as the source of information and other aspects. This casts doubt on the enforceability of legal protection and requires consideration of alternative approaches. Domestic courts usually dismiss claims and do not recognise information disseminated via the Internet as unreliable, without obliging it to be refuted. This may be because the courts consider evaluative statements about the plaintiffs to be residual and do not consider them defamatory, thereby limiting the possibility of obtaining adequate protection and compensation. Thus, domestic courts need to maintain a balance between the right to freedom of expression and the right to protection of dignity and privacy. The key to resolving defamation disputes is to maintain this balance.

Further research could include analysing measures to prevent abuse on the Internet and in the media. Additional research could include an analysis of measures aimed at preventing abuse on the Internet and in the media. This could include examining the effectiveness of various control strategies, the implementation of technological solutions to detect and block inappropriate content, and an assessment of the regulatory environment to ensure safety and compliance with online behaviour.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Akrami, K., Ghafari, H., & Rostami, V. (2021). Censorship in the media: Freedom versus responsibility with emphasis on the United States legal system. *Public Law Studies Quarterly*, 52(3), 1319-1340. doi: 10.22059/jplsq.2021.299084.2354.

[2] Al-Zoubi, M. (2023). Crimes of electronic defamation, libel, and slander under Jordanian cybercrimes law. *International Review of Law*, 12(1), 267-284. doi: 10.29117/irl.2023.0260.

[3] Arbatman, L., & Villasenor, J. (2022). Anonymous expression and "unmasking" in civil and criminal proceedings. *Minnesota Journal of Law, Science & Technology*, 23(1), 77-130.

[4] Banjo, A.O., & Dokunmu, O.O. (2023). Implications of application of the law of defamation in social media. *Timbou-African Academic International Journal of Social Science Research and Anthropology*, 12(6), 181-188.

[5] Bevz, S., & Samchynska, O. (2021). Application of article 173-1 of the Code of Ukraine on Administrative Offenses. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 2(115), 50-60. doi: 10.31733/2078-3566-2021-6-50-60.
[6] Blikhar, M. (2023). Legal basis of protection of personal data on the Internet. *Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 62, 20-24. doi: 10.32841/2307-1745.2023.62.4.
[7] Čelofiga, A.K., & Tomažič, T. (2023). Anonymous media sources & sentiments: A case study of Slovenian newspapers. *Heliyon*, 9(12), article number e22934. doi: 10.1016/j.heliyon.2023.e22934.
[8] Chaudhary, N. (2023). Examining the legal boundaries of online anonymity. *White Black Legal Law Journal*, 2(15), article number 18.
[9] Civil Code of Ukraine. (2003, January). Retrieved from http://teplydim.com.ua/static/storage/filesfiles/Civil%20Code_Eng.pdf.
[10] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10#Text.
[11] Communications Act. (1934, June). Retrieved from: https://transition.fcc.gov/Reports/1934new.pdf.
[12] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/254%D0%BA/96-%D0%B2%D1%80#Text.
[13] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://www.echr.coe.int/documents/d/echr/Convention_ENG.
[14] Decision of the Frankivsk District Court of Lviv in the Case No. 465/1964/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111542290.
[15] Decision of the New York State Supreme Court in the Case "Stratton Oakmont v. Prodigy". (1995, May). Retrieved from https://www.dmlp.org/threats/stratton-oakmont-v-prodigy.
[16] Decision of the Sviatoshynskyi District Court of Kyiv in the Case No. 759/769/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/112103455.
[17] Decision of the Zvenyhorod District Court of Cherkasy Region. in the Case No. 694/1379/22 . (2023, February). Retrieved from https://reyestr.court.gov.ua/Review/109038927.
[18] Department for Digital, Culture, Media & Sport. (2022). *Abuse and anonymity*. Retrieved from https://assets.publishing.service.gov.uk/media/639730d78fa8f553092e67d0/Report_into_the_Connection_between_Abuse_and_Anonymity.pdf.
[19] Indriasari, D.T., & Karman, K. (2023). Privacy, confidentiality, and data protection: Ethical considerations in the use of the Internet. *International Journal Islamic Education, Research and Multiclturalism*, 5(2), 431-450. doi: 10.47006/ijierm.v5i2.239.
[20] Jain, A.K., Sahoo, S.R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157-2177. doi: 10.1007/s40747-021-00409-7.
[21] Kukh, O.M., & Lukh, A.M. (2021). Methods of information culture in the formation of critical thinking in the fight against negative content of the internet network. *Collection of Scientific papers Kamianets-Podilskyi National Ivan Ohiienko University. Pedagogical Series*, 27, 160-164. doi: 10.32626/2307-4507.2021-27.160-164.
[22] Kurniawan, I.D., & Kristiyadi, K. (2022). Criminal sanctions against the performers of damage through social media. *Bullet: Journal of Multidisciplinary Science*, 1(3), 352-356.
[23] Lee, G., & Soonah, A. (2022). Anonymity and gender effects on online trolling and cybervictimization. *Journal of Cybersecurity Education, Research and Practice*, 2023(1), article number 5. doi: 10.32727/8.2023.14.
[24] Lincoln, K., Vong, A., & Quinn, K. (2022). The role of defamation in Australia: Developments in the legal and regulatory landscape continue to shape the approach to online content. *Internet Law Bulletin*, 25(2), 18-21.
[25] Onyshchenko, S., Burbii, A., Boikov, A., Riabiy, S., & Korniiko, S. (2023). Personal data protection on the internet under martial law: The case of Ukraine. *Amazonia Investiga*, 12(69), 204-215. doi: 10.34069/AI/2023.69.09.18.
[26] Pakhnin, M. (2023). *Criminological protection of the media: Phenomenology and mechanism of provision*. Kharkiv: Kharkiv National University of Internal Affairs.
[27] Qu, R. (2023). Identification and countermeasures of network defamation crime: Present situation, supervision status, and criminal applications. *International Journal of Law and Politics Studies*, 5(5), 43-48. doi: 10.32996/ijlps.2023.5.5.6.
[28] Resolution of the Plenum of the Supreme Court of Ukraine No. 1 "On Judicial Practice in Cases on Protection of Dignity and Honour of an Individual and Business Reputation of an Individual and Legal Entity". (2009, February). Retrieved from https://zakon.rada.gov.ua/laws/show/v_001700-09#Text.
[29] Romanova, V., Nikitin, Y., Vozniuk, N., Sverdlyk, Z., Boichuk, N., & Kunderevych, O. (2021). Responsibility for dissemination of inaccurate information on the Internet. *International Journal of Computer Science and Network Security*, 21(8), 137-140. doi: 10.22937/IJCSNS.2021.21.8.18.
[30] Shimizu, H. (2023). Reform of procedure about civil remedies for victims of slander on the Internet in Japan. *Japanese Society and Culture*, 5, 25-44.
[31] Wang, L. (2022). The civil law protection of Internet privacy. *International Journal of Education and Humanities*, 6(1), 170-175. doi: 10.54097/ijeh.v6i1.3086.

Практичні способи притягнення до юридичної відповідальності за анонімні наклепи у мережі Інтернет та ЗМІ

Ліана Вікторівна Спицька
Доктор психологічних наук, кандидат юридичних наук, професор
Київський Міжнародний Університет
03179, вул. Львівська, 49, м. Київ, Україна
https://orcid.org/0000-0002-9004-727X

Анотація. Станом на 2024 рік існує необхідність у координації загальноприйнятих стандартів щодо юридичної відповідальності за анонімні наклепи у віртуальному просторі Інтернету та в ЗМІ, оскільки це стає актуальним у контексті швидкого технологічного розвитку та цифрової трансформації. Тому мета цього дослідження полягала у виявленні найпоширеніших та ефективних підходів до притягнення до відповідальності за поширення недостовірної інформації у віртуальному просторі Інтернету та ЗМІ. Для досягнення даної мети застосовувалися різноманітні методи наукового та юридичного характеру, зокрема: порівняння, прогнозування, узагальнення, системного аналізу, формально-юридичний, формально-логічний та інші. Проаналізовано спірні аспекти, пов'язані з захистом індивідуальної гідності, честі та комерційної репутації фізичних осіб у контексті Інтернету, охоплюючи основи виникнення правових зв'язків у даній області та практичні виклики, з якими стикаються особи, які прагнуть захистити свої права на гідність та комерційну репутацію, порушені через поширення в мережі інформації, що розглядається як необ'єктивна чи неточна. Виявлено, що більшість національних судів сьогодні відхиляють позовні вимоги, спрямовані на захист приватності в Інтернеті, і не визнають розповсюджену через цей канал інформацію як недостовірну, не вимагаючи її спростування. У роботі розроблені та аргументовані рекомендації, які можуть бути реалізовані на практиці для притягнення осіб до юридичної відповідальності за неправдиву інформацію, поширену анонімно в мережі Інтернет і ЗМІ. Запропоновано практичні способи, які можуть бути використані для здійснення правового впливу на осіб, які здійснюють анонімні наклепи у мережі Інтернет та ЗМІ

Ключові слова: поширення недостовірної інформації; приниження честі та гідності; захист ділової репутації; дезінформація в Інтернеті; достовірність інформації