IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 3, Issue: 5
2025

Tort Liability of Digital Platforms for User-Generated Content

Allakuliev Mirzhalol Davronbekovich
Tashkent State Law University

Abstract

This article examines the problem of liability allocation for harmful content posted by users on digital platforms. The author analyzes the contradiction between protecting victims' rights from defamation, hate speech, and intellectual property violations, and ensuring freedom of expression and the development of the digital economy. The study highlights the inadequacy of the traditional dichotomy between publishers and passive intermediaries in the context of modern platforms that actively curate, rank, and monetize user content through algorithmic systems. Based on comparative legal analysis, the author identifies three regulatory models: the American broad immunity model under Section 230, the European conditional exemption model with notice and takedown mechanism under the E-Commerce Directive and Digital Services Act, and the German differentiated liability model. Special attention is given to content moderation problems, risks of excessive censorship through automated filtering, and opacity of algorithmic decisions. The author identifies the absence of special platform liability rules in Uzbek legislation and proposes comprehensive regulatory modernization measures.

Keywords: Digital Platforms, Intermediary Liability, User-Generated Content, Online Defamation, Freedom of Expression, Notice and Takedown, Digital Services Act, Uzbekistan

APA Citation:

Allakuliev, M. (2025). Tort Liability of Digital Platforms for User-Generated Content. *Uzbek Journal of Law and Digital Policy, 3*(5), 20–35. https://doi.org/10.59022/ujldp.376

I. Introduction

The rapid development of digital technologies and internet proliferation have radically transformed the ways information is created, distributed and consumed, giving rise to a new ecosystem of digital platforms that have become the primary communication environment for billions of people worldwide. Social networks, video hosting platforms, online marketplaces, blogging platforms, forums and other services based on user-generated content have created unprecedented opportunities for free expression, idea exchange, social interaction and economic activity (Bates, 2007). The democratization of information production and distribution, where every internet user can become a publisher potentially reaching a global audience, is viewed by many as the greatest achievement of the digital age, realizing ideals of free speech and pluralism of opinion.

However, this same freedom to create and distribute content generates serious risks of abuse and harm to the rights and legitimate interests of third parties. Digital platforms are used to disseminate defamatory materials damaging the honor, dignity and business reputation of citizens and organizations, to incite ethnic and religious hatred, to call for violence and terrorism, to distribute child pornography and other illegal content, to infringe intellectual property through pirate distribution of protected works, to defraud consumers through deceptive advertising and counterfeit product sales (Liu et al., 2024). The anonymity or pseudonymity that the internet provides lowers social and legal barriers to aggressive and illegal behavior, creating the phenomenon of online disinhibition, where people permit themselves statements and actions that would be unthinkable in offline contexts.

When harmful content is published on a digital platform, a fundamental question arises about liability allocation: should the platform bear liability alongside the content author, or is it merely a neutral technical intermediary not responsible for what its users publish? Traditional tort law has developed a clear distinction between the primary publisher, who controls publication content and bears full liability for its contents, and the secondary distributor, such as a bookstore or newsstand, which simply transmits information without controlling its content and bears liability only with actual knowledge of the illegal nature of distributed material. However, digital platforms do not fit clearly into either category.

On one hand, platforms do not create content themselves but merely provide technical infrastructure for user posting, making them similar to passive intermediaries. On the other hand, modern platforms do not simply store and transmit content but actively curate it through moderation mechanisms, rank it using recommendation algorithms determining what content users will see, monetize it through targeted advertising, and often edit or comment on user publications, giving them characteristics of active publishers (Gillespie, 2019). Moreover, platforms derive direct economic benefit from user content attracting audiences and generating

advertising revenue, creating financial incentives to maximize user engagement even if achieved through provocative or harmful content.

Legal regulation of digital platform liability must balance several competing values and interests. First, effective protection of victims' rights from illegal content must be ensured, including the right to protection of honor and dignity, right to privacy, intellectual property rights and other legally protected rights. Second, users' freedom of expression must be preserved and creation of a total censorship regime avoided, where platforms would block any potentially controversial content out of fear of liability, including legitimate criticism and discussions on matters of public importance. Third, innovative digital economy development must be ensured without imposing on platforms, especially small and medium-sized ones, excessive burdens of monitoring and controlling billions of units of user content, which could make business models technically impossible or economically unviable.

The Civil Code of the Republic of Uzbekistan contains general provisions on tort liability for dissemination of defamatory information, establishing in Article 1021 that moral harm caused by dissemination of information damaging honor, dignity and business reputation is compensated regardless of tortfeasor's fault. However, the legislation lacks special provisions regulating liability of digital platforms as intermediaries through which users disseminate such information. This creates legal uncertainty and risk of applying general publisher liability provisions to platforms, which could have catastrophic consequences for internet industry development in the country.

The relevance of this study stems from the need to develop a balanced approach to regulating digital platform liability in Uzbekistan, considering both international experience and best practices, as well as specifics of the national legal order, cultural traditions and strategic digital economy development goals. The work aims to comprehensively analyze platform liability problems for user content, study various legal regulation models applied in developed jurisdictions, and develop concrete proposals for Uzbek legislation modernization to create a legal environment ensuring effective protection of citizens' rights while preserving freedom of expression and incentives for innovative digital technology development.

II. Methodology

This study employed a qualitative research methodology to examine digital platform liability regulations across different jurisdictions. The research used content analysis as the primary analytical approach. This method allowed for systematic examination of legal texts, regulatory frameworks, and policy documents from multiple countries. The qualitative approach was chosen because it enables deep understanding of complex legal concepts and regulatory philosophies. It helps identify patterns, themes, and relationships in legal frameworks. The study focused on three main jurisdictions: the United States, European Union, and Germany. Primary sources

included legislation texts, court decisions, and official regulatory documents. Secondary sources included academic articles, policy reports, and expert analyses. This approach provided comprehensive insights into how different legal systems address platform liability challenges.

The content analysis process involved several systematic steps. First, relevant legal documents and scholarly materials were collected and organized by jurisdiction. Second, key themes were identified including liability models, procedural requirements, and enforcement mechanisms. Third, comparative analysis was conducted to identify similarities and differences between regulatory approaches. The research examined specific provisions regarding notice-and-takedown procedures, content moderation timelines, and platform obligations. Special attention was given to recent developments like the Digital Services Act and NetzDG. The analysis also reviewed empirical studies on automated moderation systems and their impacts. Data was coded and categorized based on regulatory principles, implementation challenges, and effectiveness outcomes. This methodological approach enabled the development of evidence-based recommendations for Uzbek legislation that consider international best practices and local context.

III. Results

This research examined how different countries regulate digital platform liability for user-generated content. The study focused on three main questions. First, what are the different approaches to platform liability? Second, how do these approaches balance user protection with freedom of expression? Third, what regulatory model would work best for Uzbekistan? The analysis reviewed legal frameworks from the United States, European Union, and Germany. It explored how each system handles illegal content on social media and other platforms. The research also examined problems with automated content moderation systems. The goal was to propose practical reforms for Uzbek legislation on digital platforms.

The research found three distinct regulatory models for platform liability. The American model under Section 230 provides broad immunity to platforms. This protects them from lawsuits over user content. The European model uses conditional exemption. Platforms avoid liability if they remove illegal content quickly after notification. The German model is stricter. It requires platforms to remove obviously illegal content within 24 hours. Each model reflects different priorities between innovation, user protection, and freedom of speech. Large platforms like Facebook and YouTube have resources for sophisticated moderation systems. Small platforms struggle to meet the same standards. This creates market consolidation risks.

Automated content moderation creates serious accuracy problems. Machine learning systems make both false positives and false negatives. They block lawful content by mistake. They also miss some illegal content. The systems often cannot understand context, satire, or cultural differences. Studies show algorithms may discriminate against minority groups. They reproduce biases from their training data. Platforms keep their moderation algorithms secret as trade secrets. This opacity makes

it impossible to verify fairness. Users cannot effectively appeal automated decisions. The European Digital Services Act introduced graduated obligations based on platform size. Large platforms face stricter transparency and risk assessment requirements. This differentiated approach recognizes that one-size-fits-all rules do not work.

The conditional exemption model balances competing interests better than absolute immunity or strict liability. Notice-and-takedown procedures work when properly designed with clear standards. Platforms need specific timelines for different content types. Obviously dangerous content requires removal within 24 hours. Other content allows seven days for verification. Procedural protections for users are essential. Users must receive reasons for content removal. They need effective appeal mechanisms. Trusted flagger systems improve notice quality. Accredited organizations with expertise can flag illegal content more accurately. Transparency requirements help ensure accountability. Regular public reports on moderation statistics are necessary. Out-of-court dispute resolution can reduce litigation costs while protecting user rights.

The research revealed surprising problems with strict deadlines. Germany's 24-hour removal requirement causes over-censorship. Platforms remove controversial but lawful content to avoid fines. They lack time for proper legal assessment. This effectively privatizes censorship decisions. Private companies make judgments that should come from courts. Another unexpected finding concerns human moderators' mental health. Reviewing traumatic content causes serious psychological harm. This creates tension between automation benefits and accuracy concerns. The study also found that transparency reports after NetzDG adoption showed increased removals. However, research suggests many removed items were actually lawful. This reveals unintended consequences of well-intentioned strict enforcement regimes.

IV. Discussion

A. Classification of Digital Platforms and Differentiation of Liability Regimes

Before analyzing liability issues, it is necessary to recognize the heterogeneity of digital platforms and differences in their functional characteristics, degree of content control and business models, necessitating differentiated legal regulation. The general term "digital platforms" encompasses extremely diverse services, from passive hosting providers offering only technical space for file placement to highly integrated social networks actively curating, ranking and monetizing user content (Gorwa, 2019).

At one end of the spectrum are basic technical infrastructure providers, such as website hosting providers, cloud storage or network connectivity providers, which perform automatic transmission or temporary caching of content without any control over its substance. These services function as neutral communication channels, analogous to telephone networks or postal services, and their liability for content transmitted through their infrastructure is traditionally excluded provided they lack

knowledge of content's illegal nature and act purely mechanically.

At the opposite end of the spectrum are platforms with high degrees of editorial control, which actively select, curate and edit user-posted content, apply detailed editorial policies, hire professional moderators to review content before publication, and actually function as traditional publishers using user content as raw material for creating their information product. For such platforms, arguments for liability exemption are significantly weaker, and they should bear liability comparable to traditional media.

Between these poles lies enormous diversity of intermediate forms, including forums and bulletin boards with minimal moderation, blogging platforms providing users with content creation tools but not controlling substance until receiving complaints, social networks using automated moderation systems combined with reactive content removal based on user complaints, video hosting platforms applying algorithmic systems for illegal content recognition, online marketplaces verifying seller and product legitimacy (Matias, 2019). For each of these categories, different liability regimes may be justified, reflecting the platform's degree of content control and ability to prevent illegal material publication.

A critically important differentiation factor is the nature of posted content and associated risks. Publishing text messages on a forum creates different risks and requires different control measures compared to posting video content that may contain child pornography or extremist materials, or selling goods on a marketplace that may prove counterfeit or dangerous. Accordingly, legal regulation may establish stricter monitoring and control obligations for platforms specializing in high-risk content categories while maintaining a more liberal regime for general communication platforms (Helberger et al., 2018).

Another important factor is platform size and its technical and financial capabilities for implementing content control systems. Large global platforms such as Facebook, YouTube or Amazon, with billions of dollars in revenue and thousands of employees, have resources to create sophisticated automated and manual content moderation systems, including applying artificial intelligence for detecting illegal materials and hiring armies of moderators to review controversial content. Conversely, small and medium platforms, startups and non-profit services may lack financial and technical capabilities to implement similar systems, and imposing the same obligations on them could lead to their market displacement and consolidation of the digital ecosystem in the hands of a few giants.

These considerations justify the need for differentiated regulation establishing basic obligations for all platforms but providing enhanced requirements for large platforms, specialized high-risk content platforms and platforms with high degrees of editorial control. This approach is implemented in the recently adopted European Union Digital Services Act, which introduces a graduated system of obligations

depending on platform size and role.

B. American Platform Immunity Model: Section 230 and Its Criticism

The United States historically chose the most liberal approach to regulating digital platform liability, enshrining in Section 230 of the Communications Decency Act of 1996 broad immunity for interactive computer services from liability for user-posted content. Section 230 establishes two key provisions: first, no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider; second, no provider or user of an interactive computer service shall be held liable on the basis of any voluntary good-faith actions to restrict access to or availability of material that the provider or user considers obscene, excessively violent, harassing, or otherwise objectionable.

These provisions created extremely broad immunity for internet platforms, protecting them from civil lawsuits based on third-party content posted on the platform, including claims for defamation, invasion of privacy, intentional infliction of emotional distress, violation of right of publicity and many other torts. American courts have interpreted Section 230 very broadly, applying immunity even in cases where the platform played an active role in organizing or structuring content, edited user-provided headlines or descriptions, or derived direct commercial benefit from illegal content.

The justification for such broad immunity was the need to protect freedom of expression on the internet and stimulate development of innovative online services. Legislators and courts reasoned that if platforms bore liability for all user content, they would be forced either to exercise total prior censorship of all publications, making interactive services in their current form impossible to operate, or completely refrain from any content moderation for fear that any control attempts would be interpreted as assuming editorial responsibility. Section 230 resolved this dilemma by guaranteeing that platforms could moderate undesirable content without risk of losing immunity, thereby incentivizing voluntary removal of illegal or harmful material.

The American platform immunity model played a critical role in the formation of the U.S. internet industry and transformation of American technology companies into global leaders. Protected from risks of mass lawsuits, platforms could experiment with new user content formats, scale their services to billions of users and create innovative business models without fearing ruinous litigation over every potentially illegal publication among billions of daily posted content units. Section 230 proponents argue it is the foundation of a free and open internet, and its repeal or substantial restriction would lead to transformation of digital space into a tightly controlled environment dominated by a few large platforms capable of bearing liability risks.

However, in recent years Section 230 has been subject to intense criticism from

various ideological positions. Conservative critics accuse large technology platforms of censoring right-wing views and selectively applying moderation rules, arguing that immunity should be conditioned on platforms observing principles of political neutrality and free speech (Maddox & Malson, 2020). Liberal critics point to insufficient platform efforts to combat disinformation, hate speech, harassment and other harmful content, arguing that broad immunity eliminates incentives for responsible moderation and allows platforms to profit from harmful content without bearing corresponding risks.

Victims of online defamation, harassment and other torts face practical impossibility of obtaining compensation, since anonymous or pseudonymous authors of harmful content are often unidentifiable or insolvent, while platforms, the only entities with sufficient resources for compensation, are protected by absolute immunity. Studies show that online harassment and defamation have serious negative impacts on victims' mental health, careers and personal lives, yet the legal system leaves them without protection, shifting all digital communication risks onto potential victims.

In response to this criticism, bills to reform or repeal Section 230 have been repeatedly introduced in the U.S. Congress, but consensus on reform direction is absent. Proposals range from complete immunity repeal to conditioning it on platform compliance with certain transparency and fairness standards in content moderation, from creating exceptions for certain illegal content categories to introducing differentiated regimes depending on platform size. As of 2025, large-scale Section 230 reform has not been adopted, and the American broad platform immunity model persists, though its future remains subject to intense political debate.

C. European Conditional Exemption Model: From E-Commerce Directive to Digital Services Act

The European Union chose a different path for regulating digital platform liability, based not on absolute immunity but on conditional exemption contingent on meeting certain procedural requirements. The 2000 E-Commerce Directive established a limited liability regime for three intermediary categories: mere conduit providers, caching providers and hosting providers. Most relevant for digital platforms is the hosting provider category, i.e., services storing user-provided information.

According to Article 14 of the Directive, a hosting provider is not liable for stored information provided that it does not have actual knowledge of illegal activity or information, and as regards claims for damages, is not aware of facts or circumstances from which illegal activity or information is apparent, or upon obtaining such knowledge or awareness acts expeditiously to remove the information or disable access to it. This creates a regime known as "notice and takedown," whereby the platform is exempted from liability if it did not know about illegal content but must remove it after receiving notice of illegality.

The Directive also establishes that Member States shall not impose general monitoring obligations on providers regarding information they transmit or store, or actively seeking facts or circumstances indicating illegal activity. This prohibition on general monitoring obligations aims to protect platforms from unbearable burdens of checking billions of user content units and preserve technological neutrality, allowing platforms to function as passive intermediaries.

The European conditional exemption model represents a compromise between the American absolute immunity approach and traditional publisher liability provisions. On one hand, it recognizes that platforms cannot realistically control all user content before publication and should not bear automatic liability for all illegal user-posted materials. On the other hand, it establishes that platforms bear certain obligations to respond promptly to illegal content notices and cannot completely ignore obvious violations of which they become aware.

However, practical Directive application revealed several serious problems. First, the concept of actual knowledge of content illegality remains indeterminate, and various Member States and courts interpret it differently. Some jurisdictions require merely notice of content existence, others require detailed substantiation of its illegality, still others require judicial determination of illegality. Second, uniform standards are lacking for what constitutes expeditious content removal, and platforms may delay responding to complaints while avoiding formal liability (Fiala & Husovec, 2022). Third, the notice and takedown mechanism creates abuse risks, where claimants send unfounded demands to remove lawful content, and platforms, fearing liability, prefer to remove controversial material without verifying complaint validity, leading to excessive censorship phenomenon.

In response to these problems and digital ecosystem evolution, the European Union adopted the Digital Services Act in 2022, which modernizes and expands the regime established by the E-Commerce Directive. The Act preserves the basic principle of conditional exemption for intermediaries but substantially details platforms' procedural obligations and introduces a differentiated regime depending on platform size and role.

The Digital Services Act establishes detailed requirements for notice and content removal procedures, including mandatory indication in notices of specific information about illegal content location, justification of its illegality, claimant contact details and good-faith statement of information accuracy. Platforms must provide clear and easily accessible notice submission procedures and process them without undue delay. Users whose content was removed must receive notification indicating removal reasons and have the opportunity to appeal the platform's decision.

For large platforms reaching more than forty-five million users in the European Union, the Act establishes enhanced obligations, including the need to conduct annual systemic risk assessments created by their services, including risks of illegal content

dissemination, negative impact on fundamental rights and manipulation of their services. Platforms must take reasonable, proportionate and effective measures to mitigate identified risks, which may include adapting interface design, recommendation algorithms, terms of service and content moderation procedures. Very large platforms must also ensure transparency of ranking and recommendation algorithms, provide users with choice of alternative ranking systems not based on profiling, and provide researchers with access to certain data for studying systemic risks.

The Digital Services Act represents the most ambitious attempt to date at comprehensive regulation of digital platform liability, balancing protection of victims' rights, preservation of freedom of expression, and ensuring platform transparency and accountability. However, the new regime's effectiveness will depend on implementation and enforcement quality, as well as regulatory authorities' ability to adapt to rapid technological changes.

D. German Differentiated Liability Model and Network Enforcement Act

Germany has taken a leading role among European countries in establishing stricter platform requirements to combat illegal content, adopting in 2017 the Act to Improve Enforcement of the Law in Social Networks, known as NetzDG. The law was adopted in response to concerns about the scale of hate speech, defamation and other illegal content dissemination on social networks, especially in the context of the migration crisis and rise of right-wing populism, as well as ineffectiveness of platforms' voluntary content moderation measures (Riedl et al., 2021).

NetzDG applies to social networks with more than two million registered users in Germany and establishes strict deadlines for removing obviously illegal content. Platforms must remove or block access to obviously illegal content within twenty-four hours of receiving a complaint and to other illegal content within seven days. Obviously illegal is content whose illegality requires no further investigation or legal assessment, such as child pornography or direct threats of violence. For other potentially illegal content, the platform must conduct legal assessment within the established timeframe.

The law provides for significant administrative fines for systematic non-compliance with illegal content removal obligations, reaching fifty million euros for particularly serious violations. Additionally, platforms must publish semi-annual transparency reports containing statistics on the number of complaints received, their processing times, amount of removed content and decision-making procedures. Platforms must also create effective user complaint procedures, appoint a contact person in Germany for receiving official requests, and ensure the possibility of appealing content removal decisions.

NetzDG has sparked intense debates both in Germany and internationally. Law supporters argue it effectively incentivizes platforms toward more responsible content

moderation and ensures user protection from hate speech and other harmful content that before the law's adoption spread virtually unpunished (Kohl, 2022). Transparency report data show that platforms substantially increased illegal content removal volumes after the law's entry into force, evidencing its effectiveness in achieving stated goals.

Law critics point to excessive censorship risks, where platforms remove controversial content without thorough legality verification out of fear of fines, leading to suppression of lawful freedom of expression. Short deadlines for content removal decisions do not allow full legal assessment of complex cases, especially regarding satire, parody, quoting illegal statements in critical context, or other context-dependent expression forms. Studies show that a significant portion of content removed by platforms under NetzDG may be lawful, but platforms prefer to err on the side of caution, blocking any potentially controversial material.

Moreover, NetzDG is criticized for transferring content legality determination functions to private companies, blurring the boundary between private content moderation and state censorship. When platforms remove content under threat of state sanctions, this effectively turns them into state censorship agents, raising concerns from freedom of expression and rule of law perspectives. Decisions on statement legality should be made by independent courts based on established legal procedures, not corporate moderators under pressure of financial sanctions.

Despite this criticism, the German approach has influenced regulatory initiatives in other countries, and NetzDG elements have been incorporated into legislation in France, Austria, Singapore and several other jurisdictions (Suzor et al., 2018). The European Digital Services Act also incorporated some NetzDG ideas, though in more balanced form with greater guarantees of users' procedural rights.

E. Problems of Automated Content Moderation and Algorithmic Opacity

The scale of modern digital platforms, where billions of users daily publish hundreds of millions of content units, makes manual moderation of all content technically impossible and economically unviable. In response, platforms are massively implementing automated content moderation systems based on artificial intelligence and machine learning technologies. These systems use text and image classification algorithms to automatically detect potentially illegal or rule-violating content, such as child pornography, extremist materials, hate speech, graphic violence or spam (Gorwa et al., 2020).

Automated moderation has obvious advantages in terms of speed and scalability. Algorithms can process enormous content volumes in real-time, identifying and blocking violations before they are seen by other users, which is impossible with manual moderation. Machine learning systems can train on millions of illegal content examples, identifying patterns and violation signs that may not be obvious to human moderators [60]. Automation also protects human moderators from

having to view large volumes of traumatic content, such as violence images or child abuse, which is a serious mental health problem for commercial moderators.

However, automated moderation generates serious problems of accuracy, fairness and transparency. Content classification algorithms, especially those based on machine learning, inevitably make errors, both false positives, when lawful content is mistakenly classified as violating, and false negatives, when illegal content is not detected. Studies show that even the most advanced systems have significant error rates, especially for context-dependent expression forms, such as satire, irony, quotation, reappropriation or culturally specific communication forms.

False positive classification errors leading to removal or blocking of lawful content and suppression of freedom of expression are especially problematic. Automated systems trained on certain illegal content examples may overgeneralize violation signs and block a wide spectrum of lawful statements containing the same keywords, visual elements or patterns as illegal content (Crawford & Paglen, 2021). For example, systems trained to remove racist statements may block discussions about racism, quotation of racist statements in critical context, or statements by minority representatives using controversial lexicon for self-identification or reappropriation of stigmatizing terms.

The problem is exacerbated by automated moderation system opacity. Platforms treat moderation algorithms as trade secrets and do not disclose details of their operation, justifying this by the need to prevent manipulation by malicious actors seeking to circumvent detection systems. However, this opacity makes it practically impossible to verify fairness and accuracy of automated decisions, identify systematic biases and discriminatory patterns, and appeal erroneous blocks. Users whose content was removed by an automated system often receive only a standard notification of platform rule violation without explanation of specific removal reasons and factors leading to content classification as violating.

Additionally, automated systems may reproduce and amplify existing social biases if trained on historical data reflecting discriminatory practices. Studies show that content moderation algorithms may systematically more frequently block content created by representatives of certain demographic groups, ethnic minorities or political views, reproducing biases present in training data or encoded in the algorithm development process. Such algorithmic discrimination can have serious consequences for equal access to digital public space and pluralism of opinion (Flew et al., 2019).

Regulating automated content moderation requires balancing recognition of technological necessity of automation for processing large-scale content volumes and ensuring adequate safeguards against excessive censorship and discrimination. The European Digital Services Act takes a step in this direction, requiring platforms to ensure users can challenge content moderation decisions and receive explanations of decision grounds. However, detailed transparency and explainability requirements for

automated moderation systems remain to be developed in the implementation and enforcement process.

F. Proposals for Modernizing Uzbek Legislation on Digital Platforms

Based on the conducted analysis of digital platform liability problems for user content and study of foreign regulatory experience, a complex of concrete proposals can be formulated for creating in Uzbekistan a modern legal environment ensuring balance between protecting victims' rights from illegal content, preserving freedom of expression and stimulating digital economy development.

The first and most fundamental proposal is adoption of a special Law of the Republic of Uzbekistan on Digital Platforms and Liability for User Content, systematically regulating the legal status of digital platforms, their rights and obligations regarding user-posted content, content moderation procedures and liability mechanisms for violations. The law should be based on the European conditional exemption model, adapted to Uzbekistan conditions, rejecting both the American absolute immunity model creating risks of illegal content impunity and the traditional automatic platform liability as publishers' model, which would make interactive service operation impossible.

The law should establish differentiated platform response timeframes to notices depending on content nature. For categories of obviously illegal and particularly dangerous content, such as child pornography, direct threats of violence, extremist materials calling for terrorism, the platform must remove content or block access within twenty-four hours of receiving notice. For other categories of potentially illegal content, the platform must conduct verification and make a decision within seven business days. If the platform in good faith believes content is lawful despite the received notice, it may reject the removal demand but must provide the claimant with a reasoned explanation of its decision.

The law should establish procedural guarantees for users whose content was removed or blocked. The user must receive notification of content removal indicating specific reasons and legal grounds, the complainant's name unless it contradicts protecting their safety, and information about appeal possibilities. The user must have the right to appeal the content removal decision, and the platform must consider the appeal within a reasonable time not exceeding fourteen days, providing a reasoned decision. If the platform rejects the appeal, the user must have the right to turn to an independent out-of-court dispute resolution body or court.

The second proposal is creating a system of accredited trusted flaggers, modeled on the mechanism provided by the European Digital Services Act. Trusted flaggers may be recognized as organizations with special expertise in certain illegal content areas, such as human rights organizations specializing in combating hate speech, child rights protection organizations, intellectual property protection organizations. Notices sent by accredited trusted flaggers should be prioritized by platforms and reviewed

expeditiously, while statistics on accuracy of notices sent by trusted flaggers should be monitored, and status may be revoked for systematic submission of unfounded notices.

The third proposal is establishing transparency obligations for large digital platforms, defined by the criterion of reaching more than a certain number of active users in Uzbekistan, for example, more than one million users. Large platforms must publish semi-annual transparency reports containing statistics on the number of illegal content notices received broken down by violation categories, amount of removed content, average notice response time, number of user appeals against content removal and their consideration results, use of automated content moderation means. Reports should be publicly available and submitted to the regulatory authority for analysis.

The fourth proposal is establishing special requirements for using automated content moderation systems. The law should recognize platforms' right to use automated means for detecting and removing illegal content but establish safeguards against excessive censorship and algorithmic discrimination. Platforms using automated moderation must ensure users can request review of decisions by human moderators. Content removal decisions made by automated systems must be accompanied by explanations in understandable form of reasons for classifying content as violating. Platforms must conduct regular audits of automated moderation systems to identify systematic biases and discriminatory patterns and take measures to eliminate them.

The fifth proposal is creating at the Agency for Development of Information and Communication Technologies of the Republic of Uzbekistan a specialized Department for Digital Platform Regulation, responsible for supervising platform compliance with established obligations, considering complaints against platform actions, conducting investigations of systemic violations and applying administrative sanctions. The Department should have powers to request information from platforms, conduct inspections, issue orders to eliminate violations and impose fines. Sanctions should be proportionate and effective but not excessive, so as not to create insurmountable barriers to market entry for new platforms.

The sixth proposal is creating a system of out-of-court dispute resolution between users and platforms regarding content moderation decisions. At the Chamber of Commerce and Industry of Uzbekistan or other independent body, a specialized body for resolving content moderation disputes should be created, which could promptly consider user complaints about content removal or blocking and issue advisory decisions. Although the body's decisions should not be legally binding, platforms should be obliged to consider them in good faith and provide reasoned explanations in case of disagreement with recommendations. Users should retain the right to go to court regardless of out-of-court procedure results.

The seventh proposal is introducing amendments to the Civil Code of the Republic of Uzbekistan, clarifying application of tort liability provisions to digital platforms. It is proposed to supplement Chapter 57 with a new article establishing a

special platform liability regime for user content in accordance with principles enshrined in the special law on digital platforms. The article should directly indicate that a platform complying with established procedures for responding to illegal content notices does not bear liability for this content if it lacked actual knowledge of its illegality or acted expeditiously after obtaining such knowledge. This will create legal certainty and protect good-faith platforms from risks of ruinous lawsuits over the entire volume of user content.

Conclusion

The conducted study revealed a fundamental contradiction between the need to protect victims' rights from illegal content posted on digital platforms and the imperatives of ensuring freedom of expression, stimulating innovation and avoiding excessive regulatory burden on platforms. Traditional tort law categories, developed for the world of offline publishers and distributors, prove inadequate for digital platforms, which combine characteristics of passive technical intermediaries and active content curators. Comparative legal analysis demonstrated various approaches to resolving this contradiction, from the American broad platform immunity model to the European conditional exemption model contingent on meeting procedural requirements and the German strict illegal content removal deadline model. Each model has its advantages and disadvantages, reflecting different balances between competing values and interests.

For Uzbekistan, striving to develop the digital economy while preserving cultural values and social stability, the most suitable appears to be an adapted version of the European conditional exemption model, supplemented with elements of the German approach establishing clear notice response deadlines and transparency requirements. The proposed complex of measures includes adoption of a special law on digital platforms, establishment of differentiated content moderation procedures depending on its nature, creation of procedural guarantees for users, introduction of transparency requirements for large platforms, establishment of standards for using automated moderation systems, and creation of specialized regulatory and out-of-court bodies.

Implementation of these proposals will require coordinated efforts of legislative bodies, government, judicial system, technology industry and civil society. However, these efforts are necessary to create a legal environment ensuring effective protection of citizens' rights in digital space while preserving freedom of expression and incentives for innovative development, positioning Uzbekistan as a progressive jurisdiction with modern digital law.

Bibliography

Bates, B. J. (2007). Yochai Benkler. *The Wealth of Networks: How Social Production Transforms Markets and Freedom . Journal of Media Economics*, *20*(2), 161–165. https://doi.org/10.1080/08997760701193787

Crawford, K., & Paglen, T. (2021). Excavating AI: the politics of images in machine learning training sets. *AI & SOCIETY*. https://doi.org/10.1007/s00146-021-01162-8

Fiala, L., & Husovec, M. (2022). Using experimental evidence to improve delegated enforcement. *International Review of Law and Economics*, *71*, 106079. https://doi.org/10.1016/j.irle.2022.106079

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, *10*(1), 33–50. https://doi.org/10.1386/jdmp.10.1.33_1

Gillespie, T. (2019). *Custodians of the Internet*. Yale University Press. https://doi.org/10.12987/9780300235029

Gorwa, R. (2019). The platform governance triangle: conceptualising the informal regulation of online content. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1407

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 205395171989794. https://doi.org/10.1177/2053951719897945

Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, *34*(1), 1–14. https://doi.org/10.1080/01972243.2017.1391913

Kohl, U. (2022). Platform regulation of hate speech – a transatlantic speech compromise? *Journal of Media Law*, *14*(1), 25–49. https://doi.org/10.1080/17577632.2022.2082520

Liu, Z., Luo, C., & Lu, J. (2024). Hate speech in the Internet context: Unpacking the roles of Internet penetration, online legal regulation, and online opinion polarization from a transnational perspective. *Information Development*, *40*(4), 533–549. https://doi.org/10.1177/02666669221148487

Maddox, J., & Malson, J. (2020). Guidelines Without Lines, Communities Without Borders: The Marketplace of Ideas and Digital Manifest Destiny in Social Media Platform Policies. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120926622

Matias, J. N. (2019). The Civic Labor of Volunteer Moderators Online. *Social Media + Society*, *5*(2). https://doi.org/10.1177/2056305119836778

Riedl, M. J., Naab, T. K., Masullo, G. M., Jost, P., & Ziegele, M. (2021). Who is responsible for interventions against problematic comments? Comparing user attitudes in Germany and the United States. *Policy & Internet*, *13*(3), 433–451. https://doi.org/10.1002/poi3.257

Suzor, N., Van Geelen, T., & Myers West, S. (2018). Evaluating the legitimacy of platform governance: A review of research and a shared research agenda. *International Communication Gazette*, *80*(4), 385–400. https://doi.org/10.1177/1748048518757142