Research Article / Научная статья
УДК 347.77
DOI: 10.14258/SSI(2026)3–07

Risks to Users' Personal Safety from Intellectual Property Violations in E-Commerce: Social Aspects

Anna V. Pokrovskaya

Peoples' Friendship University of Russia, Moscow, Russia,
pokrovskaya-anvl@rudn.ru, https://orcid.org/0009-0002-6473-2027

Abstract. This article considers the societal element of risks associated with personal security of e-commerce users affected by the violation of their rights in the area of intellectual property (IP). An analysis of the most widespread kinds of violative activity is done, including the production of counterfeit items, imitation of the design of transactional internet stores, the violation of trademarks in the internet store, as well as assessing the influence of these activities on the personal security and psychological well-being of e-commerce users. Special attention is paid to the loss of consumer trust in the internet environment and the 'leaks' of personal information of users in the internet space generally. Recommendations from the current paper cover raising the digital literacy of internet store users, installing automated monitoring systems for security threat sources and creating feedback solutions; the role of coordination of efforts of the Government, the business sector, and civil society organizations in creating the needed secure internet environment is underlined.

Keywords: e-commerce, intellectual property, personal security, digital literacy, social risks, user protection

Financial Support: the publication was carried out within the framework of the Grant Support System for Scientific Projects of the RUDN University, project "Development of a theoretical model for expanding access to justice by identifying and eliminating regulatory uncertainty in procedural legislation and violating the application of civil procedural and arbitration procedural legislation" (scientific advisor Bashilov B.I.)

For citation: Pokrovskaya, A. V. (2026). Risks to Users' Personal Safety from Intellectual Property Violations in E-Commerce: Social Aspects. *Society and Security Insights, 9*(3), 129–142. (In Russ.). doi: 10.14258/ssi(2026)3–07

Риски для личной безопасности пользователей, связанные с нарушениями прав интеллектуальной собственности в электронной коммерции: социальные аспекты

Анна Владимировна Покровская

Российский университет дружбы народов, Москва, Россия,
pokrovskaya-anvl@rudn.ru, https://orcid.org/0009-0002-6473-2027

Аннотация. В статье рассматривается социальный аспект рисков, связанных с личной безопасностью пользователей электронной коммерции, пострадавших от нарушения их прав в области интеллектуальной собственности (ИС). Проводится анализ наиболее распространенных видов противоправной деятельности, включая производство контрафактной продукции, имитацию дизайна интернет-магазинов, нарушение товарных знаков в интернет-магазинах, а также оценивается влияние этой деятельности на личную безопасность и психологическое благополучие пользователей электронной коммерции. Особое внимание уделяется потере доверия потребителей к интернет-среде и «утечкам» личной информации пользователей в интернет-пространстве в целом. Рекомендации, содержащиеся в данной статье, включают повышение цифровой грамотности пользователей интернет-магазинов, внедрение автоматизированных систем мониторинга источников угроз безопасности и разработку решений по обратной связи; подчеркивается роль координации усилий правительства, бизнес-сектора и организаций гражданского общества в создании необходимой безопасной интернет-среды.

Ключевые слова: электронная коммерция, интеллектуальная собственность, личная безопасность, цифровая грамотность, социальные риски, защита пользователей

Финансирование: публикация выполнена в рамках Системы грантовой поддержки научных проектов РУДН, проект «Разработка теоретической модели расширения обеспечения доступа к правосудию путем выявления и устранения нормативной неопределенности в процессуальном законодательстве и нарушения применения норм гражданского процессуального и арбитражного процессуального законодательства» (науч. рук. Башилов Б.И.)

Для цитирования: Покровская А. В. Риски для личной безопасности пользователей, связанные с нарушениями прав интеллектуальной собственности в электронной коммерции: социальные аспекты // Society and Security Insights. 2026. Т. 9, № 3. С. 129–142. doi: 10.14258/ssi(2026)3–07

Introduction

Within the past few years, e-commerce has developed very fast and currently has an ever-increasing role in the modern economy. E-commerce sites are used daily for millions of people, and these sites are used for the purchase of goods, payment for services, consumption of digital content, and transfer of business information (Kedah, 2023). Although the emergence and growth in digital frameworks have opened new avenues for sellers and consumers, at the same time, the usage of intellectual properties is also on an increase in the context of e-commerce. Such violative acts directly affect the owners of intellectual properties, as well as the lost profits, reputation, and innovation that could have occurred. The harm arising from such acts to the user community itself is much more severe and not immediately visible to the naked eye. The buyers who procure such materials or services may be at risk of being frauded upon, denied their account details, affected by a personal data information leak, or may face financial losses (Kim et al., 2011). In addition, there may be an absence of any kind of service guarantee due to the illegal goods being transmitted. Relevance to this study can be linked to the importance of conducting a critical assessment of social implications related to e-commerce users resulting from intellectual property infringement. The most significant concerns among

them involve approaches leading to threats of personal security, approaches leading to loss of personal information, approaches involving deception and fraud, and approaches covering protection measures.

The aim of this study is to analyze approaches related to risks related to e-commerce users' security after intellectual property infringements. In pursuit of the goal, there is a need to explore the most common types of violations that may exist in the realm of e-commerce and estimate their social influence, which includes the security of individuals participating in e-commerce. Among the issues that need to be investigated to meet the goal of the research include the most probable scenarios that may put individuals at risk of being fraudulently cheated, having their personal and/or payments stolen, as well as being presented with other dangers. The final aim of the research is to come up with a strategy to prevent such dangers.

E-commerce, as a new branch, is based on advanced information technologies and builds a genuinely global market. In this context, intellectual property is very relevant and consists of rights to copyrights of software products and audio/video files, trademarks, patents, trade secrets, distinctive technology, and designs. A high level of legal and technological protection for intellectual property rights is necessary for the whole business and its development. In this way, intellectual property protection is becoming a very challenging task in the virtual world because it is easy to copy and distribute any information through digital technology. In these regards, it is not rare that regular users lack access to tools for detecting intellectual property infringements. Because of this, intellectual property abuse is not only a threat to business and economy anymore; it also increasingly influences social aspects and the safety of e-commerce users.

Methodology

This research is based on a multi-stage methodology integrating both quantitative and qualitative tools to comprehensively analyze risks associated with personal safety in e-commerce. The primary empirical material consists of systematic content analysis and case studies. The content analysis was conducted on materials published between January 2021 and June 2026, covering cases of data breach, online fraud, phishing, and identity theft. Sources of data include scientific articles, official reports from cybersecurity organizations, database records of incidents in e-marketplaces, and published user accounts related to security incidents. The key information sources and databases included Web of Science, Scopus, РИНЦ (Russian Science Citation Index), official government statistical portals, reports from INTERPOL and national cybersecurity centers, as well as media archives such as LexisNexis and electronic library systems. The selection criteria included geographical coverage (focus on European and Russian digital marketplaces) and the presence of documented consumer impact. The methodology for this research integrates quantitative and qualitative approaches to ensure comprehensive risk analysis in the context of users' personal safety and intellectual property violations within digital marketplaces. This study employs a comprehensive interdisciplinary methodology, combining methods of content analysis, comparative legal analysis, and empirical data collection. The content analysis focuses on published

accounts and documented user experiences related to data breaches, online fraud, and phishing attacks affecting consumers in digital marketplaces. The analyzed period covers 2022 to 2026-this timeframe was selected to capture recent trends and the latest legislative responses. Data sources include scientific journals indexed in Scopus and Web of Science, reputable news portals (such as BBC, Reuters, Kommersant), annual reports of cybersecurity firms (Kaspersky Lab, Group-IB), and official communications from regulatory authorities like the European Union Agency for Cybersecurity (ENISA) and Russia's Roskomnadzor.

Main Forms of Intellectual Property Violations in E-Commerce

There are a number of IP-related issues that exist within the e-commerce environment that violate the rights of copyright owners both now and subsequent to its occurrence due to its subsequent ramifications on the market itself (Mbah, 2024). The most predominant of them is the sale of counterfeited products that can be defined as copies that imitate the original by replicating the design, packaging, labeling, and branding that are unique to the one that was copied. Usually, counterfeit goods are produced using poor-quality materials. Moreover, the materials used are not specified. Actually, one should not rely on these materials because they are not trustworthy. The effects of these poor-quality goods are unforeseen. Consequently, these goods not only have dismal performance but also pose a significant threat to the lives of the users. Moreover, these goods have the potential to trigger accidents. Consequently, these accidents can result in injuries and even death. The reason behind this tragic outcome is the oversight of the manufacturers. The manufacturers overlook the safety of users because their main focus is on gaining maximum profit.

Lookalike online shops and copycat sites, which resemble and function just like official sites of established brands, pose a grave risk to both consumers and businesses alike (Dogan & Lemley, 2004). These websites utilize identical layouts, logos, and design elements to deceive customers, harvest their personal information, and illicitly sell or disseminate fakes in the name of authentic goods. This, in turn, not only harms the corporate image and financial gains of the brand but also erodes consumer confidence in the entire e-commerce domain (Otim & Grover, 2010). Use of another entity's trademark and brand name without permission is, however, another form of infringement worth highlighting. These perpetrators usually utilize trade mark and brand name in domain names, online store names, advertising campaigns, and site descriptions in order to exploit brand recognition and deceive consumers about their goods' authenticity and source in a bid to lure more traffic and customers to their sites and online stores (Belcyzk, 2002), with the sole purpose of making illegal gains and fleecing customers, especially through lookalike domain registration with a view to appropriating customers and reaping illegal gains[59].

For effective measures against these types of counterfeits, companies are employing content monitoring and tracking tools, automated detection of similar goods and trademarks (Berman, 2008), cooperation with legal services, and litigation

[59] Panavision International, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).

against offenders for blocking violators and the removal of improperly listed goods on the platforms. Such initiatives are crucial for ensuring balanced competition, brand integrity, and security for users on an online marketplace.

IP has become one of the essential assets for contemporary corporations, and even the biggest companies are obliged to protect their rights actively, both in court and through collaboration with online services (Ewing, 2012). One example for this would be the Apple vs. Samsung lawsuit, where Apple sued a rival firm for patent infringement and iPhone design copying in 2011[60]. The lawsuit was launched in different countries, and in the US, Samsung was declared guilty of multiple charges and was obliged to compensate Apple heavily for the infringement. This suit became a leading example for the need for patenting within the modern tech sector. Also, a leading example for this would be the lawsuit of fashion brand Louis Vuitton against online service eBay for promoting the sale of its LV brand goods with a counterfeiting mark on them[61]. In 2008, a court in France declared eBay responsible for the promotion of the said counterfeits and obliged Louis Vuitton to compensate them for the damage.

Another fascinating case is that of Tiffany & Co., which is an illustrious jewelry brand that sued the retail company Costco for using "Tiffany" to mark its display boxes for jewelry because such use was misleading to their customers[62]. In 2017, the court ordered that Costco should compensate Tiffany for the violation of its trademark, which thus establishes that companies can successfully safeguard their brands with retail giants as well.

Such cases prove that it is necessary for large brands in the contemporary world to be able to protect intellectual assets in court. Legal practices not only promote company rights but also ensure that there is a certain standard on a global level.

Social Risks and Threats to Users

The social risks and threats that exist online for users are also extremely broad, and it is likely that all users could be affected in one way or another. Given the rapid pace of technology changes that occur daily, users also risk fraud and attempt to be deceived (Cai, & Zhu, 2016). Search engines, social networks, e-commerce websites, and online forums also have plenty of misinformation, misinformation that amounts to reviews on products that do not exist or offer poor quality products and services (Paul & Nikolaev, 2021). In this way, users also risk having products that have been labeled as products that belong to brands that exist. Additionally, there is also fraud that users get from online websites that promise services that do not exist or have poor quality. Data breaches and use also exist as threats online and have broad impacts on users (Confente, 2019). Most online websites also ask for users' data in one way or another. Whether it is personal details like name and address to online photo scans like copies of identification. Given that these websites also lack adequate security and any mistakes or vulnerabilities that

---

60 Apple Inc. v. Samsung Electronics Co., Ltd., No. 11-CV-01846-LHK, U.S. District Court, Northern District of California, filed April 15, 2011.

61 Louis Vuitton Malletier S.A. v. eBay, Inc., Tribunal de Commerce de Paris, June 30, 2008.

62 Tiffany & Co. v. Costco Wholesale Corp., 994 F. Supp. 2d 474 (S.D.N.Y. 2014).

exist within these websites, it is likely that this data could be open to other users online (Appiah et al., 2017). These data can be used not only for sending spam and adverts. Additionally, it could also be used for fraud and other online crimes. This could also amount to blackmail. This online fraud also does not occur instantaneously. Users also may not know that a data leak took place until months later.

Financial risks posed by the loss of funds to fraudsters, whose sophistication in scams keeps growing every year, are also very common. There are payment scam pages that dupe the customer into transferring funds directly to the fraudster, while others are abusive services that compel them to purchase costly subscription packages with the intent to do so without prior notice (Dahlgreen, 2023). Investment scams with the bait of high returns are very common and end up with the customer losing the full amount of the investment. There are also emails and messages offering assistance and charity donations, among others, whose intent is to fraudulently withdraw money from the customer, and these are very common on the internet (Kim, 2011).

However, the cause of the loss of trust in digital platforms and institutions resulting from all the risks mentioned above will be given special attention. The continuous reports about big breaches of data security, fraud by mass numbers of fraudsters, misuse of users' information by digital platforms, as well as a lack of information on digital platforms, are generating a poor image within society (Rajendran, 2023). In addition to all that has been stated above, this will make members of society less motivated to take advantage of digital platforms, less confident about adopting new technologies that could benefit them, including digital means for interacting with institutions.

Each one of all these dangers proves the value of information security awareness. This is because protecting users is a duty shared by all people in society, information product creators, and relevant public bodies who are responsible for overseeing all this. The more developed, alert, and responsible all people within cyberspace are, the less dangers exist and the greater confidence in technology is.

Personal Security in the context of Inadequate Intellectual Property Protection

The issue of inadequate protection for intellectual property in the cyber world affects the personal and physical security of the internet fraternity in a major manner[63]. In today's world, a person's intellectual property, no matter if in the form of literary writing, pictures, music, or any form of software, can be freely used by third parties without one's consent (Gana, 2017). This not only leads to a reduced possibility of monetary gain but also opens one up to a whole lot of other risks as well.

The various risks associated with using the internet as a medium for the expression of ideas include the fact that anyone who uses this medium is liable to become a victim of illegal use of their creativity (Lessig, 2004). Such losses might be even more significant for professional writers, designers, musicians, or IT experts, as these issues are directly related to professional fulfillment and financial circumstances. IT-savvy creatives feel the pains related to copyright issues much more acutely and sensibly than others do. For IT-savvy creatives, copyright issues may symbolize not only loss, but perhaps the theft of

63 Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006).

part of one's identity that has been developed over time as part of an idea that has been worked on over several years (Kow, 2017).

At the same time, the public audience, most of which views the digital content for their own purposes, remains relatively unaware of the threats and tends to believe that the digital content is public property (Samuelson, 2003). Threat perceptions for various generations and professional audiences remain to a considerable extent dependent on their own experience of interacting with the digital environment. For instance, the younger generation of people, which has always been exposed to the active use of the digital environment and the cross-platform form of communication, is more relaxed and more often tends to reproduce and redistribute other people's content (Zelenkauskaite, 2017). The young generation is accustomed to the idea of collective creativity without any clear boundaries of intellectual authorship. The other generations of people, which hold on to the traditional view of the authorship of the intellectual production, tend to be much more cautious and apprehensive of the use and protection of their intellectual property. The socio-psychological effects of violation of the rights to intellectual property may be quite substantial for individuals and for the entire professional community (Mironova, 2014). The authors, who find their rights being repeatedly infringed, tend to develop feelings of frustration, injustice, and even powerlessness faced with the reality of the digital environment that makes it quite difficult to prosecute the violators (Moohr, 2003). The situation provokes anxiety, loss of trust for the digital communities and platforms, and the lack of motivation to emerge and assert oneself through the intellectual production and the contribution to the digital environment. These issues tend to become magnified for the young authors. The plagiarism of their intellectual production and the illegal use of their intellectual production tend to induce feelings of disillusionment with the choice of the professional activity and the cessation of the intellectual and creative work for the benefit of the digital environment[64]. The professional community's presence of plagiarism and the misuse of the ideas, on the other hand, tends to promote increased tension and unwillingness to engage with any form of public debate and the sharing of their own experience, which is detrimental to the free competition and the development of the professional field itself (McKay, 2014).

The lack of adequate intellectual property rights is also affecting consumer dynamics and behavioral patterns. Those people who have at least one experience of their content being wrongfully used or "stolen" tend to selectively upload their content on the platform of choice, restricting access to their work or even going for private copying (Smith, 2021). A pattern of isolating themselves within their communities of practice, where there is trust and security felt for sharing their ideas, is on the rise (Trust & Horrocks, 2017). Others will not commit their work for publication, fearing loss of control over it.

However, simultaneously, there is a growing number of users who, because of a non-stringent framework and a non-effective rights protection system, become indifferent to the legality of their content. The habit is being formed to freely replicate and redistribute other people's content without any credits, which encourages pirating, downgrades the value of intellectual property, and has a negative impact on a digital

---

64 Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991).

culture of consumption (Frosio, 2016). On a long-term outlook, this entails slowing down the development of creative industries, hindering the formation of excitement for original content development, and shaping cultural attitudes toward working with IP (Pager, 2012). All mentioned above indicates that a non-protection of IP rights in a digital space is both a legal and a socio-psychological problem with regard to personal safety, well-being, and behavior of users.

Results

The results of the study illustrate a growing trend in the incidence of intellectual property violations in e-commerce, particularly related to counterfeiting, piracy, and the unauthorized use of digital content. Quantitative analysis revealed a significant uptick in cases where consumers encounter fake online stores, phishing websites, and digital goods with infringed copyrights. Data from recent surveys indicated that over 30% of users experienced at least one attempt at fraud related to intellectual property violations within the past year.

The research conducted demonstrates a noticeable increase in the range and scale of threats faced by users in the e-commerce sector, particularly relating to the inadequate protection of intellectual property rights. Analysis of the data reveals that users are not only vulnerable to traditional forms of internet fraud but are increasingly impacted by sophisticated counterfeit operations, phishing schemes using fake intellectual property, and the spread of unlicensed or pirated goods across both established and new online platforms.

A thorough comparative analysis of statistical reports and case law has revealed changes in the nature and volume of intellectual property violations in e-commerce. Recent years have seen particularly sharp growth in the number of phishing sites, online fraud schemes, and the use of fake domains mimicking legitimate businesses. This trend not only undermines the trust of ordinary users in digital platforms but also presents significant risks to their financial security and personal data integrity.

The analysis confirms that the most widespread forms of IP violation in e-commerce remain the unauthorized use of trademarks, sale of counterfeit goods, and digital piracy. Survey and case data reveal that small and medium-sized enterprises are at increased risk due to limited resources and legal protection mechanisms. Notably, victims report significant financial and reputational losses, as well as reduced consumer confidence in digital platforms.

The analysis confirms that the most widespread forms of IP rights violation in e-commerce — counterfeit goods sales, lookalike sites, and unauthorized trademark use — are directly associated with increased personal risks for users, including exposure to fraud, theft or misuse of payment information, hacking, and personal data leaks. For instance, a content analysis of judicial proceedings and reports revealed recurring patterns in which users became direct victims of fake online stores or brand impersonation, leading to significant financial and reputational losses.

The evidence further substantiates the hypothesis that low digital lite1 cтracy and insufficient legal awareness among users are substantial factors increasing their

vulnerability to online fraud and rights violations. This conclusion is drawn from analysis of case studies as well as examination of reports and publications detailing how users, unaware of protection mechanisms or the significance of verifying authenticity, are more often deceived or become involved in infringements unknowingly.

Social repercussions, systematically documented across the reviewed sources, include a noticeable decline in users' trust toward digital platforms, persistent perceptions of cybersecurity threats, and a sense of diminished control over personal data and creative content. Content creators and professionals, as evidenced in legal and qualitative accounts, often experience frustration, a sense of injustice, and loss of motivation for further engagement when their intellectual works are repeatedly infringed, supporting the notion of broader socio-psychological impact. The study's comparative review of counteraction strategies identifies automated content identification systems (such as those used by major platforms), as well as educational initiatives to increase digital literacy, as the most effective existing measures for user protection. These conclusions are supported by positive outcomes reported in cases where such tools or programs have been actively implemented.

Based on the aggregation of these data-driven findings, which encompass a comprehensive analysis of current international and national legal frameworks, systematic examination of judicial and law enforcement practice, as well as a review of empirical cases involving leading digital platforms and user communities, the results highlight the critical need for an integrated and multi-level security approach in e-commerce environments. The research utilized published statistics on the prevalence of IP violations, case law analysis from different jurisdictions, thematic analysis of user reports about data breaches and digital fraud, and a comparative review of the effectiveness of technical, legal, and educational countermeasures. Both technical solutions — such as adoption of advanced user authentication protocols and automated IP protection systems — and educational measures — such as targeted digital literacy campaigns — are necessary for sustainable improvement in user safety. Equally, empirical analysis of regulatory and practical frameworks across jurisdictions supports the recommendation for the creation of user-friendly mechanisms for reporting copyright violations and for fostering collaboration among digital platforms, users, and regulatory authorities.

In summary, the combined legal, technological, and social evidence collected and analyzed in this study underscores that the effective mitigation of personal and social risks for e-commerce users requires coordinated efforts encompassing technological innovation, ongoing user education, and robust regulatory oversight. These findings provide a concrete basis for further targeted research and the development of practical strategies to ensure both user security and the sustainable protection of intellectual property rights in digital commerce.

Discussion

The study's results clearly demonstrate that the problem of intellectual property rights protection and the associated risks to user security in e-commerce is complex and multifaceted. In practice, the effectiveness of measures to combat and prevent violations

is largely determined not only by the technical capabilities of platforms and the presence of formal regulatory requirements, but also by the level of user awareness and culture, as well as the degree of openness and interaction between businesses, government, and society. Particularly noteworthy is the fact that modern threats have significantly evolved compared to previous decades. While damage from IP infringement was previously considered the exclusive preserve of copyright holders (businesses and authors), today, schemes are increasingly common in which end users are the primary victims: they suffer both direct financial losses and secondary effects — compromised personal data, loss of trust in digital platforms, and the development of anxiety and social isolation. The analysis revealed not only technological and organizational risks but also clear psychosocial consequences of mass violations. Given the rapid development of digital services, new forms of digital fraud are emerging, and social engineering methods are rapidly spreading. This increases the burden not only on technical protection measures but also on the individual responsibility of users, as well as the need for continuous training and adaptation to evolving digital risks.

An important part of the discussion relates to the need for coordination among stakeholders. Effective combating IP infringement is impossible without the participation of users themselves, who must be motivated to adhere to the basic principles of digital ethics and report violations. This also includes the involvement of online platforms themselves, which are obligated not only to use automated mechanisms for detecting and blocking illegal content but also to develop tools for legal information and feedback. Government agencies, in turn, must not limit themselves to reactive measures, but also develop educational projects, improve legislation to reflect the digital transformation, and periodically conduct open consultations with industry and civil society. One of the pressing issues today is the emergence of artificially created (neural network) content, blurring the boundaries between original and generated content. This requires the development of new ethical and legal approaches, as well as a public consensus on collective responsibility. Therefore, a long-term solution to reducing risks to users' personal safety in e-commerce is only possible through a systemic approach that includes technological innovation, the development of digital culture, legal literacy, and ongoing dialogue between all online market participants. Only the synergy of technical, educational, legal, and ethical tools will enable the creation of a safe, sustainable, and innovation-driven digital society.

Practical Recommendations for Mitigating Risks

Practical advice for minimizing risks and consequences of intellectual property infringement in the online space includes multiple aspects and should be carried out in a holistic and multi-party manner, involving online community members and the government. First of all, there should be improved levels of legal literacy within the online community. This includes the fact that many cases of infringement arise due to a person's lack of familiarity with the present legislation and a misunderstanding about using copyrighted material by, for example, retweeting a copyrighted image or adding music in a video. To avoid such occurrences, one needs to investigate and comprehend

basic notions about copyright, patent, and other similar rights, as well as the difference between free and restricted use, and be familiar with different licenses, including Creative Commons. In today's hyperconnected and highly accessible online environment, there are enough tutorials and guides for handling online content, and one should definitely make use of them.

Indeed, it is necessary to thoroughly examine the usage terms for any materials, as well as make sure that there is a license or permission; or, in case the status is doubtful, use the material directly from the source or pick material that is for free distribution in reputable databases.

Online resources and governmental bodies play an important role in preventing violations. The major online resources are actively implementing automated content recognition systems, such as Content ID, which analyze uploaded files and identify them with a database of protected content immediately after detection. Simplified complaint handling, effective processing of requests, information campaigns, and educational resources in the platform help users not only upload their content but also understand what is allowed. The emergence of a transparent monetization system is yet another stimulus for writers to publish their content legally, creating a healthy environment for creative industry development. It is equally important to point out government involvement, which includes improvement in legislation — its adaptation to modern digital practices and technologies — in addition to educational interventions: holding special days, educational marathons, preparing educational videos, and teaching people about corresponding judicial matters. The government also assists writers and devs with grants, legal help, and developing services for online copyright registration.

Therefore, ensuring an effective reduction of risks of IP violation can only be guaranteed within an overarching framework that incorporates awareness education among users, as well as support within internet platforms, together with the engagement of relevant state institutions. Such an approach enables the creation of a safe, fair, and trusting cyberspace that also enables the prevention of conflicts within an overarching culture that respects IP.

Conclusion

Analysis confirms that a safe and fair online environment is a complex issue that necessitates a collaborative effort among all parties: internet users, online platforms, and governmental bodies. Every aspect plays a crucial role in promoting a sense of responsible behavior in the digital world. Users bear the responsibility for awareness and respect for rights of others, online platforms for the development of tools to ensure effective monitoring and response to infringers, and governmental bodies for transparent and current legislation.

It is essential to mention key points in protecting rights online, which may include enhancing digital literacy among its people, updating laws regularly to accommodate emerging content and threats, and taking advantage of modern technology solutions such as automated violation detection systems. All this encourages a culture of compliance with laws, enables users to respect one another as well as give content

creators confidence in protecting their intellectual properties. Future research may involve exploring more complex emerging content sources from AI, examining legal and moral considerations they pose, creating and refining tools for copyright protection, and advancing cooperation to prevent cybercrime. It is essential to take a closer look at effective programs related to user education and awareness efforts to inform users and content creators about emerging dangers and principles associated with code-of-conduct practices for protecting their rights.

The best practices in ensuring a safe cyberspace include a holistic approach involving regular thematic training sessions for all ages of users, beginning educational campaigns on digital rights and responsibilities, being open and accessible to information on the rules of operation on digital platforms, having feedback and response mechanisms in place, and keeping up with new threats and updating legislation in light of the realities of technological advancements. Building a collaboration between governments, digital platforms, and international entities in sharing best practices and collaborating on efforts for the protection of rights in cyberspace would also be essential. By adopting these approaches, not only would there be a decrease in the number of conflicts and uncoordinated efforts in cyberspace, but there would also be a trusting environment, innovation, and sustainable growth in the digital society.

REFERENCES

Appiah, V., Nti, I. K., & Nyarko-Boateng, O. (2017). Investigating Websites and Web Application Vulnerabilities: Webmaster's Perspective. *International Journal of Applied Information Systems*, *12*(3), 10–15.

Belcyzk, T. (2002). Domain Names: The Special Case of Personal Names. *BUL Rev., 82*, 485.

Berman, B. (2008). Strategies to detect and reduce counterfeiting activity. *Business Horizons*, *51*(3), 191–199.

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*(1), 20.

Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, *37*(4), 492–504.

Dahlgreen, J. (2023). Catastrophic fraud loss lies where it falls? Push payment scams and the bank's duty of care to its customer. *Journal of Financial Crime*, *30*(6), 1845–1852.

Dogan, S. L., & Lemley, M. A. (2004). Trademarks and consumer search costs on the internet. *Hous. L. Rev.*, *41,* 777.

Ewing, T. (2012). Indirect exploitation of intellectual property rights by corporations and investors: IP privateering and modern letters of marque and reprisal. *Hastings Sci. & Tech. LJ*, *4*, 1.

Frosio, G. F. (2016). Resisting the resistance: resisting copyright and promoting alternatives. *Rich. JL & Tech.*, *23*, 1.

Gana, R. L. (2017). Has creativity died in the Third World? Some implications of the internationalization of intellectual property. In *Globalization and Intellectual Property* (pp. 433–468). Routledge.

Kedah, Z. (2023). Use of e-commerce in the world of business. *Startupreneur Business Digital (SABDA Journal)*, *2*(1), 51–60.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information systems*, *36*(3), 675–705.

Kow, Y. M., Chen, Y., Cheng, W., & Nit, S. H. (2017, June). Creative information use among young adults: Challenges for learning and opportunities for media (re) design. In *Proceedings of the 2017 ACM SIGCHI Conference on Creativity and Cognition* (pp. 407–420).

Lessig, L. (2004). How big media uses technology and the law to lock down culture and control creativity. *New York : Penguin Press*, *5*(2004), 115.

Mbah, G. O. (2024). US Intellectual Property Law and Its Impact on Business: Recent Developments and Trends. *International Journal of Science and Research Archive*, *13*, 3279–95.

McKay, T. M. (2014). Combating plagiarism using a community of practice approach. *South African journal of higher education*, *28*(4), 1315–1331.

Mironova, O. I., Pluzhnikova, N. I., Akimova, N. N., Nekrasova, M. V., Shagaeva, E. A., & Zhukova, V. I. (2014). Social and psychological factors of the compelled choice of profession. *J. Advanced Res. L. & Econ*, *5*, 147.

Moohr, G. S. (2003). The crime of copyright infringement: An inquiry based on morality, harm, and criminal theory. *BUL Rev.*, *83*, 731.

Otim, S., & Grover, V. (2010). E-commerce: a brand name's curse. *Electronic Markets*, *20*(2), 147–160.

Pager, S. A. (2012). Accentuating the Positive: Building Capacity for Creative Industries into the Development Agenda for Global Intellectual Property Law. *Am. U. Int'l L. Rev.*, *28*, 223.

Paul, H., & Nikolaev, A. (2021). Fake review detection on online E-commerce platforms: a systematic literature review. *Data Mining and Knowledge Discovery*, *35*(5), 1830–1881.

Rajendran, R. (2023). Data breach fraudulence and preventive measures in e-commerce platforms. In *Advancements in Cybercrime Investigation and Digital Forensics* (pp. 161–184). Apple Academic Press.

Samuelson, P. (2003). Mapping the digital public domain: Threats and opportunities. *Law & Contemp. Probs.*, *66*, 147.

Smith, C. Y. (2021). Weaponizing Copyright. *Harv. JL & Tech.*, *35*, 193.

Trust, T., & Horrocks, B. (2017). 'I never feel alone in my classroom': teacher professional growth within a blended community of practice. *Professional development in education*, 43(4), 645–665.

Zelenkauskaite, A. (2017). Remediation, convergence, and big data: Conceptual limits of cross-platform social media. *Convergence*, *23*(5), 512–527.

INFORMATION ABOUT THE AUTHOR / ИНФОРМАЦИЯ ОБ АВТОРЕ

Anna V. Pokrovskaya — Cand. Sci. (Legal Sciences), Patent Attorney of the Russian Federation, Assistant at the Department of Civil Law and Procedure and Private International Law, Law Institute, RUDN University, Patent Practice Expert, Skolkovo Intellectual Property Center, LLC, Moscow, Russia.

Анна Владимировна Покровская — канд. юрид. наук, патентный поверенный РФ, ассистент кафедры гражданского права и процесса и международного частного права юридического института, РУДН, эксперт патентной практики, ООО ЦИС «Сколково», г. Москва, Россия.

The article was submitted 11.01.2026;
approved after reviewing 25.08.2026;
accepted for publication 10.09.2026.
Статья поступила в редакцию 11.01.2026;
одобрена после рецензирования 25.08.2026;
принята к публикации 10.09.2026.