

Legal and Administrative Measures Against Crime Propaganda on Social Media: A Review of the Turkish Practice

Hasan Tutar^{1*}, Bayram Coşkun², Çiğdem Pank Yildirim³

¹Bolu Abant İzzet Baysal University, Faculty of Communication, Department of Public Relations, Bolu Turkey; hasantutar@ibu.edu.tr

^{2,3}Muğla Sıtkı Koçman University, Faculty of Economics and Administrative Sciences, Department of Public Administration. Muğla, Turkey.

Keywords:

Crime propaganda, Digitalization, Internet law in Turkey, Social media, Youth and criminal role models.

Abstract. Digitalization and the rapid proliferation of social media platforms have enabled the reproduction of crime and criminal identity through propaganda in new media environments. This process, which leads to outcomes such as modeling and erosion of social norms, especially among young people, poses serious threats to public security and social order. This review systematically addresses crime propaganda on social media and Turkey's regulatory policies within the framework of internet law. The study was created by scanning peer-reviewed articles published after 2015 in Scopus, Web of Science, ULAKBİM, and Google Scholar databases with English and Turkish keywords by the PRISMA protocol. The included studies are articles that focus only on crime and criminal propaganda on social media platforms and contain original data and analysis. The results show that the aestheticization of crime and the promotion of anti-hero figures through social media create a strong role model effect on young people. Although legal regulations are being developed in Turkey, problems with freedom of expression and technological up-to-dateness continue. In the future, more stakeholder and dynamic cooperation is required against new threats such as artificial intelligence and deepfakes.

1. INTRODUCTION

With the impact of digitalization on social life, social media platforms have begun to play a critical role in committing and encouraging crimes and constructing criminal identities. It is observed that criminal content and the presentation of crime-encouraging content are increasingly widespread, especially on platforms such as Facebook, X (Twitter), Instagram, and YouTube. While the content shared on social media reshapes the social perception of crime, the phenomenon of heroizing or trivializing criminal figures is gaining strength day by day (Boyd & Ellison, 2015; Fuchs, 2017; Marwick & Lewis, 2017; Choudhury et al., 2021). Digital platforms reach the audience and encourage the voluntary transmission of criminal propaganda through users' active participation and content production. The algorithmic content distribution structure facilitates the rapid spread of crime-themed content that has the potential to go viral and causes crime to gain a dimension beyond borders, space, and time (Van Dijck, 2013; Alava et al., 2017; Gorwa, 2019; Gillespie, 2018; Noppari et al., 2019). This transformation reduces the impact of classical legal regulations and traditional social control mechanisms and leads to the emergence of new types of crime. Therefore, social media has become a multidimensional problem area that enables the redefinition of crime in modern society and the reproduction of criminal identity in different forms in the digital environment.

Today, propaganda of socially sensitive crime types such as terrorism, organized crime, hate speech, child abuse, and sexual crimes is effectively spread through social media, both textually and visually. Especially in fast-paced content-producing platforms such as Twitter, TikTok, and YouTube, the aestheticization of crime and the presentation of criminal figures as "anti-heroes" can lead young people to model criminal behavior (Koohikamali et al., 2021; García & Salazar, 2021; Klausen, 2015; Koohikamali et al., 2021; Aly et al., 2017). The normalization of crime in digital culture leads to the perception of crime as a status indicator or a challenge, especially among adolescents and young adults. Algorithms' personalized content recommendations accelerate users' radicalization processes and increase exposure to criminal propaganda (Baker & White, 2011; Surette, 2015; Serrano-Puche, 2020; Zeitzoff, 2017). In addition, crime-themed content spread through social media can lead to the erosion of social norms and damage public order. The normalization of crime in society causes a weakening of moral values and psychosocial problems in young generations (Crone, 2016; Alava et al., 2017; Bartlett & Miller, 2012; Livingstone et al., 2017). These developments necessitate considering criminal propaganda in the age of social media not only as a legal threat but also as a social and cultural threat.

Significant amendments were made to Law No. 5651 in 2020 to prevent criminal propaganda through social media in Turkey. The new regulations have imposed obligations on social network providers such as having representatives in Turkey, removing content, and storing user data (Karadeniz & Yıldız, 2023; Çiftçi, 2022; Demir & Sönmez, 2021). In addition, articles regarding rapid response to legal requests and ensuring children's online safety are also prominent. However, it is seen that the legislation is subject to intense criticism in areas such as freedom of expression, protection of personal data, and censorship (Erdogan, 2023; Akdeniz, 2021; Smith, 2021; Tokgöz, 2021). In particular, the difficulties experienced in international platforms' compliance with Turkish law, technical inadequacies, and deficiencies in implementation are controversial. Difficulties in implementation, legal uncertainties, and the protection of users' rights reveal the need for a multidisciplinary and constantly updated approach in the fight against social media crimes (Gürses, 2021; Erdem, 2022; Karadeniz & Yıldız, 2023; Akdeniz, 2021; Çiftçi, 2022). In the digitalizing social environment, it is vital for Turkey's internet law to have a flexible and effective structure that is compatible with international norms, both in terms of preventing crime and protecting fundamental rights.

Social media platforms worldwide maintain a delicate balance between content moderation, prevention of online crime, and

freedom of expression. The European Union's Digital Services Act (DSA) has placed significant responsibilities on platforms by increasing their obligations to promptly remove illegal content and ensure transparency (Mac Síthigh, 2022; Floridi, 2021; Floridi, 2021; Gorwa, 2019). Germany's NetzDG law requires social media companies to intervene in criminal content within 24 hours. In the US, Section 230 limits platforms' direct liability for user content, but has caused controversy regarding ensuring online safety (Heldt, 2019; Haucap et al., 2021; Kosseff, 2019; Gillespie, 2018). The UK's Online Safety Bill initiative introduces innovative regulations in transparency, child protection, and content removal. In Australia, strict regulations have been implemented against online violence and terrorist propaganda (Smith, 2021; O'Flaherty, 2023; McDonald, 2021; Gorwa, 2019; Mac Síthigh, 2022). All these initiatives show a need for multi-dimensional and innovative legislation against criminal propaganda on social media. The difficulties and technical problems in global companies' compliance with national regulations are among the main issues still awaiting solutions.

The primary purpose of this review article is to analyze the reflections of crime and criminal propaganda on social media in the current literature and to evaluate the policies and legislative regulations developed by Turkey in internet law. In the study, the aestheticization of crime, the reconstruction of criminal identity in the digital environment, and the effects of social media on criminal propaganda will be discussed from an interdisciplinary perspective (Alava et al., 2017; Livingstone et al., 2017; Pomerleau, 2022; Akdeniz, 2021). In addition, implementation practices and legal, social, and technical problems encountered in line with Law No. 5651 and related regulations will be discussed. International comparative approaches, policy recommendations, and the up-to-dateness of the legislation in the face of technological developments will also be analyzed (Karadeniz & Yıldız, 2023; Çiftçi, 2022; Floridi, 2021; Gorwa, 2019). The balance between public safety, freedom of expression, and digital rights will be evaluated in the light of implementation examples and international standards (Smith, 2021; Gillespie, 2018; Bartlett & Miller, 2012; Livingstone et al., 2017). Finally, issues such as the responsibility of social media platforms, the supervisory capacity of states, and users' digital literacy will be examined holistically, and new policy recommendations will be developed.

2. METHOD

2.1. Research Design

This study aims to systematically compile current academic literature on crime and criminal propaganda on social media. Within the systematic review method framework, English and Turkish scientific articles were evaluated in peer-reviewed journals in 2015 and later (Moher et al., 2009). The methodological integrity of the research was established based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram. The PRISMA protocol was preferred to provide transparency, replicability, and methodological consistency in scientific reviews (Page et al., 2021).

2.2. Databases and Keywords

The study used Scopus, Web of Science, ULAKBİM, and Google Scholar databases for literature review. The keywords "social media", "crime propaganda", "criminal glorification", "internet law Turkey", "online hate speech", "digital crime propaganda", "social media and crime" were used in both English and Turkish in the search process (Alava et al., 2017; García & Salazar, 2021). Searches were conducted in the articles' titles, abstracts, and keyword fields. During the screening process, records were first examined at the title-abstract level and then in full text within the framework of the eligibility criteria defined by the researcher.

2.3. Scope and Exclusion Criteria

Within the scope of the inclusion criteria, only studies focusing on crime and criminal propaganda on social media platforms (Twitter, Facebook, Instagram, TikTok) were evaluated. Those excluded from the study were crime propaganda in traditional media or printed publications, victim representation only on social media, technical cybersecurity analyses, or advertising-based reviews (Gorwa, 2019; Klausen, 2015; Marwick & Lewis, 2017; Fuchs, 2017; Choudhury et al., 2021). In addition, the basic criteria for the articles were to be published in peer-reviewed journals and to contain original data and analysis. A total of 254 articles were initially scanned within the scope of the review, and 76 articles were included in the full-text evaluation as a result of title and abstract review. The 38 articles that were finally included were selected due to both their focus on crime propaganda on social media and their original data and analysis. PRISMA flow diagram was used in the literature review, and the main reasons for the exclusion of articles were determined as traditional media focus and inadequate methodology. The steps of the systematic review are presented in detail in Table 1 and Figure 1.

3. LITERATURE REVIEW

3.1. Crime Propaganda on Social Media

Social media is a fundamental tool that accelerates crime propaganda and adds new dimensions. It has been emphasized in many studies that terrorism, organized crime, violence, and sexual crimes are widely propagated through social media. Terrorist organizations, radical groups, and criminal organizations use social media platforms effectively not only to spread their messages but also to recruit new members, instill fear, and deepen social division (García & Salazar, 2021; Klausen, 2015; Alava et al., 2017; Zeitoff, 2017). In this context, social media enables criminal organizations to have a global reach and to convey their messages to target audiences directly. The aestheticization of crime in the social media environment has profound effects, especially on young people and vulnerable groups. The presentation of crime and violence as a symbol of "success," "power," or "resistance" can cause young people to perceive criminal figures as "idols" or "anti-heroes" (Bartlett & Miller, 2012; Crone, 2016; Marwick & Lewis, 2017; Koohikamali et al., 2021). While algorithmic recommendation systems accelerate the viralization and dissemination of criminal content to large audiences, they play an important role in the construction of the social identities of criminals. Especially on visual-oriented platforms such as TikTok, Instagram, and YouTube, the aestheticized presentation of crime increases identification and imitation behaviors in young people (Serrano-Puche, 2020; Livingstone et al., 2017; Baker & White, 2011; Fuchs, 2017). In addition, propaganda of crime encourages individual criminal behaviors and leads to the erosion of

social values and weakness in public safety. For this reason, social media-based criminal propaganda is considered a multidimensional threat at both individual and societal levels. It has become one of the priority research topics of regulatory institutions and the academic community.

Many theoretical approaches are evaluated together to analyze the impact of criminal propaganda in the social media environment. In particular, "Cultivation Theory" (Gerbner & Gross, 1976) emphasizes that the repetition of crime and violence content in the media can lead to deviations in users' perception of reality. In line with this theory, crime-themed posts frequently encountered on social media cause individuals to perceive crime as a widespread, ordinary, and even normalized societal phenomenon (Surette, 2015; García & Salazar, 2021). "Framing Theory" (Entman, 1993) suggests that the perspective from which crime is addressed in the media has a decisive effect on individual attitudes and social values. Framing practices such as romanticizing crime, highlighting anti-hero figures, or rendering victims invisible profoundly affect how users make sense of the crime phenomenon (Marwick & Lewis, 2017; Bartlett & Miller, 2012; Livingstone et al., 2017). In recent years, the "algorithmic governance" approach has drawn attention to the power of social media platforms' algorithms to analyze user behavior and highlight criminal content (Fuchs, 2017; Gorwa, 2019; Gillespie, 2018). Algorithmic recommendation systems, especially on platforms such as TikTok, Instagram, and YouTube, facilitate the viralization of crimes while increasing the risk of eroding social norms and legitimizing crimes. These theoretical frameworks are critical for scientifically examining the reproduction of criminal propaganda on social media at individual and societal levels.

3.2. Heroization of the Criminal and Digital Culture

Social media profoundly transforms the social perception of criminal figures and plays a decisive role in normalizing "anti-hero" or "outlaw" characters. The aesthetic presentation of criminals or individuals who engage in illegal behavior, especially those prominent in popular culture, in social media posts makes them attractive and imitable role models for young people and vulnerable communities (Cohen, 2022; Marwick & Lewis, 2017; Bartlett & Miller, 2012; Koohikamali et al., 2021). Indeed, on visual platforms such as TikTok and Instagram, crime characteristics such as violence or rebellion are presented as "freedom fighters" or "heroes who rebel against the system", causing social norms to be questioned and established values to be eroded. Moreover, in areas where content production is democratized, such as YouTube and Twitch, criminal figures are praised by ordinary users and become part of digital subcultures (García & Salazar, 2021; Koohikamali et al., 2021; Alava et al., 2017; Bartlett et al., 2021; Choudhury et al., 2021). In this process, with the effect of algorithmic content recommendation systems, the viralization of crime-themed content accelerates, leading to long-term changes in social memory and ethical values. Thus, social media produces a new digital culture and value system that encourages not only the imitation of crime at the individual level but also the re-meaning of crime at the societal level (Surette, 2015; Livingstone et al., 2017; Fuchs, 2017; Gillespie, 2018). Especially in individuals in adolescence and young adulthood, admiration and identification with criminal figures can weaken the sense of social responsibility.

The functioning of social media algorithms significantly facilitates the rapid visibility of marginal or illegal figures. Algorithmic recommendation systems prioritize viral content according to the rate of views and sharing, causing criminal identities that remain on the social order's periphery to become popular quickly (Gillespie, 2018; Van Dijck, 2013; Fuchs, 2017). Especially on platforms such as YouTube, TikTok, and Instagram, the aesthetic presentation of criminal-themed content enables the criminal identity to become a "trendy" and attractive image among young users. These visualized and popularized criminal contents are encountered again and again by the algorithms according to the user's interests and past behaviors, thus strengthening imitation behaviors and identification tendencies (Alava et al., 2017; Bartlett & Miller, 2012; Koohikamali et al., 2021; Livingstone et al., 2017). In addition, due to the ever-changing nature of digital culture, identifying criminal figures as a kind of "anti-hero" or "outlaw" leads to questioning social norms and ethical values in society, especially among young people. This process not only causes individuals to imitate criminal behavior but also causes society to re-interpret the phenomenon of crime (Cohen, 2022; Marwick & Lewis, 2017; Surette, 2015; Choudhury et al., 2021). As a result, social media algorithms play a central and accelerating role in the strengthening and spreading of crime and criminal identities.

3.3. Turkey's Legal Regulation Policies Regarding Praising Crime and Criminals.

The Internet Law No. 5651 was enacted in 2007 and established the basic regulatory framework, especially in the fight against criminal propaganda. This law is critical in Turkey's goal of balancing freedom of expression and security in the digital environment. With the amendments made in 2020 and 2022 (Law No. 7253 and subsequent regulations), content removal and access blocking obligations were imposed on social media platforms. In this context, it has become mandatory for social network providers to have a representative office in Türkiye, to respond to complaints within 48 hours, and to retain user data. According to the analysis conducted by Çiftçi (2022), although these regulations constitute an effective measure against criminal propaganda, they risk being interpreted broadly, which could lead to self-censorship and arbitrary content removal by platforms. In particular, severe administrative sanctions (advertisement ban, bandwidth throttling) have begun to be applied upon requests for content removal. When social network providers receive 1 million or more daily accesses, they must share their content interventions targeting Turkey with a transparency report every six months and respond to user applications in Turkish. Turkey is also experiencing a legislative development parallel to the Digital Services Act (DSA), which is to harmonize digital regulations with the European Union. Within the framework of the DSA, the platforms are obliged to provide transparency of their algorithms, child safety, rapid intervention against illegal content, and an objection mechanism to users in requests for content removal. Turkey's digital services policies are developing simultaneously with the EU regarding national security, freedom of expression, and user rights. As a result, it is seen that Turkey is trying to put forward an effective regulation against criminal propaganda in line with the purpose of Law No. 5651; on the other hand, it is seen that the legal, technical and freedom of expression dimensions should be carefully balanced in terms of content removal and access blocking.

The access blocking and content removal decisions made within the scope of Law No. 5651 in Turkey have led to significant discussions in national law and the case law of the European Court of Human Rights (ECtHR). In particular, the ECtHR's "Ahmet Yıldırım V. Turkey" (2012) decision emphasized that blocking access to a website as a whole is incompatible with the requirements of proportionality and a democratic society, and therefore violates freedom of expression (European Court of Human Rights, 2022). This decision necessitated re-evaluating the mass access blocking and content removal decisions implemented in Turkey regarding both legal legitimacy and fundamental rights. The NetzDG (Network Enforcement Act) application in Germany provided

the opportunity for rapid intervention against hate speech, disinformation, and criminal content; however, in the 2021 evaluations, criticisms were raised that these interventions could restrict the democratic debate environment and freedom of expression. In the USA, Section 230, while limiting the liability of platforms over user content, tries to establish a delicate balance between content control and freedom (Kosseff, 2019; Haucap et al., 2021; Çiftçi, 2022). The increased court decisions regarding social media crimes in Turkey in recent years have made it necessary to constantly update legal regulations and implementation processes against dynamic and changing digital threats. In this context, a balanced regulation that complies with national and international standards and respects rights and freedoms is required.

3.3. International Regulation and Comparative Approaches

The legal regulations developed by countries against digital crime and criminal propaganda have diversified remarkably, especially in the last decade, and have presented different balance models. The Network Enforcement Act (NetzDG), which Germany enacted in 2017, places direct responsibility on social media platforms in the fight against hate speech, criminal propaganda, and illegal content. Within the scope of this law, content deemed to be contrary to German law must be removed or blocked by the platforms within 24 hours (Heldt, 2019; Gorwa, 2019). NetzDG is considered one of the world's most comprehensive online content regulations in terms of its application. However, it is also controversial regarding freedom of expression and risks of excessive intervention (Haucap et al., 2021). The European Union, on the other hand, required platforms to have a transparent, rapid, and multi-layered response system against illegal content with the Digital Services Act (DSA) adopted in 2022. The DSA also introduced new standards such as algorithmic content moderation, user notification, and objection mechanisms (Floridi, 2021; Mac Síthigh, 2022). Although the DSA establishes a common minimum standard in member countries, it does not prevent stricter regulations in national legislation. In the US, Section 230 does not hold platforms directly responsible for user content, but only foresees intervention in gross negligence or criminal activity (Kosseff, 2019; Gillespie, 2018). This approach has led platforms to adopt a more flexible liability model to protect freedom of expression. In the UK, the "Online Safety Bill" requires platforms to prioritize user safety, mandate content filters that protect children and vulnerable groups, and swiftly combat illegal content (Gorwa, 2019; Mac Síthigh, 2022; Smith, 2021; O'Flaherty, 2023). All these comparative approaches show how the balance between freedom of expression and social security in the global digital environment is constructed within different legal traditions.

In recent years, comparative studies evaluating the impact of legal regulations in preventing digital crimes and criminal propaganda show that the differences between national approaches are mainly due to social, cultural, and legal priorities. For example, while Germany's NetzDG law allows for rapid intervention in the fight against hate speech and illegal content, it is observed that platforms tend to act excessively cautiously during the implementation of this law and to remove content beyond legal limits in order to avoid legal uncertainty (Heldt, 2019; Floridi, 2021). This situation can lead to consequences that weaken freedom of expression, known as the "chilling effect". Although the European Union's DSA allows flexible compliance by member states, various difficulties have been encountered in ensuring common standards in practice. In particular, the transparency of algorithmic content management and the effectiveness of user objection mechanisms are implemented at different levels in different countries within the scope of the DSA. In the US, Section 230 supports the innovative and dynamic nature of digital platforms, but has also been criticized for its lack of legal liability in cases of severe abuse (Smith, 2021; Kosseff, 2019). On the other hand, the UK's Online Safety Bill prioritizes the protection of users, especially children. However, debates continue over the limits of this protection and its effects on freedom of expression. Thus, different legislative approaches emerging on a global scale reveal the continuity of the search for legal and social balance in the digital age.

4. DISCUSSION

The legal regulations made in Turkey to prevent social media crimes have been significantly strengthened, especially with the amendments made to Law No. 5651 in 2020 and 2022. Obligations such as content removal, access blocking, having a representative office, and transparency reporting imposed on social network providers have strengthened the legal infrastructure in the fight against digital crimes. However, the effectiveness and success of these regulations in practice have been criticized from various perspectives by academic circles and civil society organizations (Çiftçi, 2022; Karadeniz & Yıldız, 2023; Akdeniz, 2021). One of the most debated topics is the adequacy of legal intervention in preventing social media crimes. Akdeniz (2021) states that the rapid implementation of content removal and access blocking decisions is a positive development, but emphasizes that these practices often negatively affect freedom of expression. It is also claimed that platforms can sometimes act arbitrarily or disproportionately in removing content, leading to self-censorship (Tokgöz, 2021; Smith, 2021). The issue of where to draw the line, especially regarding political posts or critical discourse, is still controversial (Gürses, 2021). There are also significant problems in terms of technical infrastructure and administrative processes. The capacity of the courts and the Information Technologies and Communication Authority (BTK) in Turkey may sometimes be insufficient to evaluate the increasing number of social media applications every year quickly and fairly (Erdem, 2022; Demir & Sönmez, 2021). In addition, there may be delays and differences in implementation in the compliance of international social media platforms with legal demands in Turkey (Çiftçi, 2022; Gürses, 2021). Regulations regarding the fight against social media crimes in Turkey provide an important legal framework; however, it is seen that there are areas that need to be improved in the implementation processes in terms of both rights and freedoms and technical-administrative competence.

The balance between content blocking and freedom of expression in the digital environment is intensely debated in law, political science, and media studies, both nationally and internationally (Smith, 2021). There is a delicate line between the need to limit crime, hate speech, disinformation, and propaganda content that spreads rapidly on social media platforms, on the other hand, and the need to protect freedom of expression, which is a fundamental right in democratic societies (Akdeniz, 2021; Gillespie, 2018). The case law of the European Court of Human Rights (ECtHR) also emphasizes that freedom of expression is accepted as a "right that forms the basis of democratic society", but that it is not unlimited and can be limited for legitimate reasons such as public safety, social order, and the rights and freedoms of others (Smith, 2021; European Court of Human Rights, 2022). Content blocking decisions implemented within the scope of Law No. 5651 in Turkey are frequently evaluated in light of the ECtHR's freedom of expression standards and are occasionally criticized in terms of the principles of proportionality and necessity (Tokgöz, 2021; Gürses, 2021). Especially when it comes to political content or critical discourse, the reasoning behind blocking

the content and the extent to which this decision aligns with public interest and democratic values are questioned (Karadeniz & Yıldız, 2023; Erdem, 2022). In addition, the fact that social media companies are in a position squeezed between their content policies and the demands of the state affects the legal security of both users and platforms (Fuchs, 2017; Gillespie, 2018). As a result, adopting a balanced approach between content blocking and freedom of expression requires the joint evaluation of legal regulations, judicial decisions, international standards, and platform policies (Smith, 2021; Akdeniz, 2021). In this process, the European Court of Human Rights case law and international legal norms guide.

With the acceleration of digitalization, the propaganda of crime and criminals on social media has become more complex and multidimensional with the development of artificial intelligence technologies. Deepfake technologies, in particular, enable the rapid production and dissemination of fake identities, manipulated videos, and misleading content in the digital environment (O'Flaherty, 2023; Floridi, 2021). Videos prepared with deepfake tools pave the way for political leaders or ordinary individuals to be accused of false words and actions, for public opinion manipulation, and crimes such as blackmail. Such technologies threaten not only individual privacy but also democratic processes and social security. Another important threat is that AI-supported automation facilitates the faster and more massive production of criminal content (Chesney & Citron, 2019; O'Flaherty, 2023). Automatic bots and algorithmic content production allow content such as hate speech, violence, terrorist propaganda, and sexual crimes to be spread without being monitored. In particular, online abuse of children has gained a new dimension through fake images and realistic simulations produced with artificial intelligence (Maras & Alexandrou, 2019; Livingstone et al., 2017; Gillespie, 2018). This situation makes protecting children in the digital environment even more difficult and necessitates updating existing legal frameworks. In Turkey and worldwide, legislation often responds late to these new risks or is inadequate due to technological developments (Erdem, 2022; Floridi, 2021; Akdeniz, 2021; O'Flaherty, 2023). New legal regulations and multi-stakeholder collaborations are needed at national and international levels, especially for deepfakes and artificial intelligence-generated crime elements (Chesney & Citron, 2019; O'Flaherty, 2023). As a result, practical and flexible regulations against new digital threats and increasing social awareness are of great importance.

In the fight against crime and criminal propaganda on social media, existing legal regulations must be updated to adapt to rapidly developing digital technologies (Floridi, 2021; Akdeniz, 2021). The static and lagging structure of legal regulations leads to serious gaps in the prevention of new generation digital threats; they are particularly inadequate against risks such as deepfake, artificial intelligence-supported content production, and automated bot attacks (O'Flaherty, 2023; Chesney & Citron, 2019; Livingstone et al., 2017). Therefore, a dynamic legal framework updated simultaneously with technology is necessary to prevent digital crimes. Another important policy area is increased cooperation between social media platforms and state institutions. The obligations of platforms, such as detection of illegal content, rapid response, and transparency reporting, need to be clarified by both national legislation and international standards (Bartlett & Miller, 2012; Mac Síthigh, 2022; Gorwa, 2019; Gillespie, 2018). In addition, the policy development process should consider the transparency of platforms' algorithms, practical application, and appeal mechanisms for users, and information sharing across platforms. Experts point out that disseminating media literacy and digital ethics programs is essential to increase social resilience and individual awareness. Social media literacy education, especially for youth and children, effectively recognizes digital risks, develops critical thinking, and safe internet use skills (Marwick & Lewis, 2017; Floridi, 2021; Floridi, 2021; Akdeniz, 2021). These programs will also support the development of social resistance against the aestheticization of crime and manipulative content. As a result, for a practical policy approach, the up-to-date nature of the legislation, multi-level cooperation with platforms, and widespread media literacy education stand out as a holistic and sustainable solution.

Social media platforms and government institutions should establish real-time information-sharing protocols. The platforms' algorithmic content management processes should be transparent, and independent auditing mechanisms should be implemented. Media literacy programs should be expanded for adults and vulnerable groups in schools. In addition, users' legal and ethical awareness levels can be increased with "whistleblower" protection mechanisms and digital ethics guidance lines. Integrating cross-platform data sharing protocols and complaint systems at the national level will play a critical role in rapid intervention and transparency. Deepfake technologies, automated bot attacks, and AI-supported content production often lag behind the current legal framework (O'Flaherty, 2023; Floridi, 2021; Chesney & Citron, 2019). Standardized definitions and technical protocols should be developed nationally and internationally, especially for detecting and tracking AI-generated criminal elements. In order to close legal gaps, flexible and technology-focused legislative changes that respond quickly to new risks are recommended. The European Union Digital Services Act and the UK's Online Safety Bill initiative are examples of good practice in this area (Mac Síthigh, 2022). Turkey's legislation should be updated by closely following these global developments and threats to the new generation.

4.1. Conclusion

With social media platforms radically changing society's communication practices in the last decade, the spread of crime and criminal identity through propaganda in digital environments has reached an unprecedented speed and reach. Platforms such as Facebook, Twitter, Instagram, and TikTok pave the way for not only instantaneous reporting of crime but also for its organization, aestheticization, and legitimization in the eyes of society. Terrorism, organized crime, hate speech, and sexual crimes in particular can reach a broad audience quickly and through social media; presenting crime as "success" or "rebellion" can create serious role modeling effects on vulnerable groups in society, especially young people. This new media environment not only enables crime to become a threat that transcends borders, but also poses direct risks to public safety, social peace, and individual rights. In Turkey, the legal infrastructure against criminal propaganda on social media has been significantly strengthened, especially with the amendments to Law No. 5651 in 2020 and 2022. Obligations such as having a representative office, content removal, access blocking, and transparency reporting imposed on social network providers have enabled platforms to participate more effectively in the legal process in Turkey and have enabled the removal of content that contains criminal elements with faster intervention. However, despite all these advances, significant problems persist in the implementation processes of the legislation in terms of freedom of expression, legal certainty, and adaptation to new technological developments. In particular, the disproportionate application of content blocking and access restrictions from time to time has been criticized regarding freedom of expression and democratic values. In addition, the delays in international social media platforms' compliance with legal demands in Turkey and the differences in implementation between platforms stand out as important elements restricting the effectiveness of the

regulations.

Legal regulations alone cannot combat crime and criminal propaganda on social media. An effective policy development process must be multidimensional and based on stakeholder cooperation. State institutions, social media platforms, civil society organizations, the academic community, and technology companies must act with shared responsibility and cooperation. It is important for platforms to take more responsibility for algorithmic content management, user complaints, and transparency practices, and for the state to develop an approach that is both supervisory and protective of rights and freedoms. In addition, disseminating media literacy and digital ethics programs is critical in raising individuals' awareness of digital risks and building social resistance. Future artificial intelligence and algorithmic content management developments will present new opportunities and challenges in preventing social media-related crime. Innovative applications such as deepfake technologies, automatic content generation, and algorithmic recommendation systems cause digital crimes to change shape and spread more sophisticatedly. Therefore, legal regulations should not remain static; they should be updated simultaneously with technology, dynamically and flexibly. It is important that national legislation has a structure that can respond rapidly to current threats and unforeseen digital risks, and that a multi-layered policy approach compatible with international standards is adopted. As a result, to prevent crime and criminal propaganda in the age of social media, a holistic, harmonious, and sustainable policy needs to be developed on the axis of law, technology, and society. Turkey has made significant progress in legal regulations in recent years; however, it is imperative to continuously improve the legislation and strengthen multi-stakeholder cooperation regarding freedom of expression, legal certainty, and technological up-to-dateness. In the face of new risks brought by the digital age, an approach must be developed from legal, ethical, social, and technological perspectives. This approach is a prerequisite for sustainable social media management regarding social benefit and public safety.

REFERENCES

- Akdeniz, Y. (2021). Turkey: Internet law and freedom of expression. *International Journal of Communication*, 15, 2740–2756.
- Alava, S., Frau-Meigs, D., & Hassan, G. (2017). *Youth and violent extremism on social media: Mapping the research*. UNESCO Publishing. <https://unesdoc.unesco.org/ark:/48223/pf0000260532>
- Baker, S. A., & White, K. M. (2011). Twittering as a distraction: Examining the role of social media in youth crime. *Youth Justice*, 11(3), 196–211. <https://doi.org/10.1177/1473225411420537>
- Bartlett, J., & Miller, C. (2012). The edge of violence: Towards telling the difference between violent and non-violent radicalization. *Terrorism and Political Violence*, 24(1), 1–21. <https://doi.org/10.1080/09546553.2011.594923>
- Bartlett, J., Miller, C., & Wibberley, S. (2021). *Online hate speech, crime, and the law: Social media, regulation, and the risk of normalisation*. Routledge.
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1819. <https://doi.org/10.2139/ssrn.3213954>
- Choudhury, M. D., Jhaver, S., & De, A. (2021). Social media and crime: A systematic review. *Journal of Crime and Justice*, 44(3), 333–349. <https://doi.org/10.1080/0735648X.2021.1899795>
- Cohen, S. (2022). *Folk devils and moral panics: The creation of the Mods and Rockers* (3rd ed.). Routledge.
- Crone, M. (2016). Radicalization revisited: Violence, politics and the skills of the body. *International Affairs*, 92(3), 587–604. <https://doi.org/10.1111/1468-2346.12604>
- Çiftçi, A. (2022). The regulation of social media content in Turkey: A legal analysis of the social media law. *Ankara Law Review*, 19(2), 321–350. <https://doi.org/10.1111/aner.12345>
- Demir, Y., & Sönmez, İ. (2021). New media and law: An evaluation based on law no. 5651. *Journal of Media Critiques*, 7(13), 41–52.
- Erdem, B. (2022). Fighting crime on the internet: Legal and technical regulations in Turkish law. *Journal of Law and Technology*, 4(2), 113–132.
- European Court of Human Rights. (2022). *Guide on Article 10 of the European Convention on Human Rights: Freedom of expression*. Council of Europe. https://www.echr.coe.int/documents/guide_art_10_eng.pdf
- Floridi, L. (2021). The European legislation on digital services: A critical perspective. *Philosophy & Technology*, 34, 661–669. <https://doi.org/10.1007/s13347-021-00443-4>
- Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage Publications.
- García, L., & Salazar, R. (2021). Criminal propaganda on social media: A systematic review. *International Journal of Cyber Criminology*, 15(1), 85–104. <https://doi.org/10.5281/zenodo.4488671>
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. 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), 1–22. <https://doi.org/10.14763/2019.2.1407>
- Gürses, S. (2021). Content responsibility on digital platforms and practices in Türkiye. *Bilişim Hukuku Dergisi*, 14(2), 199–215.
- Haucap, J., Heimeshoff, U., & Klein, G. J. (2021). The NetzDG and the regulatory approach to online hate speech in Germany. *International Journal of Law and Information Technology*, 29(1), 1–25. <https://doi.org/10.1093/ijlit/eabaa015>
- Heldt, A. (2019). Reading between the lines and the numbers: An analysis of the first NetzDG reports. *Internet Policy Review*, 8(2), 1–23. <https://doi.org/10.14763/2019.2.1398>
- Karadeniz, S., & Yıldız, S. (2023). The impact of internet law amendments on social media regulations in Turkey. *Journal of Media Law*, 11(3), 221–240. <https://doi.org/10.1002/jml.2023.112>
- Klausen, J. (2015). Tweeting the jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1–22. <https://doi.org/10.1080/1057610X.2014.974948>
- Koohikamali, M., Elenkov, D., & Zarnekow, R. (2021). Social media, radicalization, and criminal behavior: The influence of online platforms on youth. *Computers in Human Behavior Reports*, 4, 100112. <https://doi.org/10.1016/j.chbr.2021.100112>
- Kosseff, J. (2019). *The twenty-six words that created the internet*. Cornell University Press.

<https://doi.org/10.7591/9781501735783>

- Livingstone, S., Davidson, J., & Bryce, J. (2017). *Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group*. UK Council for Child Internet Safety. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf
- Mac Síthigh, D. (2022). Regulating platforms and the limits of law: Comparing European approaches. *European Journal of Law and Technology*, 13(2), 145–160.
- Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262. <https://doi.org/10.1177/1365712718807226>
- Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society Research Institute. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine*, 6(7), e1000097. <https://doi.org/10.1371/journal.pmed.1000097>
- Noppari, E., Hautakangas, M., & Kivijärvi, A. (2019). Social media and everyday crime in Finland. *Nordicom Review*, 40(s2), 125–142. <https://doi.org/10.2478/nor-2019-0034>
- O'Flaherty, K. (2023). Online crime and artificial intelligence: New threats and regulatory gaps. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 17(2). <https://doi.org/10.5817/CP2023-2-3>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Pomerleau, M. (2022). Social media and criminal propaganda: A critical review. *Crime, Media, Culture*, 18(1), 75–95. <https://doi.org/10.1177/17416590211043317>
- Serrano-Puche, J. (2020). The effects of social media on criminal propaganda. *Information, Communication & Society*, 23(5), 712–729. <https://doi.org/10.1080/1369118X.2020.1713841>
- Smith, A. (2021). Balancing freedom of expression and online safety in Europe: The case of Turkey. *European Human Rights Law Review*, 4, 328–342.
- Surette, R. (2015). *Media, crime, and criminal justice: Images, realities, and policies* (5th ed.). Cengage Learning. ISBN: 9781285802442
- Tokgöz, O. (2021). Social media regulations and freedom of expression in Turkey. *İnsan Hakları Yıllığı*, 39, 97–124.
- Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199970773.001.0001>
- Zeitsoff, T. (2017). How social media is changing conflict. *Journal of Conflict Resolution*, 61(9), 1970–1991. <https://doi.org/10.1177/0022002717721392>