MIDA

Majalah Ilmiah Dinamika Administrasi

P-ISSN 1411-4461
E-ISSN 2830-7267

Volume 21 | Nomor 1 | April 2024

GENDER POLICY AND MAINSTREAMING: CONFRONTING INFORMATION AND ELECTRONIC TRANSACTION LAW WITH WOMEN'S CYBER SECURITY

[1] Lian Agustina Setiyaningsih
[1]Department of Communication Science, Universitas Merdeka Malang
[1]lian.agustina@unmer.ac.id

ABSTRACT (12pt Bold)

The research objective is to describe the correlation between policies and gender mainstreaming in the context of information protection and electronic transactions. Cyber security, especially for women, has become an urgent issue in the current digital era, where social media and online platforms increasingly dominate interactions. The literature review method analyses the discourse structure in several articles and literature from reputable national and international journals. Several articles from Google Scholar are categorized according to the type of case in research. This article juxtaposes several articles on electronic information and transactions law (ITE law) with women's specific cyber safety needs. Among other things, articles relating to gender mainstreaming are in articles 27, 3, 28, paragraph 1, 32, paragraphs 1,2,3, and articles 45, paragraph 1. Through this approach, inclusive and gender-oriented public policies can provide a strong foundation for strengthening security—female cyber. By highlighting existing challenges and opportunities, this article proposes concrete strategies for integrating gender aspects in cyber policy, especially in the domain of cyber security for women.

Keywords; Policy; Gender Mainstreaming; Women; Cyber Security.

A. INTRODUCTION

Gender policies and mainstreaming intersect in various sectors of life and intersect with various fields (Caglar, 2013; Walby, 2005a, 2005b), especially today with digitalization (Ariansyah et al., 2023; Radulović & Hervías-Parejo, 2022) and protection of information in electronic transactions (Cain & Imre, 2022; Mashatan et al., 2022). At the same time, cyber security is considered a primary need for an information society amidst a flood of information in the media. The foundation of digital interaction is maintaining integrity (Wang et al., 2020) and data confidentiality (Chen

P-ISSN 1411-4461
E-ISSN 2830-7267

et al., 2020). Amid advances in information and communication technology, the role of gender in cyber security is becoming increasingly important. Women, often vulnerable subjects in the online world, require special protection and attention in this context.

The Information and Electronic Transactions Law (UU ITE) directly relates to various issues of gender mainstreaming and freedom of information. This article explores the correlation between policy and gender mainstreaming in dealing with the ITE Law by focusing on aspects of cyber security for women, which are often ignored in policy discussions. Several articles in this law are often considered an important legal basis for regulating various aspects of electronic activities in Indonesia, especially those related to user safety (Perdana, 2020).

In its implementation, there are challenges and debates related to gender equality and cyber security. Various provisions in the ITE Law, such as regarding misuse of social media (Stephenson et al., 2018) and online content (Wardani & Indrayani, 2018), can have a significant impact on women, both in terms of privacy and security (Setiyaningsih et al., 2021). It should be noted that women are often the targets of online crimes, such as online sexual harassment, fraud and other cyber harassment. This emphasizes the importance of developing policies that integrate gender aspects and consider women's special needs in cyber security.

Mainstreaming gender in cyber policy can ensure that women's perspectives, needs and experiences are accommodated effectively in cyber protection efforts (Vida, 2021). However, efforts to present inclusive and gender-oriented policies in cyber security take work. Challenges faced include limited understanding of how gender influences risks and vulnerabilities in the cyber domain, a lack of detailed data on the impact of cybercrime on women, and unequal access to and use of information technology between men and women.

Analysis was carried out on policy products from several articles of the ITE Law and cyber security approaches focusing on women and gender mainstreaming efforts. By considering the social, cultural and political context surrounding policy development, laws are used to ensure better protection of women in the digital space. Article 27(1) relates to the distribution of electronic data that violates morality. Another article involved in this research relates to the dissemination of information that causes insults and defamation (article 27, paragraph 3). Meanwhile, in article 28 (1), the

P-ISSN 1411-4461
E-ISSN 2830-7267

spread of false news that is misleading results in losses in electronic transactions. Then also those related to personal data protection (article 32, paragraphs 1, 2,3). Furthermore, the article that has much to do with the exchange of information is 45 A (1) concerning hoaxes and false information (Information and Electronic Transactions, 2016).

Distribution of electronic data that violates decency and gender issues is a daily problem faced by women in the digital era (Maris et al., 2020; Клоков & Тихонов, 2023). Concrete forms can be exemplified by the spread of pornographic content, virtual rape in online games, and online sexual harassment via social media platforms. This phenomenon not only violates the norms of decency that exist in society but also often creates an unsafe environment for individuals, especially women and children. To respond to this challenge, firm and inclusive policies are needed. This includes strong regulations to enforce the law against perpetrators of violations, cooperation between government, industry and civil society to monitor and report violating content, and public education efforts on digital ethics and gender awareness.

Hoaxes, personal data protection, and electronic transaction losses are interrelated issues in cyber security, with gender aspects playing an important role (Rumlus & Hartadi, 2020; Siahaan, 2022). Hoaxes spread via social media often create vulnerability to identity theft and online fraud, which can disproportionately impact women. Protecting personal data is becoming increasingly important in preventing the exploitation of women, who are often the main targets of cybercriminals. Additionally, electronic transaction losses, such as credit card fraud or illegal money transfers, can harm women economically and even exacerbate gender gaps. Therefore, policies that integrate gender aspects to prevent and enforce laws against hoaxes protect personal data and electronic transactions are crucial for creating a safer and more inclusive digital environment for all individuals.

Meanwhile, cases of disseminating information that causes insults and defamation in the context of gender issues are a serious form of cybercrime. This can include spreading false rumours, manipulative photos or videos that insult or slander someone based on their gender or sexual orientation. The impact can be very damaging, both emotionally and socially, especially for the individual who is the victim. Efforts involving strict supervision of harmful online content, effective law enforcement against cyber

P-ISSN 1411-4461
E-ISSN 2830-7267

criminals, and public education campaigns are the answer (Castaño-Pulgarín et al., 2021). In addition, it is important to strengthen gender awareness among internet users to better understand and respect individual rights and treat everyone with respect and empathy, regardless of sex, gender or sexual orientation.

B. METHOD

This type of descriptive research is done by reviewing several articles related to the specified topic. In determining topics, issues are categorized based on the content of the articles in the ITE Law that intersect with gender mainstreaming issues. The categories include information containing insults, hoaxes, verbal and non-verbal violence, and personal data protection. Research sources were selected based on issues and categories involving several articles found on Google Scholar. Data collection techniques were carried out by selecting journals based on categories and collecting articles (Lewis, 2006). The analysis method is carried out by grouping issues based on categories, filtering articles by year, topic and country (Cairney et al., 2022), and conducting structured and narrative analysis of selected articles; the final step is to conclude the synthesized analysis results (Pandey et al., 2023).

C. RESULT AND DISCUSSION

Women's Cyber Security Challenges in Framing Electronic Information and Transaction Law Policies

In an increasingly complex digital era, cyber security for women is becoming increasingly important in the policy-framing process related to the ITE Law. Women often face unique risks and threats in the online environment, which require special attention in cyber policy development. In this context, several main challenges need to be addressed to ensure adequate protection for women within the framework of the ITE Law.

Firstly, one of the main challenges is the inequality of information technology access and skills between men and women. Women often have lower access to information technology and cyber security training than men. This can increase women's vulnerability to cyberattacks and make it more difficult for them to take

P-ISSN 1411-4461
E-ISSN 2830-7267

effective action to protect themselves online. Therefore, in the ITE Law policy framing process (Ramadhani, 2023), it is important to consider these challenges and include measures to increase women's access to cybersecurity training and information technology resources.

Secondly, gender stereotypes and patriarchal cultural norms also pose serious challenges in protecting women in the online environment. Women are often targets of sexual harassment, blackmail and gender-based discrimination online. It can create an unsafe and unfriendly online environment for women, hindering their participation in digital spaces. Therefore, in the ITE Law policy framing process (Suci et al., 2023), it is important to integrate gender perspectives and recognize the impact of gender differentiation in online experiences. Policies must be designed to protect women under Article 27 from gender violence and online discrimination, as well as promote an online environment that is inclusive and safe for all individuals, regardless of gender (Novitasari et al., 2023).

Another challenge is the need for more awareness and education about cyber security among women. Many women may need to be more educated about cyber risks and precautions, making them more vulnerable to cyber-attacks. Therefore, in the policy framing of the ITE Law, it is important to include initiatives to increase awareness and education about cyber security among women. It can be done through education, training and outreach campaigns aimed specifically at women so that they can recognize and address cyber threats more effectively.

In facing the challenges of Women's Cyber Security (O'Connell, 2012; von Solms & van Niekerk, 2013) in the policy framing of the ITE Law, it is important to adopt a holistic and inclusive approach. Policies must consider women's specific experiences and needs in online environments and recognize the important role women play in advancing overall cyber security. Only by taking gender aspects into account in the policy-framing process can we ensure that the ITE Law provides adequate protection for all individuals, regardless of gender.

Another connection is with various policy products where several articles of the ITE Law (2016) and cyber security approaches focus on women and efforts to pay attention to gender equality (O'Connell, 2012; Sun et al., 2018). Considering the social, cultural and political context that influences policy formation, this law ensures more

P-ISSN 1411-4461
E-ISSN 2830-7267

effective protection of women in the digital realm. Article 27(1) relates to the distribution of electronic data that violates moral norms. Another article analyzed in this research is related to disseminating derogatory and defamatory information (article 27, paragraph 3).

Meanwhile, article 28 (1) discusses the spread of fake news, which can mislead and result in losses in electronic transactions. In addition, article 32, paragraphs 1, 2 and 3 deal with protecting personal data. Another significant article is 45 A (1), which regulates the spread of false information and hoaxes. Through analysis of these articles, steps can be taken to strengthen cyber security policies and practices that are more inclusive and responsive to the needs and safety of women in the digital world.

Gender Sensitive Cyber Policy in strengthening Women's Protection

Gender-sensitive cyber policy is a policy approach that considers gender differences and their impact on women's protection in the digital space (Indah et al., 2023). In this context, the adopted policy integrates a gender perspective in every stage of planning, implementation and evaluation to ensure that women's needs, experiences and safety are accommodated effectively (Dewi, 2021). This approach aims to address gender inequalities in access, control, and security in the online world and reduce the risks and vulnerabilities experienced by women about cyber threats.

The first, gender-sensitive cyber policies consider gender differentiation in online experiences and needs (Birchall, 2018). It includes recognizing that women often face unique risks and threats in the digital environment, such as sexual harassment, blackmail, and gender-based discrimination. Therefore, the policy is designed to identify and address these issues, providing greater protection for women in vulnerable situations.

The second, the policy considers information technology access and skills inequality between men and women (Teixeira, 2023; Utami, 2019). Women often need more access to information technology and cyber security training, which can increase their vulnerability to cyberattacks. Therefore, gender-sensitive cyber policies propose measures to increase women's access to information technology training and

P-ISSN 1411-4461
E-ISSN 2830-7267

resources and ensure that online infrastructure and services consider women's needs and capabilities.

The third, the policy also considers the important role of women in promoting cyber security (Anwar et al., 2017; Bagchi-Sen et al., 2010). Women often have a significant role in protecting families, communities and organizations from cyber threats. Therefore, gender-sensitive cyber policies encourage women's active participation in efforts to prevent, detect and deal with cyber crimes. It can be done through education, training and support for women to become leaders in cyber security.

Furthermore, the policy considers gender stereotypes and patriarchal cultural norms that can influence women's perceptions and experiences in the digital space. Gender-sensitive cyber policies emphasize the importance of addressing online gender discrimination and creating an online environment that is inclusive and safe for all individuals, regardless of gender. This can be done through gender awareness campaigns, training on gender justice, and support for women who are victims of cybercrime (Wardhani & Maulina, 2022).

Adopting gender-sensitive cyber policies requires involving all stakeholders, including government, non-governmental organizations, the private sector and civil society. Only with strong cross-sector collaboration can we build a safer, more inclusive and equitable online environment for all individuals, regardless of gender. Thus, this policy is important in strengthening women's protection and realizing the vision of an internet free from violence and discrimination.

Examples of relevant policies include laws on cybercrime, social media platform regulations prohibiting harmful content, and training programs to increase gender awareness among online users. Countries such as Australia, Canada, and Europe have a similar approach to approaches to the problem. Through cross-sector efforts and strong collaboration between government, industry and civil society, it is hoped that the distribution of electronic data that violates decency and gender can be significantly reduced, creating a safer and more inclusive online environment for all individuals.

P-ISSN 1411-4461
E-ISSN 2830-7267

D. CONCLUSION

Gender policies and mainstreaming confronting the Information and Electronic Transactions Law with Women's Cyber Security demonstrate efforts to ensure gender protection, participation and equality in information and communication technology. Forms of policy implementation to support gender mainstreaming include cyber security for women, increasing participation in spreading and countering hoaxes, equality of access and opportunities in obtaining and distributing information, gender partnerships and collaboration, and integrating regulations supported by culture. In various articles related to distribution, consumption and production, information needs to be matched with gender mainstreaming values to be balanced. Public policies that consider all groups and focus on gender equality can be a solid basis for improving cyber security for women. By identifying the challenges faced and the opportunities available, this article proposes specific steps to incorporate gender dimensions in cyber policy, especially regarding cyber security for women.

REFERENCES

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Ariansyah, K., Setiawan, A. B., Darmanto, D., Nupikso, D., Budhirianto, S., Hidayat, D., & Hikmaturokhman, A. (2023). Digital inclusion for all? A gender-disaggregated analysis of e-government service use in Indonesia. *Transforming Government: People, Process and Policy*, *17*(4), 655–672. https://doi.org/10.1108/TG-04-2023-0043

Bagchi-Sen, S., Rao, H. R. , &, Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional*, *12*(1), 24–31.

Birchall, J. (2018). Gender sensitive strategic communications interventions. . In https://opendocs. ids. ac. uk/opendocs/handle/20.500 (Ed.), *K4D Helpdesk Report. Brighton, UK: Institute of Development Studies.* (pp. 12413-14265.).

Caglar, G. (2013). Gender Mainstreaming. *Politics & Gender*, *9*(03), 336–344. https://doi.org/10.1017/S1743923X13000214

Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, *24*(12), 2705–2724. https://doi.org/10.1177/14614448211000327

P-ISSN 1411-4461
E-ISSN 2830-7267

Cairney, P., St Denny, E., Kippin, S., & Mitchell, H. (2022). Lessons from policy theories for the pursuit of equity in health, education and gender policy. *Policy & Politics*, *50*(3), 362–383. https://doi.org/10.1332/030557321X16487239616498

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech. Systematic review. *Aggression and Violent Behavior*, *58*, 101608. https://doi.org/10.1016/j.avb.2021.101608

Chen, Y., Luo, F., Li, T., Xiang, T., Liu, Z., & Li, J. (2020). A training-integrity privacy-preserving federated learning scheme with trusted execution environment. *Information Sciences*, *522*, 69–79. https://doi.org/10.1016/j.ins.2020.02.037

Dewi, O. (2021). Implementasi Gender Mainstraiming dalam Konteks Pembangunan: Studi Kasus Keberhasilan Kesetaraan Gender di Filipina tahun 2018. . *Jurnal Ilmiah Hubungan Internasional* , *17*(2), 200–218.

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). . *Jurnal Bidang Penelitian Informatika*, *1*(1), 57-64.

Informasi Dan Transaksi Elektronik, Republik Indonesia (2016).

Lewis, J. (2006). Employment and care: The policy problem, gender equality and the issue of choice. *Journal of Comparative Policy Analysis: Research and Practice*, *8*(2), 103–114. https://doi.org/10.1080/13876980600682014

Maris, E., Libert, T., & Henrichsen, J. R. (2020). Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites. *New Media & Society*, *22*(11), 2018–2038. https://doi.org/10.1177/1461444820924632

Mashatan, A., Sangari, M. S., & Dehghani, M. (2022). How Perceptions of Information Privacy and Security Impact Consumer Trust in Crypto-Payment: An Empirical Study. *IEEE Access*, *10*, 69441–69454. https://doi.org/10.1109/ACCESS.2022.3186786

Novitasari, D., Bihaqqis, R. A., & Hastarini, A. (2023). Tinjauan Hukum Terhadap Pasal 27 Ayat 3 UU ITE Dalam Hak Kebebasan Berpendapat Masyarakat. LENTERA PANCASILA: . *Jurnal Riset Hukum & Pancasila*, *2*(2).

O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209. https://doi.org/10.1093/jcsl/krs017

Pandey, S. K., Smith, A. E., Pandey, S., & Ojelabi, O. A. (2023). Reimagining race and gender in public administration and public policy: Insights from an interdisciplinary systematic review. *Public Administration Review*, *83*(1), 14–34. https://doi.org/10.1111/puar.13570

P-ISSN 1411-4461
E-ISSN 2830-7267

Perdana, A. P. (2020). UU ITE, Media Sosial, Generasi M UU ITE TENTANG EFEK MEDIA SOSIAL TERHADAP GENERASI MILENIAL. *Inovasi Pembangunan : Jurnal Kelitbangan*, *8*(03), 297. https://doi.org/10.35450/jip.v8i03.214

Radulović, B., & Hervías-Parejo, V. (2022). *Mainstreaming Gender into Public Policies: A Tale of Two Countries* (pp. 43–67). https://doi.org/10.1007/978-3-031-14706-7_3

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan Siber. Kultura: . *Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(1), 89–97.

Rumlus, M. H. , & Hartadi, H. (2020). Policy the Discontinuation of Personal Data Storage in Electronic Media. *Jurnal HAM*, *11*(2), 285–301.

Setiyaningsih, L. A., Fahmi, M. H., & Molyo, P. D. (2021). Selective Exposure Media Sosial Pada Ibu dan Perilaku Anti Sosial Anak. *Jurnal Komunikasi Nusantara*, *3*(1), 1–11. https://doi.org/10.33366/jkn.v3i1.65

Siahaan, A. L. S. (2022). Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi. . *Majalah Hukum Nasional*, *52*(2), 209–223.

Stephenson, V. L., Wickham, B. M., & Capezza, N. M. (2018). Psychological Abuse in the Context of Social Media. *Violence and Gender*, *5*(3), 129–134. https://doi.org/10.1089/vio.2017.0061

Suci, I. M., Avicenna, A. H., Setiawan, S. M., Puteri, R. W., & Sirait, P. H. D. (2023). PERLINDUNGAN HAK KEKAYAAN INTELEKTUAL DI ERA DIGITAL MELALUI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE). . *Causa: Jurnal Hukum Dan Kewarganegaraan*, 1–10.

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Teixeira, T. C. (2023). Gendering Cyberwarfare: Towards a Feminist Approach to the Development of International Humanitarian Law Applicable to Cyber Operations. . *CEBRI-Revista: Brazilian Journal of International Affairs*, *7*, 58–80.

Utami, S. (2019). Eksistensi perkembangan perekonomian perempuan di era digitalisasi. . *AN-NISA: Jurnal Studi Gender Dan Anak, 12*(1), 596-609.

Vida, B. (2021). Policy framing and resistance: Gender mainstreaming in Horizon 2020. *European Journal of Women's Studies*, *28*(1), 26–41. https://doi.org/10.1177/1350506820935495

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

P-ISSN 1411-4461
E-ISSN 2830-7267

Walby, S. (2005a). Gender Mainstreaming: Productive Tensions in Theory and Practice. *Social Politics: International Studies in Gender, State & Society*, *12*(3), 321–343. https://doi.org/10.1093/sp/jxi018

Walby, S. (2005b). Introduction: Comparative gender mainstreaming in a global era. *International Feminist Journal of Politics*, *7*(4), 453–470. https://doi.org/10.1080/14616740500284383

Wang, T., Bhuiyan, M. Z. A., Wang, G., Qi, L., Wu, J., & Hayajneh, T. (2020). Preserving Balance Between Privacy and Data Integrity in Edge-Assisted Internet of Things. *IEEE Internet of Things Journal*, *7*(4), 2679–2689. https://doi.org/10.1109/JIOT.2019.2951687

Wardani, A. D., & Indrayani, H. (2018). Netralitas Konten Berita Online. . *Interaksi: Jurnal Ilmu Komunikasi*, *7*(1), 1–7.

Wardhani, D. A., & Maulina, P. (2022). Peran Pembentukan Komite Sosial Kesetaraan Gender Perempuan dalam Isu Stereotip. . *Jurnal Indonesia Sosial Teknologi*, *7*(3), 785-798.

Клоков, С. Н., & Тихонов, П. А. (2023). Producing and/or Distributing Intimate Images of a Person without its Consent. *Legal Issues in the Digital Age*, *4*(4), 92–113. https://doi.org/10.17323/2713-2749.2023.4.92.113