ISSN: 2723-9535

Available online at www.HighTechJournal.org

HighTech and Innovation Journal

Vol. 5, No. 1, March, 2024

Sociological Impact of Cyber Laws on Media: Virtue Community and Controversies

Sayid Muhammad Rifki Noval [1]*

[1] *Universitas Pasundan, Bandung, West Java Province, 40154, Indonesia.*

Received 25 May 2023; Revised 17 January 2024; Accepted 08 February 2024; Published 01 March 2024

Abstract

This study aims to delve into the sociological dimensions and repercussions of cyber law on cyber-based mass media and social media freedoms in Indonesia while shedding light on questionable aspects of the country's cyber laws. Employing qualitative research methods encompassing theoretical and investigative perspectives, the study combines normative juridical research with a legal, sociological approach and an observational survey approach. Data collection involved an examination of legal materials on information technology alongside interviews with cyber-policymaking bodies, stakeholders, cyber-media houses, journalists, bloggers, and social media influencers. The collected data were scrutinized through descriptive analysis to clarify the sociological and legal impacts of Indonesia's cyber law on media and social media. The findings reveal that implementing cyber law in Indonesia carries substantial sociological implications for both the media and society. It highlights questionable aspects of the existing cyber laws, as they pose challenges to upholding the rule of law and safeguarding social and media freedoms in the country. The insights derived from this study hold relevance for research endeavors focusing on the sociological aspects of cyber law in developing countries. This study contributes to a deeper understanding of the evolving digital landscape and emphasizes the need to address pertinent issues while balancing legal regulations and societal freedoms.

Keywords: Sociological Implications; Cyber Law; Media Freedoms; Cyber-media; Developing Countries.

1. Introduction

Increased internet connectivity has facilitated significant growth and enhanced online activity among Indonesians, leading to transformative changes in the media landscape. The advent of the internet has brought about numerous new phenomena, enabling the dissemination of information with increasing freedom and empowering individuals to wield influence over the media. However, this rise in communication technology has also raised concerns regarding social monitoring, necessitating the development of adaptable information tools [1].

Social media platforms have become popular for individuals to voice their ideas and opinions [2]. Beyond mere entertainment, social media interactions such as links, trivia, polls, ratings, and other online engagement activities strengthen social connections and offer communities a unique window into the perspectives of others daily [3]. In response, local governments in Indonesia have been compelled to balance accountability, transparency, accessibility, and service delivery. The increased civic participation facilitated by social media plays a vital role in promoting democratic avenues of community engagement and civic responsibility, ultimately enhancing government service delivery [4].

* Corresponding author: sayidrifqi@unpas.ac.id

doi http://dx.doi.org/10.28991/HIJ-2024-05-01-04

Both society and governments have embraced social media, with the latter utilizing these platforms to provide complementary channels for information sharing, connection, and engagement. By allowing individuals to contact governments and government officials, social media enables more informed decision-making processes [4, 5]. This improved communication has enabled local governments to receive valuable insights and better understand residents' perspectives, enhancing operational efficiency and effectiveness [5].

Governments and businesses have also leveraged social media to categorize and forecast public sentiments by analyzing the content and feedback posted on these platforms [6]. Governments can determine suitable solutions and address public concerns by understanding the public's views on various issues [5]. While the increased connection and public acceptance of social media have yielded significant development benefits and increased citizen involvement in Indonesia, they have also given rise to problematic issues. In response, the Indonesian government has sought to address these concerns, leading to the emergence of questionable aspects that have impacted society. This study explores the sociological impact of cyber laws on media, specifically focusing on the Virtue Community and controversies in Indonesia. The study combines normative juridical research and an observational survey approach by employing qualitative research methods encompassing the theoretical and investigative perspectives. Data collection involves examining legal materials related to information technology and conducting interviews with key stakeholders, including cyber-policymaking bodies, cyber-media houses, journalists, bloggers, and social media influencers.

There has been little published study on the social effects of cyber laws on media freedoms in Indonesia. Previous research on relevant themes, such as the use of social media in government communication and local government service delivery in underdeveloped countries, has been conducted [3, 5]. These studies have underlined the importance of social media in promoting democratic participation, enhancing government operations, and gauging public mood. Nonetheless, there is a knowledge deficit on Indonesia's unique sociological effects of cyber laws on media and social media freedoms. This study seeks to address that void by conducting an in-depth topic analysis.

2. Literature Review

2.1. Virtue Community Social Aspects of Cyber Law

The sociology of cyber law comprises a variety of techniques that investigate the function of cyber law within society, drawing on the underlying notion of the sociology of law. The empirical analysis and understanding of the complex relationships between cyber law, legal features, institutions, and social issues are central to this field of study [7, 8]. It delves into a variety of socio-legal topics, such as the social growth of legal institutions, forms of social control, legal regulation, the interaction of legal cultures, the social construction of legal concerns, the legal profession, and the link between law and society [9–11]. To improve its knowledge of legal phenomena, the sociology of law frequently depends on research from other disciplines, such as comparative law, legal theory, law and economics, and law and literature [12–14]. Within the multidisciplinary landscape of legal analysis, sociological elements focus on institutional dynamics shaped by social and political contexts, thereby contributing to the shaping and influence of legal norms [15].

In everyday life, common societal discourse is a practical guide for individuals despite not being grounded in empirical science. This discourse does not strictly differentiate between facts and values, leading to evaluations of reality as statements about the current situation and what is considered just [16–18]. For instance, "cyber" in common societal discourse may be associated with digital devices and the internet, while "illegal" conveys something that should be avoided or reported to authorities. The sociology of law views law as a measurable variable, where changes in social control by authorities correspond to changes in this variable [16, 19]. Its goal is to predict and explain variations in the quantified aspects of law, considering the specific social context, the individuals involved, their relationships, and the broader societal setting in which their interactions occur [16, 20]. In contrast to the general perception of law found in citizens' discourse, the sociology of law highlights the significance of the criminal or illegal element in understanding citizens' reporting behavior and emphasizes the importance of the seriousness of activity in determining the likelihood of reporting it to authorities [16, 19, 21].

The law, including cyber law, is designed to bring control, governance, guidance, and order to society. The interactions between different aspects of the law, society, and the internet have been extensively studied in previous research. By examining these interplays, scholars have gained insights into the complex dynamics and implications of legal frameworks in the digital age.

2.2. Cyber Mass Media

Like other sectors, the mass media recognized the necessity of moving their activities online, although not without concerns. Cyberspace brought new technologies and socio-legal and political developments that blurred the line between media elites, mediocrity, and even less reputable sources. Scholars argued that the institutional and technological contexts in which journalism operates are influenced by cyberspace, potentially reshaping the definition of journalism itself and its relationship with the audience [22–26].

While cyber media strengthens democracy, it is not without challenges. Power elites can exploit it to defend their viewpoints and exert more effective control, leading to an interweaving of the media and society [25, 27]. In developing countries, the question arises as to whether the majority of society possesses sufficient digital literacy to navigate through real mass media platforms and social media amidst the influx of distracting paid content [28]. Additionally, the lack of user data protection laws and policies in many developing countries has fostered reluctance among individuals to share personal information online, which poses challenges for media outlets that rely on subscriptions to distribute their content. The need for ethical cyber media management regarding social issues has become increasingly apparent to media outlets [29]. In Indonesia, collaboration between the Indonesia Press Board, media organizations, academia, and civil society led to the establishment of cyber-media news coverage rules in 2012, governed by Law Number 40 Year 1999 on the press and journalistic ethics. These standards require periodic assessments of sensitive and challenging topics in news coverage [28]. Criticism has been directed at recent media freedoms in Indonesia due to incidents where government censorship and internet shutdowns were employed, often on the grounds of national security or moral concerns [30, 31].

Maintaining the public's trust in cyber media requires unbiased and accurate reporting that reflects the reality of events rather than favoring specific organizations or political perspectives. Concerns about questionable news reporting tendencies, particularly in online media, have deviated from established journalistic ethics, prompting calls to review news coverage regulations. Despite the large number of Indonesian cyber-media outlets, only 68 are formally registered and adhere to the rules set by the Indonesian Press Board [28]. Dissatisfaction within segments of society and the media fraternity persists regarding the coverage of contentious issues by cyber-media outlets, leading to ongoing discussions and potential sanctions for publishers who breach Indonesian laws [30].

2.3. Social Media

Social media, characterized by high decentralization and virtual organization, has become a collection of technologies that facilitate detailed data exchange in a virtual environment [32, 33]. Policymakers recognize the potential of social media to enhance information management, increase transparency, and foster user collaboration during decision-making processes [34]. The widespread usage of social media in industrialized emerging economies like Indonesia is evident, with a growing number of wireless access users, particularly among the younger population. Indonesian culture has embraced social media platforms, permeating various social, economic, and political aspects, especially in urban areas [31, 35]. Social media serves as a platform for expression, communication, and public policy integration, allowing active accounts to publish content that facilitates communication [36]. The extensive internet usage in Indonesia, with an estimated 142.8 million users, highlights the significant presence of social media and its impact on society (Masduki, 2022). Transparency is crucial in generating ideas, raising finance, and improving decision-making processes [37]. Social media networks can deliver timely and accurate data by encouraging meaningful interaction among individuals involved in decision-making [38].

The role of social media as a news source has grown, providing instantaneous and widespread access to the most recent coverage and catering to specific user interests and demographics [39, 40]. Social media platforms offer the possibility of microblogging to niche audiences, enabling users to publish content with the power and influence of a media house without the traditional responsibilities [41]. The increased use of social media has raised expectations for civic involvement and political participation, highlighting Indonesia's active participation in social media [35, 42]. While social media platforms have been hailed for their potential to foster citizen involvement, civic dialogue, and transparency, critical voices have emphasized the negative effects of surveillance, privacy invasion, misinformation, and extremist online communities [35]. Social media has facilitated the spread of harmful content, including fake news and divisive ideologies, amplifying societal problems and crimes [30, 43]. Instances of blasphemy trials in Indonesia exemplify the controversies surrounding cyber law and the country's struggles with social media and the internet [30].

The rise of social media and cyberspace in Indonesia has brought about social and political issues, exacerbating existing societal divisions and challenges within the political, social, and economic systems [30]. However, the policy responses of the Indonesian government to these challenges raise concerns regarding the rule of law and the preservation of societal and media freedoms.

3. Research Methodology

This study used a qualitative approach, combining normative legal research and observational surveys. The normative legal research component involved an extensive review of primary and secondary sources obtained through library research. This approach allowed for a comprehensive examination of relevant legal materials. Additionally, the study incorporated observational survey research, a reliable method for capturing the current and prevalent conditions at a specific time. Using this technique, the study obtained accurate and trustworthy information to support its findings [44].

3.1. Study Sample

The population for this study consisted of three cyber-policy regulatory bodies in Indonesia, three mass media organizations with active online publishing platforms, three bloggers, and three active social media users/influencers. Purposive sampling was employed to determine the study sample. This sampling method was chosen to ensure easier access to the sub-group of individuals and organizations involved in cyber-policymaking, cyber-law, and cyber-media activities who possess valuable information related to the research objectives. The study sample was specifically selected from bodies recognized as key custodians of cyber-law in Indonesia and from organizations and individuals actively engaged in cyber-media activities.

3.1.1. Cyber-law Custodial Bodies

The unit of analysis for this study was organizations; therefore, data were collected from the leadership of each organization to represent their respective organizations best. The organizations included the Indonesia Security Incident Response Team on Internet and Infrastructure (Id-SIRTII), established in 2007 as an independent state body responsible for monitoring cyber threats and handling legal matters related to cyber disputes. The Directorate of Information Security and Cryptography, established in 2010 under the Ministry of Communication and Information Technology (MCIT), was another organization included in the study. The national cyber authority, Badan Siber dan Sandi Negara (BSSN), which centrally coordinates Indonesia's cyber governance across the government, was also part of the study. As the organization was the focus of analysis, the information gathered from the heads of these organizations was considered representative of the required data from each organization.

3.1.2. Cyber-media Operatives

The units of analysis in this study were organizations and individuals. The information collected from the heads of these units was considered reflective of the necessary data to make informed decisions. The organizations included mass media organizations with online publication platforms, while the individuals comprised bloggers and active social media influencers. It is important to note that the anonymity of this population was maintained as per the respondents' request. This was done to protect them from any potential consequences that may arise after the publication of this study.

3.2. Data Collection

The literature reviewed for this study primarily consisted of online sources focusing on Indonesian cyber-law, the social aspects of cyber-law, and the role of mass media and social media in Indonesia. During the interviews, specific questions were posed to the cyber-law custodial bodies, as outlined in Table 1. Similarly, Table 2 presents a selection of questions directed toward the individuals identified as cyber-media operatives. The structured questions were designed to gather information directly related to the study's scope and objectives.

Table 1. Some of the questions were directed to respondents from cyber-law custodial bodies

1.	What Indonesian legislation constitutes cyber law?
2.	How does Indonesian law enforcement identify and designate an online activity as illegal?
3.	What is the legal basis for censoring the internet and or internet content?
4.	Why is Indonesia not having a data protection law?
5.	How is the Indonesian legal system dealing with disinformation?

Table 2. Some of the questions were directed to respondents from cyber-law custodial bodies

1.	What does Indonesian cyber law as a cyber-media organization?
2.	What legal implications do you deal with as social media operative in Indonesia?
3.	Are you free to publish any content you wish as an online publisher in Indonesia?
4.	How do you deal with disinformation, a social media operative?
5.	What is your take on data protection in Indonesia?

Here is a brief description of the methodology process:

1. Begin the qualitative study by combining normative legal research and observational surveys.
2. Define the study sample: three cyber-policy regulatory bodies, three mass media organizations, three bloggers, and three social media users/influencers.
3. Collect data from the selected organizations' leadership and individuals involved in cyber-media activities.

4. Conduct normative legal research by extensively reviewing primary and secondary sources related to Indonesian cyber-law, social aspects of cyber-law, and the role of mass media and social media in the country.
5. Use observational surveys to capture current and prevalent conditions related to the research objectives.
6. Pose specific questions to the cyber-law custodial bodies, focusing on topics such as Indonesian legislation constituting cyber-law, identification of illegal online activities, the legal basis for internet censorship, the absence of data protection law in Indonesia, and the handling of disinformation by the legal system.
7. Pose specific questions to the cyber-media operatives, addressing their understanding of Indonesian cyber-law, legal implications faced as social media operatives, freedom to publish content as online publishers, approaches to dealing with disinformation, and perspectives on data protection in Indonesia.
8. Gather interview responses and data to support the study's findings and analysis.
9. Analyze the collected data, incorporating the information obtained from normative legal research and observational surveys.
10. Interpret the findings and conclude the sociological impact of cyber laws on media in Indonesia.
11. Based on the study's results, discuss the questionable issues in Indonesia's cyber law.
12. Emphasize the need for safeguards, comprehensive measures, and a balanced approach to cyber law that upholds media freedoms while addressing societal concerns.
13. Provide recommendations for policymakers and stakeholders to enhance cyber-law frameworks and preserve democratic principles and societal cohesion.

4. Results

4.1. From Cyber-law Custodial Bodies

The collected data revealed that the custodial bodies responsible for cyber-law in Indonesia have distinct roles, including formulating and drafting cyber-laws and policies, monitoring the internet for cyber threats, and handling legal matters arising from cyber activities. The findings highlight that Information and Transaction Electronic Law (ITE Law) No. 11/2008 served as the initial framework for cyber law in Indonesia and was pivotal in shaping cyber-related governance and discourse in the country.

The results also indicate that Indonesian law enforcement identifies illegal cyber activity through various processes, including receiving victim complaints, online monitoring and surveillance, and collaborations with civil society organizations, the private sector, and academia. The investigation of cases typically involves forensic analysis of digital systems belonging to alleged perpetrators to gather sufficient evidence for prosecution. This process may encompass witness testimonies, interaction records, and cross-checking IP addresses with Internet Service Providers (ISPs) assistance. Additionally, criminal law and procedure provisions often address illicit cyber activity in Indonesia. Furthermore, the findings reveal that the enactment of the Law Against Pornography and Pornographic Acts, along with ITE Law No. 11/2008, provided legal grounds for Indonesia's Ministry of Communication and Information Technology (MCIT) to employ internet control mechanisms, utilizing ISPs to censor or block content.

Despite the significant amount of data generated by online activities in Indonesia's cyberspace, the country has yet to implement comprehensive data protection legislation. This study uncovers that although there have been calls from practitioners and the public, the draft Law on the Protection of Personal Data, first formulated in 2015, was submitted by the President to the House of Representatives in February 2020 but has not been passed yet. Previous research highlights Indonesia's slow progress in enacting legislation related to cyberspace, with some attributing it to budgetary constraints in the law-making process.

The expansion of the internet in Indonesia has coincided with the proliferation of disinformation, which has been a significant issue [30]. In response, Indonesian authorities have implemented measures to combat disinformation through awareness campaigns conducted by MCIT agencies and their partners. Notably, a program aimed at countering the spread of disinformation was established, involving collaborations between cyber-media companies, journalists [35], and civil society organizations in Indonesia. Their joint efforts focus on monitoring the internet for hoaxes and debunking them before they gain wide dissemination.

4.2. From Cyber-Media Operatives

The responses from the media operatives surveyed in this study, including both organizational entities and individual influencers, highlighted several significant concerns. Individual respondents expressed frustration with annoying unsolicited messages, calls, mail, and advertisements, which they attributed, in part, to the uncontrolled circulation of their contact information and personal data due to the absence of regulations on personal data use in Indonesia. These respondents strongly expressed their desire for Indonesian cyber law to regulate personal data and address these issues. On the other hand, cyber-media organizations raised concerns about cloning and spoofing of their platforms, as well as fraudulent activities such as cloned academic journals used to collect fees from unsuspecting victims. The respondents reported instances where platform spoofing was utilized by perpetrators seeking to disseminate disinformation or attract user traffic by impersonating platforms with high engagement. These challenges underscored the need for increased cybersecurity measures to protect the integrity of cyber-media organizations.

The study revealed that the media operatives surveyed did not have complete freedom to publish as they wished, as their content had to comply with the provisions of Indonesian law. Certain issues and topics perceived as potentially problematic by the authorities were often not published in the desired manner due to concerns about community backlash, censorship, and potential legal consequences. However, some respondents supported certain censorship measures, arguing they were necessary to uphold the country's moral values. Three influencers disclosed that they operated direct messaging groups with encrypted content, allowing them to engage in discussions deemed sensitive and subject to censorship on open media and social media platforms. By sharing such information within these closed groups, they aimed to keep society informed despite the restrictions imposed on public discourse.

One blogger emphasized that cyber law significantly impacted the information society received due to censorship. They noted that censored information often found alternative channels through actors who chose not to abide by the law or through "non-established" actors, leading to concerns about the quality of information available to the public. The blogger further highlighted that many internet users resorted to tools like virtual private networks (VPNs) to bypass censorship and avoid detection or sanctions by the authorities. In addressing the issue of misinformation and disinformation, media houses stressed the importance of fact-checking their information before publication and taking prompt corrective action in case of any errors to mitigate potential social and legal consequences. Additionally, one social media influencer revealed her involvement as a volunteer in an initiative dedicated to countering disinformation by sharing debunked hoaxes and cautioning her followers about the circulation of false information.

These findings underscore the challenges cyber-media operatives face in navigating data privacy, censorship, misinformation, and disinformation in the context of Indonesian cyber law.

5. Discussion

The findings of this study reveal the influence of culture on societal perceptions of cyber law. Supportive attitudes toward internet censorship are influenced by cultural preferences for reducing exposure to ambiguity and uncertainty [45]. In the Indonesian context, the importance of social harmony has led to the perception that the government should protect societal peace by regulating certain content [45, 46]. The enforcement of cyber-law through internet surveillance and monitoring, as well as the response to reported complaints, has resulted in known internet users, such as media houses and influential individuals, refraining from engaging with sensitive content due to fear of sanctions [47, 48]. This illustrates how the law influences people's behavior, even when their personal preferences differ.

The impact of cyber-law on cyber-media is evident in the findings, as encrypted direct messaging groups have emerged as alternative channels for information sharing and social discourse, allowing individuals to bypass censorship [49, 50]. This finding aligns with studies conducted in Iran and highlights the societal response to internet censorship.

The concerns expressed by respondents regarding the possibility of facing sanctions or prosecution for cyber activities reflect elements of authoritarianism and suppression of free speech in Indonesia [30]. Examples of blasphemy cases and the use of cyber law to target political opponents demonstrate the potential for the exploitation of legislation to stifle dissenting voices [47, 48, 51]. The absence of a user data protection policy in Indonesia has led to cautious internet usage and reveals the slow progress in enacting relevant legislation [30]. Existing laws related to personal data create confusion and overlap, making implementation challenging [52]. The rampant manipulation of personal data by criminal elements and corrupt officials further highlights the need for stronger data protection measures [30]. In light of the insights from this study and previous research, it is clear that cyber-laws in Indonesia have broader implications beyond guiding online activities, significantly impacting the relationship between society and the media, both in cyberspace and in real life. The distorted use of cyber-laws and technologies to promote divisive sentiments raises concerns about rising authoritarianism, socio-religious intolerance, and political opportunism [30].

6. Questionable Issues in Indonesia's Cyber Law

The flagship cyber-law in Indonesia is ITE Law No.11/2008, which underwent revisions in 2016. While some positive changes were made, such as the inclusion of provisions for data breach notification and the right to be forgotten, additional amendments granted officials the power to directly block electronic information they deemed prohibited, posing threats to free expression [30, 52, 53]. The amendments strengthened the legal basis for banning online content and increased administrative authority under the ITE Law. Article 40 of the revised law grants officials the authority to ban internet material and directs ISPs to do so directly [30, 54]. Censorship in Indonesia initially targeted pornographic material but has expanded to include blocking blogs, platforms, and social media accounts that express socio-political critical discourse, raising concerns about the suppression of socio-political expression [30].

The BSSN, responsible for controlling Indonesia's internet and content moderating, has shown concern about disinformation and implemented policies regulating cyberspace. However, the stricter regulation and control raise concerns about the potential curtailment of online liberties [54, 55]. Using technologies like the Cyber Drone 9 to automate censorship further tightens the suppression of online freedoms [45, 55]. Questionable issues arise regarding the cyber-law reform of the Criminal Code, particularly Article 309, which criminalizes disinformation resulting in a disturbance without clearly defining what constitutes a disturbance [56]. This ambiguity poses a risk to freedom of speech, as it can potentially be used to prosecute journalists, bloggers, and social media activists [30, 31, 57].

These developments raise concerns about strict censorship, the potential misuse of power, and the suppression of socio-political expression. Combining these factors seriously risks Indonesia's online social freedom. Implementing drastic amendments, using automated censorship technology, and the readiness to censor online social expression irrationally cast doubt on recent progressions in Indonesia's cyber-law. These developments highlight the need for safeguards and comprehensive measures to address cyberspace-enabled problems. The risk to Indonesia's cyber-media and online social freedoms requires careful consideration and a strengthened cyber-legal framework [58, 59].

7. Conclusion

Implementing cyber laws in Indonesia has substantial sociological implications for the media and society. Questionable aspects of existing cyber laws are highlighted, as they pose challenges to upholding the rule of law and safeguarding social and media freedoms. The study uncovers concerns regarding internet censorship, the lack of comprehensive data protection legislation, and the potential for the misuse of cyber laws to suppress free speech and stifle dissenting voices. The study underscores the need for a balanced approach, considering legal regulations while preserving societal freedoms. It emphasizes the importance of addressing pertinent issues in cyber law to maintain a democratic and inclusive digital landscape. The insights derived from this study hold relevance for Indonesia and other developing countries grappling with similar challenges. To enhance media freedoms and societal well-being in the digital age, policymakers and stakeholders must prioritize the development of comprehensive and inclusive cyber laws. These laws should protect individuals' privacy, uphold freedom of expression, and promote responsible media practices. Additionally, there is a need for increased transparency, accountability, and public participation in formulating and implementing cyber laws to ensure that they align with societal needs and values. By addressing the questionable aspects of cyber laws and fostering a favorable environment for media and social media freedoms, Indonesia and other developing countries can navigate the evolving digital landscape while preserving democratic principles and societal cohesion. Overall, this study contributes to a deeper understanding of the sociological dimensions of cyber laws and their impact on media freedoms. It provides valuable insights for researchers, policymakers, and stakeholders in shaping cyber laws and navigating the digital era's complex relationship between law, media, and society.

8. Declarations

8.1. Data Availability Statement

Data sharing is not applicable to this article.

8.2. Funding

The author received no financial support for the research, authorship, and/or publication of this article.

8.3. Institutional Review Board Statement

Not applicable.

8.4. Informed Consent Statement

Not applicable.

8.5. Declaration of Competing Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

9. References

[1] Morris, M., & Ogan, C. (2018). The Internet as Mass Medium. The Media, Journalism and Democracy, 1(4), 289–400. doi:10.4324/9781315189772-25.

[2] Larsson, A. O. (2018). The News User on Social Media: A comparative study of interacting with media organizations on Facebook and Instagram. Journalism Studies, 19(15), 2225–2242. doi:10.1080/1461670X.2017.1332957.

[3] Khasawneh, A., Chalil Madathil, K., Dixon, E., Wisniewski, P., Zinzow, H., & Roth, R. (2019). An Investigation on the Portrayal of Blue Whale Challenge on YouTube and Twitter. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 887–888. doi:10.1177/1071181319631179.

[4] Nurmandi, A., Almarez, D., Roengtam, S., Salahudin, Jovita, H. D., Kusuma Dewi, D. S., & Efendi, D. (2018). To what extent is social media used in city government policy making? Case studies in three ASEAN cities. Public Policy and Administration, 17(4), 600–618. doi:10.13165/VPA-18-17-4-08.

[5] Nica, E., Popescu, G. H., Nicolăescu, E., & Constantin, V. D. (2014). The effectiveness of social media implementation at local government levels. Transylvanian Review of Administrative Sciences, 2014, 152–166.

[6] Sharif, M. H. M., Troshani, I., & Davidson, R. (2017). Determinants of social media impact in local government. Media Influence: Breakthroughs in Research and Practice, 28(3), 141–164. doi:10.4018/978-1-5225-3929-2.ch008.

[7] Yar, M. (2012). Sociological and Criminological Theories in the Information Era. Cyber Safety: An Introduction, 45–56.

[8] Drake, P., & Clarke, S. (2008). Social aspects of information security: An international perspective. In Social and Human Elements of Information Security: Emerging Trends and Countermeasures. 98–115. doi:10.4018/978-1-60566-036-3.ch007.

[9] Griffiths, A., Banakar, R., & Travers, M. (2002). An Introduction to Law and Social Theory. Hart Publishing, Oxford, United Kingdom.

[10] Treviño, A. J. (2017). The Sociology of Law Classical and Contemporary Perspectives. The Sociology of Law Classical and Contemporary Perspectives. Routledge, New York, United Kingdom. doi:10.4324/9781315135069.

[11] Čehulić, M. (2021). Perspectives of Legal Culture: A Systematic Literature Review. Revija Za Sociologiju, 51(2), 257283. doi:10.5613/RZS.51.2.4.

[12] Travers, M. (2009). Understanding law and society. Understanding Law and Society. Routledge-Cavendish, London, United Kingdom. doi:10.4324/9780203871256.

[13] Nelken, D. (2009). Comparative criminal justice: Beyond ethnocentrism and relativism. European Journal of Criminology, 6(4), 291–311. doi:10.1177/1477370809104684.

[14] Scott, R. E., & Triantis, G. G. (2021). What do Lawyers Contribute to Law and Economics? Yale Journal on Regulation, 38(2), 707–731.

[15] Scuro Neto, P. (2019). Sociologia Geral e Jurídica - A Era do Direito Cativo. Saraiva Educação SA, São Paulo, Brazil.

[16] Black, D. (1979). Common Sense in the Sociology of Law. American Sociological Review, 44(1), 18. doi:10.2307/2094814.

[17] Embree, L., & Embree, L. Introduction: Alfred Schutz's Philosophical Project. The Schutzian Theory of the Cultural Sciences, 1–12.

[18] Rawls, A. W., & Turowetz, J. (2021). "Discovering culture" in interaction: solving problems in cultural sociology by recovering the interactional side of Parsons' conception of culture. American Journal of Cultural Sociology, 9(3), 293–320. doi:10.1057/s41290-019-00079-6.

[19] Hopkins, A. (1975). On the Sociology of Criminal Law. Social Problems, 22(5), 608–619. doi:10.2307/799694.

[20] Tomasic, R. (1972). The sociology of law. Current Sociology, 20(3), 13–48. doi:10.1177/001139217202000302.

[21] Hunt, A. (1975). Perspectives in the Sociology of Law. Sociological Review, 23(S1), 22–44. doi:10.1111/j.1467-954X.1975.tb00030.x.

[22] Dahlgren, P. (1996). Media Logic in Cyberspace: Repositioning Journalism and its Publics. JAVNOST, 3(3), 59–72. doi:10.1080/13183222.1996.11008632.

[23] Tumber, H. (2001). Democracy in the Information Age: the Role of the Fourth Estate in Cyberspace. Information, Communication & Society, 4(1), 95–112. doi:10.1080/13691180122542.

[24] Srivastava, A., Goswami, M. A. K., & Gautam, D. R. (2022). Cyber Crimes against Marginalised and Vulnerable Groups in India. Cyber Crime, Regulations and Security - Contemporary Issues and Challenges, 07–17. doi:10.55662/book.2022ccrs.019.

[25] Hirst, M. (2020). News 2.0: Can Journalism Survive the Internet? News 2.0: Can Journalism Survive the Internet?, 1–235. doi:10.4324/9781003116554.

[26] Hepp, A., & Loosen, W. (2021). Pioneer journalism: Conceptualizing the role of pioneer journalists and pioneer communities in the organizational re-figuration of journalism. Journalism, 22(3), 577–595. doi:10.1177/1464884919829277.

[27] Iosifidis, P. (2011). The public sphere, social networks and public service media. Information Communication and Society, 14(5), 619–637. doi:10.1080/1369118X.2010.514356.

[28] Susanto, E. H., Loisa, R., & Junaidi, A. (2020). Cyber media news coverage on diversity issues in Indonesia. Journal of Human Behavior in the Social Environment, 30(4), 510–524. doi:10.1080/10911359.2019.1708525.

[29] TEMPO.CO. (2023). Pedoman Pemberitaan Media Siber. Bicara Fakta: TEMPO.CO, Jakarta, Indonesia. Available online: https://nasional.tempo.co/read/381612/pedoman-pemberitaan-media-siber-diresmikan (accessed on July 2023).

[30] Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. Journal of Cyber Policy, 4(2), 216–234. doi:10.1080/23738871.2019.1627476.

[31] Masduki. (2022). Cyber-troops, digital attacks, and media freedom in Indonesia. Asian Journal of Communication, 32(3), 218–233. doi:10.1080/01292986.2022.2062609.

[32] Oliveira, G. H. M., & Welch, E. W. (2013). Social media use in local government: Linkage of technology, task, and organizational context. Government Information Quarterly, 30(4), 397–405. doi:10.1016/j.giq.2013.05.019.

[33] Mergel, I. (2013). A framework for interpreting social media interactions in the public sector. Government Information Quarterly, 30(4), 327–334. doi:10.1016/j.giq.2013.05.015.

[34] Yang, J. H., & Liu, S. (2017). Accounting narratives and impression management on social media. Accounting and Business Research, 47(6), 673–694. doi:10.1080/00014788.2017.1322936.

[35] Lim, M. (2017). Freedom to hate: social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia. Critical Asian Studies, 49(3), 411–427. doi:10.1080/14672715.2017.1341188.

[36] Malawani, A. D., Nurmandi, A., Purnomo, E. P., & Rahman, T. (2020). Social media in aid of post disaster management. Transforming Government: People, Process and Policy, 14(2), 237–260. doi:10.1108/TG-09-2019-0088.

[37] Reddick, C. G., & Norris, D. F. (2013). Social media adoption at the American grass roots: Web 2.0 or 1.5? Government Information Quarterly, 30(4), 498–507. doi:10.1016/j.giq.2013.05.011.

[38] Agostino, D., & Arnaboldi, M. (2016). A Measurement Framework for Assessing the Contribution of Social Media to Public Engagement: An empirical analysis on Facebook. Public Management Review, 18(9), 1289–1307. doi:10.1080/14719037.2015.1100320.

[39] Holcomb, J., Gottfried, J., Mitchell, A., & Schillinger, J. (2013). News Use across Social Media Platforms. Pew Research Center, Washington, D.C., United States.

[40] Saez-Trumper, D., Castillo, C., & Lalmas, M. (2013). Social media news communities: Gatekeeping, coverage, and statement bias. International Conference on Information and Knowledge Management, Proceedings, October 2013, 1679–1684. doi:10.1145/2505515.2505623.

[41] Liu, I. L. B., Cheung, C. M. K., & Lee, M. K. O. (2016). User satisfaction with microblogging: Information dissemination versus social networking. Journal of the Association for Information Science and Technology, 67(1), 56–70. doi:10.1002/asi.23371.

[42] Ye, Y., Xu, P., & Zhang, M. (2017). Social media, public discourse and civic engagement in modern China. Telematics and Informatics, 34(3), 705–714. doi:10.1016/j.tele.2016.05.021.

[43] Jurriëns, E., & Tapsell, R. (2017). Digital Indonesia: Connectivity and divergence. Digital Indonesia: Connectivity and Divergence, 304.

[44] Janes, J. (2001). Survey research design. Library Hi Tech, 19(4), 419–421. doi:10.1108/EUM0000000006543.

[45] Thompson, N., McGill, T., & Khristianto, D. V. (2021). Public Acceptance of Internet Censorship in Indonesia. ACIS 2021 - Australasian Conference on Information Systems, Proceedings, 1–9.

[46] Hyland, J. (2020). Internet Censorship: An Integrative Review of Technologies Employed to Limit Access to the Internet, Monitor User Actions, and their Effects on Culture. Senior Honors Theses. Liberty University, Virginia, United States.

[47] Gibbons, A., & Carson, A. (2022). What is misinformation and disinformation? Understanding multi-stakeholders' perspectives in the Asia Pacific. Australian Journal of Political Science, 57(3), 231–247. doi:10.1080/10361146.2022.2122776.

[48] Mahy, P., Winarnita, M., & Herriman, N. (2022). Influencing the influencers: Regulating the morality of online conduct in Indonesia. Policy and Internet, 14(3), 574–596. doi:10.1002/poi3.321.

[49] Kargar, S., & McManamen, K. (2018). Censorship and Collateral Damage: Analyzing the Telegram Ban in Iran. SSRN Electronic Journal, Research Publication No. 2018-4. doi:10.2139/ssrn.3244046.

[50] Gebhart, G., & Kohno, T. (2017). Internet Censorship in Thailand: User Practices and Potential Threats. Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, 417–432. doi:10.1109/EuroSP.2017.50.

[51] Radue, M. (2019). Harmful disinformation in Southeast Asia: “Negative campaigning”, “information operations” and “racist propaganda” - three forms of manipulative political communication in Malaysia, Myanmar, and Thailand. Journal of Contemporary Eastern Asia, 18(2), 68–89. doi:10.17477/jcea.2019.18.2.068.

[52] Anak Agung Ayu Nanda Saraswati. (2019). The Need to Protect Freedom of Expression on the Internet Through a Human Rights-Based in Indonesia. ASEAN Journal of Legal Studies, 2(1), 55–69.

[53] Aditya, Z. F., & Al-Fatih, S. (2021). Indonesian constitutional rights: expressing and purposing opinions on the internet. International Journal of Human Rights, 25(9), 1395–1419. doi:10.1080/13642987.2020.1826450.

[54] Safiranita, T., Waluyo, T. T. P., Calista, E., Ratu, D. P., & Ramli, A. M. (2021). The Indonesian Electronic Information and Transactions within Indonesia’s Broader Legal Regime: Urgency for Amendment? Journal HAM, 12(3), 533. doi:10.30641/ham.2021.12.533-552.

[55] Carson, A., & Fallon, L. (2021). Fighting Fake News: A Study of Online Misinformation Regulation in the Asia Pacific. La Trobe University, Melbourne, Australia IV, 116.

[56] Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. Law Research Review Quarterly, 7(1), 69–82.

[57] Setiyawan, A. (2019). National Cybersecurity Policy in the U.S and Indonesia. UNTAG Law Review, 3(1), 71. doi:10.36356/ulrev.v3i1.1071.

[58] Allen, N. W. (2014). From patronage machine to partisan melee: Subnational corruption and the evolution of the Indonesian party system. Pacific Affairs, 87(2), 221–245. doi:10.5509/2014872221.

[59] Purdey, J. (2016). Political families in Southeast Asia. South East Asia Research, 24(3), 319–327. doi:10.1177/0967828X16659027.