Blocking Dangerous Content in Electronic Communications Networks: Evidence from Netherlands, United States and Singapore

I Gede Adhi Mulyawarman [a,*], Putu Gede Arya Sumerta Yasa [a], Lamberton Cait [b]

[a] Faculty of Law, Universitas Udayana, Denpasar, Bali, Indonesia
[b] University of Pennsylvania, Philadelphia, United States.

*Corresponding Author: adhimulyawarman95e@gmail.com

ARTICLE INFO

Article history
Received: October 05, 2023
Revised: December 27, 2023
Accepted: February 15, 2024

Keywords
Blocking;
Dangerous Content;
Electronic Communication;
Regulation;

ABSTRACT

In recent years, the blocking of internet sites with harmful content or those deemed to be (illegal content) has increased. The policy of blocking dangerous sites has pros and cons regarding freedom of expression. Blocking is considered to be carried out to control citizens' expression, which can impact all areas, especially freedom of opinion, which can be seen as a threat to certain parties. This research aims to compare criminalization policies for blocking dangerous content in electronic communications networks in the Netherlands, the United States, and Singapore and provide thoughts on law enforcement models for blocking dangerous content in more democratic electronic communication networks. This is normative legal research using a law and case approach and comparing several countries. The conceptual approach is directed at the concept of a democratic state and the protection of human rights to formulate relevant policy models. The results of blocking studies in the Netherlands, The USA, and Singapore already have regulations and policy directions for blocking dangerous content, or at least rules regarding law enforcement for cybercrime. The difference is in the level of sensitivity to the specifications of existing problems. The policy model for blocking dangerous content with special regulations outside the Criminal Code must be carried out in a non-repressive manner so that it does not violate the *ultimum remedium* principle and becomes over-criminalized. The formulation of policy model of all crime prevention plans using the criminal law system, which pays attention to the problem of formulating criminal acts (criminalization), criminal responsibility, and criminal regulations and punishment.

1. Introduction

Advances in global technology and information have implications for the use of the internet for e-commerce, e-business, and e-banking activities, as well as providing cyber freedom (cyberliberty) both for commerce (commercial cyberliberty) and social (civil cyberliberty). Humans can easily, freely,

sophisticated, and quickly carry out transactions without having to face-to-face.[1] However, cyber freedom that is not properly regulated can be misused to carry out cyber threats, cyber terrorism, cyberstalking, and various other new forms of cybercrime.[2] Not only that, unlimited cyber activity can make it easier for someone to commit crimes that damage morals, such as gambling, prostitution, or pornography. This means that cyber freedom also opens up opportunities to commit various unlawful acts, including criminal acts. These multiple forms of crime have become known as "cybercrime."[3]

Due to the rise of cybercrime, the government is blocking dangerous content. This aims to block access to certain site pages by blocking Internet Protocol (IP) addresses. The mechanisms used in securing vary greatly, depending on the goals and resources available for the action. Unfortunately, sometimes IP blocking results in blocking thousands of unrelated sites that do not contain harmful content simply because they share the same IP. What's worse is that the government may also close sites not in line with its policies. Efforts to control the country's political direction can also be carried out through blocking under the pretext of dangerous content. It is important to remember that the internet is a global forum largely governed by private actors driven by profit interests, often ignoring the human rights of historically marginalized communities.[4]

In the last few years, blocking internet sites with harmful content or those deemed unlawful (illegal content) has increased. In Indonesia, based on data from the Ministry of Communication and Information, in 2016 773,097 negatively charged sites were blocked, most of which contained pornographic material, more significant than in 2015, when 766,394 sites were blocked. Meanwhile, in the first half of 2017, 6,000 blocked internet sites or social media accounts were suspected of spreading hate speech, slander, and hoaxes (fake news) alone. Entering the year of the COVID-19 pandemic, the Government handled 565,449 pieces of content that violated legal regulations on various social media sites. In 2022, 238,226 harmful content was addressed. Meanwhile, in statistical data on managing harmful internet content on sites in 2023, 437,741 blockings were recorded.

---

[1] Charlette Donalds and Kweku-Muata Osei-Bryson, 'Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach', *Computers in Human Behavior*, 92 (2019), 403–18 https://doi.org/10.1016/j.chb.2018.11.039

[2] Emre Kocyigit and others, 'Real-Time Content-Based Cyber Threat Detection with Machine Learning', 2021, pp. 1394–1403 https://doi.org/10.1007/978-3-030-71187-0_129

[3] Sarah Gordon and Richard Ford, 'On the Definition and Classification of Cybercrime', *Journal in Computer Virology*, 2.1 (2006), 13–20 https://doi.org/10.1007/s11416-006-0015-z

[4] Eva Nave and Lottie Lane, 'Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service?', *Computer Law & Security Review*, 51 (2023), 105884 https://doi.org/10.1016/j.clsr.2023.105884

In Indonesia, at least three laws and regulations currently regulate internet content: Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions. This regulation gives the Government the authority to cut off access to content. Law no. 44 of 2008 concerning Pornography provides the Government (including regional governments) the authority to block pornographic content on the internet. Law no. 28 of 2014 concerning copyright gives the Government the authority to stop pages that are vioviolatinght.

Regulated in Article 40 paragraph (2) of Law No. 11 of 2008 concerning Electronic Information and Transactions (Law No. 11 of 2008) , the Government protects the public interest from all types of disturbances resulting from misuse of electronic information and electronic transactions that disrupt public order, per the provisions of statutory regulations. In carrying out prevention, the Government has the authority to terminate access and/or order electronic system operators to terminate access to electronic information and/or documents containing unlawful content. The phrase breaking the law must fulfill the elements of the offense and be based on a final decision, and then blocking action can be taken.

However, the policy of blocking dangerous sites has pros and cons, one of which is related to freedom of expression. Not only controlling content that contains cyber threats,[5] cyber terorism,[6] cyber talking,[7] pornography, online gambling, etc., but also includes issues of control over political expression and government criticism. There are also efforts to prevent influence from outside the country on political practices within a country. As long as the content cannot be proven to contain elements of cybercrime, blocking content fights democracy. Regulations regarding freedom of expression and opinion have been regulated in Law No. 9 of 1998 concerning Freedom to Express Opinions in Public. Freedom to express views is interpreted as the right of every citizen to express thoughts orally, in writing, and so on freely and responsibly by the provisions of applicable laws and regulations. Currently, blocking is a practice that has begun to be carried out to close user access to content presented on the internet.[8]

[5] Asaf mname Lubin, 'Cyber Law and Espionage Law as Communicating Vessels', *SSRN Electronic Journal*, 2018 https://doi.org/10.2139/ssrn.3099769

[6] Jordan J. Plotnek and Jill Slay, 'Cyber Terrorism: A Homogenized Taxonomy and Definition', *Computers & Security*, 102 (2021), 102145 https://doi.org/10.1016/j.cose.2020.102145

[7] Brian H. Spitzberg and Gregory Hoobler, 'Cyberstalking and the Technologies of Interpersonal Terrorism', *New Media & Society*, 4.1 (2002), 71–92 https://doi.org/10.1177/14614440222226271

[8] Alfina Faradisa Karin, Moch. Syafrudin Dwi Sapto Laxamanahady, and Muhamad Alief Hidayat, 'The Right to Freedom of Expression in the Digital Age', in *Proceedings of the International Conference for Democracy and National Resilience 2022 (ICDNR 2022)* (Paris: Atlantis Press SARL, 2023), pp. 47–54 https://doi.org/10.2991/978-2-494069-75-6_8

The practice of blocking content that is not properly regulated has the potential to disrupt the values of human rights to expression in various public and personal activities. Criminalization of content deemed dangerous by the government can occur even if it is assessed subjectively.[9] In the criminalization policy, an act that was initially not a criminal act (not punishable) can be determined to be a criminal act (an act that can be punished). So, in essence, criminalization policy is part of criminal policy using criminal law (penal) means, and therefore is part of "criminal law policy," especially its formulation policy. Through existing policies, it is not impossible to direct massive content blocking. Consequently, it is necessary to limit government control in this matter.[10] This means relevant laws will be essential to handle hundreds of thousands of cases that occur at one time.

This is different from the United States, the Netherlands, and Singapore countries, which are more advanced in information technology. Still, crimes that occur in cyberspace, have been anticipated by law enforcement with various existing regulations, so the sense of legal certainty is more guaranteed. Of course, apart from that, the level of legal awareness among the people is relatively better. However, in these countries, there are also shortcomings. A comparison of the regulations for blocking dangerous content in each of the countries above can be a lesson learned. Many people think that behind the various technological advances the western world has embraced. Spiritual or moral dryness means that using the above technological advances is often found to be increasingly demeaning to human dignity. Several previous studies have been carried out regarding blocking dangerous content. Still, comparing several countries with different legal systems, a more democratic model of blocking regulation has not been found in detail or specifically.

Looking at research from Yemen Akdeniz (2010), due to the limited effectiveness of state laws and the lack of harmonization at the international level, several countries have begun implementing policies to block access to Internet content and websites considered illegal and located outside their legal jurisdiction. In line with this research, it is stated that blocking policies are not always subject to the principles of legal process, the courts do not always take decisions, and often administrative bodies run by the private sector decide which content or websites should be blocked. Therefore, the appropriateness of these blocking measures is increasingly being questioned in light of the fundamental right to freedom of

[9] Ayako Hatano, 'Regulating Online Hate Speech through the Prism of Human Rights Law: The Potential of Localised Content Moderation', *The Australian Year Book of International Law Online*, 41.1 (2023), 127–56 https://doi.org/10.1163/26660229-04101017

[10] Fernando Miró Llinares and Ana B. Gómez Bellvís, 'Freedom Of Expression In Social Media And Criminalization Of Hate Speech In Spain: Evolution, Impact And Empirical Analysis Of Normative Compliance And Self-Censorship', *Spanish Journal of Legislative Studies*, 1, 2019 https://doi.org/10.21134/sjls.v0i1.1837

expression.[11] However, this research only discusses European countries, while this paper examines America and Asia, represented by the United States and Singapore.

Similarly, Jelena Surculija Milojevic (2015) conducted a comparative study on blocking, filtering, and removing illegal Internet content in 47 Council of Europe member countries. The Constitution and Media Law guarantee freedom of expression but indicate situations where freedom of expression may be restricted. The Criminal Code regulates situations that can limit freedom of expression and remove Internet content if so determined by law. However, no specific protection has been established by the European Court of Human Rights regarding restrictions on freedom of expression in general and, more specifically, the blocking, filtering, and removal of illegal content in other laws. Therefore, there is a gap between the necessity and proportionality of interference with freedom of expression on the internet.[12]

Other research is related, for example, to research by Rizky Pratama (2022) on punishment for spreading hate speech, which is considered to damage unity. This research states that hate speech is not a form of freedom of opinion. Therefore, Law Number 11 of 2008 provides punishment for everyone proven to have committed hate speech, whether in defamation or containing hate speech. This research focuses on criminalizing hate speech on social media based on someone's uploads, not on criminalization in the form of blocking content. Interestingly, the indicators that content can be considered dangerous are very tricky. There are many types, and all of them need to be clarified so there is no criminalization of freedom of opinion.[13]

Currently, countries that frequently commit human rights violations can benefit from the presence of social media in their country (as long as these can be mitigated) rather than being harmed by the presence of social media. In democratic countries that truly practice freedom of opinion, they may be able to implement citizen values in utilizing social media. But what about countries that have a history of oppressing or violating the rights of their people. Countries where traditional media are strictly regulated, and activists and journalists are persecuted by the state. Or a democratic country whose practices are not like that. Sites or

[11] Yaman Akdeniz, 'To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression', *Computer Law & Security Review*, 26.3 (2010), 260–72 https://doi.org/10.1016/j.clsr.2010.03.004

[12] Faiq Wildana, 'An Explorative Study on Social Media Blocking in Indonesia', *The Journal of Society and Media*, 5.2 (2021), 456–84 https://doi.org/10.26740/jsm.v5n2.p456-484

[13] Rizky Pratama Putra Karo Karo, 'Hate Speech: Penyimpangan Terhadap UU ITE, Kebebasan Berpendapat Dan Nilai-Nilai Keadilan Bermartabat', *Jurnal Lemhannas RI*, 10.4 (2023), 52–65 https://doi.org/10.55960/jlri.v10i4.370

social media are forced to create rules that sometimes cause them to enforce laws that severely threaten human rights.[14]

Scholars have realized the magnitude of the impact of social media platforms on the implementation of regulatory frameworks for freedom of expression and democratic processes in various countries, so further research to regulate them is necessary. To be able to carry out an in-depth discussion of this issue, it is essential to carry out an in-depth study to provide a clear picture of the policy basis for implementing blocking measures on electronic media at this time. Next, a policy concept was formulated to stop actions in dealing with media content-based crime in the future. Based on the background above, researchers are very interested in studying the criminalization policy of blocking dangerous content in electronic communications networks in the United States, the Netherlands, and Singapore. Then, a law enforcement model for stopping harmful content in electronic communications networks that aligns with democratic values is formulated.

2. Research Method

This normative legal research uses a law and case approach and compares several countries. We take the Netherlands, the USA, and Singapore as examples of developed countries that adhere to democratic ideology. The conceptual approach is directed at the concept of democratic state administration in guaranteeing citizens' freedom of opinion or expression on social media. The concept of protecting human rights is also used as a reference for formulating relevant models of policies for blocking dangerous content. Legal materials are analyzed by reviewing primary and secondary legal materials. You can find similarities, differences, and contradictions between existing legal materials. We are delivered comprehensively so that it can be compared. Comparisons between countries can provide information on effective regulations compared to criminal ones. Conclusions are drawn deductively.

3. Results and Discussion

Regulates on the Blocking of Hazardous Content in the Netherlands, the United States, and Singapore

Many countries are currently engaged in legislative efforts to regulate the impact of social media in their societies, and these efforts have a significant effect on society, especially on activists and journalists. Comparing regulations and policies made by other countries is an exciting study. Countries in North America and Western Europe are among the nations where research is often conducted

[14] Mackenzie F. Common, 'Beyond the Usual Suspects: A Taxonomy of Social Media Regulations in Countries with Human Rights Issues', *International Review of Law, Computers & Technology*, 37.1 (2023), 1–28 https://doi.org/10.1080/13600869.2022.2043093

because these countries have strong human rights protections.[15] Blocking harmful content that leads to the silencing of democracy has become an international record and research throughout the world.[16]

Take the example of cybercrime policies and regulations in the United States. The unstoppable spread of internet use has given rise to, and continues to give rise to, various studies, policies, proposals, and draft legislation regulating information technology museology. The United States has enacted different laws that criminalize acts related to information technology crimes. Cybercrime regulations in the United States include the Computer Fraud and Abuse Act (Title 18 Part I Chapter 47 Section 1030 titled "Fraud and related activity in connection with computers"), which aims to tackle computer hacking, in the 1986 United States Congress. Computer Fraud and Abuse Act Regulations were amended in 1994, 1996, and 2001.

Apart from the Computer Fraud and Abuse Act contained in Title 18 Part I Chapter 47 Section 1030, the United States Congress also regulates information technology crimes related to the internet, such as: 1) Access Device Fraud Act of 1984 (18 USC Section 1029); 2) Wire Fraud Statute of 1952 (18 USC Section 1343); 3) Criminal Infringement of a Copyright (the Copyright Act of 1976) (18 USC Section506(a)); 4) Counterfeit Trademarks (the Trademark Counterfeit Act of 1984) (USC Section2320); 5) Mail Fraud (18 USC Section 1341); 5) Conspiracy to Defraud the US Government (18 USC 371); 6) False Statements (18 USC Section 1001); 7) Identity Theft and Assumption Deterrence Act of 1998 (18 USC Section 1028); 8) The Racketeer Influenced and Corrupt Organizations Act (RICO) (18 USC Section2511); 9) Wire and Electronic Communications Interception of Oral Communications (18 USC Section 2511); 10) Unlawful Access to Stored Communications (18 USC 2701); 11) Transportation of Stolen Goods, Securities, Moneys (18 USC Section 2314); 12) Trafficking in Counterfeit Goods and Services (18 USC Section 2320); 13) Extortion and Threats (18 USC Section 875).

Also included in the Electronic Theft Prohibition Act of 1997, it was introduced to close a loophole in previous United States copyright law that did not recognize copyright infringement if the defendant did not gain a profit. The National Stolen Property Act of 1934 and the Economic Espionage Act of 1996 prohibit the misappropriation of trade secrets. The Identity Theft and Assumption Deterrence Act of 1998 was intended to create a new offense for anyone who transfers or uses, without permission, another person's means of identification with the intent to

[15] Dissa Syakina Ahdanisa and Steven B. Rothman, 'Revisiting International Human Rights Treaties: Comparing Asian and Western Efforts to Improve Human Rights', *SN Social Sciences*, 1.1 (2021), 16 https://doi.org/10.1007/s43545-020-00018-0

[16] S.M. Dhawan, B.M. Gupta, and B. Elango, 'Global Cyber Security Research Output (1998–2019): A Scientometric Analysis', *Science & Technology Libraries*, 40.2 (2021), 172–89 https://doi.org/10.1080/0194262X.2020.1840487

commit or assist, abet, in any unlawful activity. The breach included using unique biometric data and electronic means of identification.[17] Indonesia also has a legal basis for criminalizing cybercrime. Likewise, institutions are given the task of formulating policies. However, its formulation is sometimes seen as not being able to guarantee the protection of human rights because it opens up space for over-criminalization, which is less than objective. [18]

The United States has also regulated gambling via the internet through the federal government's implementation of The Wire Act, The Travel Act, The Professional and Amateur Sports Protection Act, and the Interstate Transportation of Wagering Paraphernalia Act. Much attention has also been paid to the issue of obscenity. And adult entertainment and cyberporn, especially child pornography. In this case, it can be mentioned that there are provisions regarding the Federal Obscenity Law in the form of Transportation of Obscene Matters for Sale or Distribution (18 USC Section 1465) and the Communications Decency Act of 1996. The United States regulations are at a complete and specific stage regarding forms of crime on the internet that happened or might even happen. The rules used to guarantee legal certainty and protect people's rights should be appreciated.

Meanwhile, in the policy formulation for cybercrime in the Netherlands, a commission called the Franken Commission was formed, which provided input regarding cybercrime regulation. The commission considers Mayantara crime to be an ordinary crime committed using high-tech computers, so it only refined the *Wetboek van Strafrecht* (Dutch Criminal Code) in 1993 so that it could be used to tackle Mayantara crime (of course with additions) by including specific criminal provisions. Commissie Franken formulated several cyber crimes in the formulation of *Wetboek van Strafrecht*, the formulation of nine forms of misuse (*misbruikvorme*n), namely, without the right to enter a computer system; without the right to take (*onderscheppen*) computer data; without the right to know (*kennisnemen*); without copying or copying rights; without the right to change; retrieve data; without the right to use the equipment; sabotage of computer systems; disrupt telecommunications.

The Netherlands also has criminal law provisions regarding child pornography. Amendments to the Criminal Code were made in 2002, and regulations were introduced to criminalize virtual child pornography. This change in law is necessary because modern technology facilitates the production of graphic child pornographic visual material without the direct involvement of actual children. In addition, it ratified the Council of Europe Convention on the

[17] Jonathan Lusthaus and others, 'Cybercriminal Networks in the UK and Beyond: Network Structure, Criminal Cooperation and External Interactions', *Trends in Organized Crime*, 2023 https://doi.org/10.1007/s12117-022-09476-9

[18] Benoît Dupont and Chad Whelan, 'Enhancing Relationships between Criminology and Cybersecurity', *Journal of Criminology*, 54.1 (2021), 76–92 https://doi.org/10.1177/00048658211003925

protection of children from sexual exploitation and sexual abuse (Lanzarote Convention). The implementation of the Convention has led to the tightening of Dutch criminal law provisions regarding the protection of children from sexual abuse. Provisions regarding child pornography are increasingly tightened by the criminalization of gaining access, through information and communication technology, to child pornography.[19]

There is an exciting development in the information technology crime prevention policy in Singapore, based on The Computer Misuse Act (CMA) 1993. The CMA is modeled based on the 1990 British law, which regulates 4 (four) things, namely: 1) Unauthorized access, Article 3 of the CMA prohibits "hacking," which causes a computer to play its function to secure unauthorized access to any program or data stored on the computer. Article 3, paragraph 1 CMA, the target is only on unauthorized access. Article 3 paragraph 2 of the CMA, any access that results in losses exceeding 10,000 dollars will be subject to severe penalties; 2) Access with ulterior motives, Article 4 of the CMA criminalizes unauthorized access where there is an aim to commit or facilitate an offense involving property, fraud, dishonest acts, or acts that result in bodily harm; 3) Modification of computer content, Article 5 of the CMA relates to unauthorized and intentional modification of computer content such as data, computer software programs and databases, for example by inserting viruses into the computer system; 4) Intercepting a computer service, Article 6 of the CMA introduces a new concept regarding the unauthorized use or interception of a computer service, this may be more akin to theft of services or computer usage time.

Specific to the regulation of blocking harmful content in Singapore, the Online Criminal Harm Act (OCHA) was passed in Parliament on 5 July 2023. This law aims to protect the public from harm in online spaces and introduces mechanisms for authorities to deal with activities of online crime more effectively. Although OCHA does not define "online criminal harm," it targets criminal activities such as fraud and malicious cyber activity, as well as all online communication media (e.g., websites and applications) that can be used to carry out criminal activities. The harm that OCHA seeks to prevent includes illegal money lending, unlawful gambling, and drug-related offenses. A list of "specific offenses" is set out in Schedule 1 of OCHA. This has, among other things, offenses under the Computer Misuse Act (e.g., unauthorized access to computer material) and Part 2 of the Protection from Harassment Act (POHA). For example, if threatening, abusive, or insulting communications are directed at an individual under section 3 POHA,

[19] E. Rutger Leukfeldt, Anita Lavorgna, and Edward R. Kleemans, 'Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime', *European Journal on Criminal Policy and Research*, 23.3 (2017), 287–300 https://doi.org/10.1007/s10610-016-9332-z

these online communications can be addressed through appropriate Government Guidance.

It should be understood that even in America, content blocking is still considered very controversial. As time passed, countries began to employ more subtle but insidious strategies to discourage social media use. Blocking is carried out covertly through regulations that impose a combined financial and administrative burden, making access to the platform difficult and expensive. Tax and social media licensing laws can make anonymity impossible and open users to further criminal sanctions. For example, Tanzania, requires all content creators to fill out a detailed application that includes their address, contact information, and ID/passport number.[20]

In the European Union, the adaptation of content-blocking policies of specific member states is used to assess the nature and implementation of access-blocking policies. Site blocking must be carried out for clearly detrimental and dangerous content. However, as in other democratic countries, blocking that intersects with freedom of opinion has the potential to give rise to a violation of Article 10 of the European Convention on Human Rights, especially if blocking measures or filtering tools are used at the state level to silence politically motivated speech on the internet.[21] Shifting to Serbia, where freedom of expression on the internet is still very fragile, blocking, filtering, and removing illegal internet content is not always carried out according to the law or following procedures. Occasional hacking attacks that cause websites to be unavailable for several days seem like a new form of censorship that the Council of Europe should consider more closely in its future policies.[22]

However, Eva Nave's (2023) research shows that the European Union's regulations for blocking harmful content show positive relevance. It is stated that regarding Human Rights Due Diligence (HRDD) and moderation of harmful content online, the Regulations for Digital Services Act (DSA) adds to the European Union Audiovisual Media Services Directive (AVMSD). There is increased cross-sector due diligence responsibility for digital services to remove illegal content online, including hate speech. Interestingly, the European Union has a due diligence framework in the DSA that is based on a Code of Conduct for countering illegal hate speech online. They set service providers committed to immediately reviewing and removing hate speech and encouraging transparency toward users.[23]

[20] Common.
[21] Akdeniz.
[22] Wildana.
[23] Nave and Lane.

Because service providers have access to regulate content that is suitable for posting and that violates community rules. They can even use it to interfere with the atmosphere of democratic mysticism on their platforms.[24] Arrangements like this are essential to deal with the spread of dangerous content, which harms material and personal life and can also trigger social friction. The urgency of this problem is increasingly recognized when in the European Union, 80% of people have experienced hate speech online, and 40% have felt attacked or threatened via Social Networking Sites.[25]

Meanwhile, in America, different democratic and political mechanisms can lead to increased hostility and intolerance towards other people via Social Networking Service. This anti-Islam sentiment is linked to religion, ethnicity, politics, and gender, thereby encouraging symbolic violence rather than engaging in constructive conflict.[26] Therefore, apart from blocking content by the government, people individually carry out filtering and blocking. Multiple social media users produce content that has various points of view. The spread of dangerous content can be found quickly and can cause disputes that can even lead to criminal acts. According to research by Yang et al. (2017), there is a greater possibility that social media users will face political disputes in America.[27] This aligns with research conducted by Hsu & Gil de Zúniga, 2013, where social media users often face cross-sectoral information and political disputes. Many of them filter and block accounts or posting content that they disagree with.[28] Unsurprisingly, the criminalization of content blocking is often linked to guaranteeing the human right to expression.[29]

Findings from Lance Y. Hunter's (2023) analysis of 158 United States states from 2000–2019 show that different types of social media use have other impacts on democracy. General social media consumption, diverse political viewpoints on

[24] Ugur Aytac, 'Digital Domination: Social Media and Contestatory Democracy', *Political Studies*, 72.1 (2024), 6–25 https://doi.org/10.1177/00323217221096564

[25] Björn Gambäck and Utpal Kumar Sikdar, 'Using Convolutional Neural Networks to Classify Hate-Speech', in *Proceedings of the First Workshop on Abusive Language Online* (Stroudsburg, PA, USA: Association for Computational Linguistics, 2017), pp. 85–90 https://doi.org/10.18653/v1/W17-3013

[26] Matthew Barnidge, 'The Role of News in Promoting Political Disagreement on Social Media', *Computers in Human Behavior*, 52 (2015), 211–18 https://doi.org/10.1016/j.chb.2015.06.011

[27] Sergio Andrés Castaño-Pulgarín and others, 'Internet, Social Media and Online Hate Speech. Systematic Review', *Aggression and Violent Behavior*, 58 (2021), 101608 https://doi.org/10.1016/j.avb.2021.101608

[28] JungHwan Yang, Matthew Barnidge, and Hernando Rojas, 'The Politics of "Unfriending": User Filtration in Response to Political Disagreement on Social Media', *Computers in Human Behavior*, 70 (2017), 22–29 https://doi.org/10.1016/j.chb.2016.12.079

[29] Yonghwan Kim, Shih-Hsien Hsu, and Homero Gil de Zúñiga, 'Influence of Social Media Use on Discussion Network Heterogeneity and Civic Engagement: The Moderating Role of Personality Traits', *Journal of Communication*, 63.3 (2013), 498–516 https://doi.org/10.1111/jcom.12034

social media, and the use of social media in political campaigns support democracy. However, social media disinformation, online political polarization, and the use of social media to orchestrate offline violence reduce overall levels of democracy.[30]

Freedom of speech is the right to think independently, examine the world critically, and question and hear new perspectives or information, including thoughts and debates that others consider irrational or conspiracy theories. Heike Holbig (2020), in his research, provides advice on cybercrime cases, especially regarding the criminalization of content that is always associated with hate speech, which ultimately kills democracy. Advice was given to provide open space, responding to suggestions and answers without criminalizing. This may be related to accepting ideas so that tolerance arises towards socially divisive speech. This protects the right to collect and communicate ideas to others who are unaware of the content.[31] In Singapore, the Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) also raises similar concerns about whether the law will overly restrict freedom of expression. This regulation is considered to still be able to cause problems due to a lack of transparency.[32]

Limitations on freedom of expression must of course be believed to exist so as not to demand unlimited freedom. Transparency and monitoring of these rights needs to be carried out by people who use social media, through a more relevant policy model for blocking dangerous content. Established regulations must be interpreted to clarify how (and whether) each provision stipulates that freedom of speech can be restricted, for example to protect national security.[33] In Singapore, to address fraud and malicious cyber activity carried out at high speed and scale, the threshold that must be met for the government to take action is lower, allowing them to act quickly to address such criminal activity.

A list of fraudulent and malicious cyber activities is in Part 2 of Schedule 1 of OCHA. They include 1) Offenses under the Computer Misuse Act; 2) Offenses related to extortion, gang robbery, criminal breach of trust, and fraud through false representation under the Criminal Code; 3) Conspiracy, or conspiracy or attempt to commit an offense. Additionally, designated agencies can issue directives even

[30] Lance Y. Hunter, 'Social Media, Disinformation, and Democracy: How Different Types of Social Media Usage Affect Democracy Cross-Nationally', *Democratization*, 30.6 (2023), 1040–72 https://doi.org/10.1080/13510347.2023.2208355

[31] Heike Holbig, 'Be Water, My Friend: Hong Kong's 2019 Anti-Extradition Protests', *International Journal of Sociology*, 50.4 (2020), 325–37 https://doi.org/10.1080/00207659.2020.1802556

[32] Chen Siyuan, 'Regulating Online Hate Speech: The Singapore Experiment', *International Review of Law, Computers & Technology*, 2023, 1–21 https://doi.org/10.1080/13600869.2023.2295091

[33] Nikolai Haahjem Eftedal and Lotte Thomsen, 'Motivated Moral Judgments about Freedom of Speech Are Constrained by a Need to Maintain Consistency', *Cognition*, 211 (2021), 104623 https://doi.org/10.1016/j.cognition.2021.104623

before an offense is committed if there is a suspicion that any online activity is being carried out in preparation for or as part of a fraudulent act or malicious cyber activity offense. The Government Directive can be imposed on four categories of people: 1) Those with control or ownership of online criminal content; 2) Online service providers; 3) Internet access service providers; and 4) Application distribution service providers.

Ultimately, the democratic countries above aim to maintain the human right to freedom of expression and opinion in public in common. Regulations in the United States are pretty detailed to regulate cyber crimes. Likewise, the Netherlands also formed a special commission to enforce its laws. The Netherlands is also heavily affected by European Union regulations. Unfortunately, the Netherlands and the United States do not yet have up-to-date regulations to resolve cases of blocking dangerous content using relatively new methods. Meanwhile, Singapore seems to be one step ahead with the sensitivity of its rules on the issue of hazardous content. However, the three of them are still faced with blocking matters related to democracy - the human right to expression on social media.

The Model of Regulatory for Blocking Dangerous Content in Electronic Communications Networks to Guarantee Freedom of Expression

Policy formulation is the most strategic "penal policy" stage to find relevant laws for blocking content. At the formulation stage, all crime prevention plans are prepared using the criminal law system, which includes three main problems, namely: 1) the problem of formulating criminal acts (criminalization), 2) criminal responsibility, and 3) criminal regulations and punishment. First, criminalization policy determines and formulates what actions can be punished and then provides criminal sanctions that can be imposed on violators. This is closely related to the principle of legality, which requires legislators to determine first what a criminal act means; it must be formulated more clearly. This formula plays a role in determining what is prohibited or what a person must do.

Therefore, blocking dangerous content must have a clear legal basis. Prevent freedom of opinion and expression from being damaged by a legal mindset that tends to criminalize without objectivity and protection of human rights.[34] Efforts to prevent crime are the task of law enforcement officials and law-making officials. Regarding determining which acts are considered criminal, we adhere to the principle of legality, namely that an act is only a criminal act if it is determined first in a statutory provision (Article 1 paragraph 1 of the Code Criminal Law). It

[34] Kenneth S. Gallant, *The Principle of Legality in International and Comparative Criminal Law* (Cambridge University Press, 2008) https://doi.org/10.1017/CBO9780511551826

can be interpreted that there is no crime, no criminal punishment without prior criminal law.[35]

Anyone who commits a criminal act is threatened with specific penalties determined in statutory provisions. However, in convicting someone suspected of committing a criminal act, they are not punished without fault—*geen straf zonder schuld*. Determination of how illegal imposition can be carried out if a person is suspected of committing a criminal act is regulated in formal criminal law or criminal procedural law. Van Bemmelen said that criminal procedural law studies the regulations created by the state because of allegations of violations of criminal law. Efforts to overcome future information technology crimes and ensure that the formulation of offenses in Law No. 11 of 2008 can be operational.

The problem of criminalization arises because of the emergence of acts with a new dimension, so the law for these acts has not yet been determined. The impression that emerges is that there is a legal vacuum that ultimately encourages this act's criminalization. The sources of material in policies for making changes and drafting new offenses are taken, among others, from 1) Input from various scientific meetings (symposiums/seminars/workshops), which also means from various circles of the wider community; 2) Input from several research and study results regarding the development of specific offenses in society and the development of science and technology; 3) Input from the study and observation of new forms and dimensions of crime in international meetings or congresses; 4) Input from various international conventions (both those that have been ratified and those that have not been ratified); and 5) Input from the results of comparative studies of various Criminal Codes from other countries. Criminalization in cyberspace with special regulations outside the Criminal Code must be carried out carefully, lest it gives the impression of being repressive, which violates the *ultimum remedium* principle (*ultimum ratio* principle) and backfires in social life in the form of excessive criminalization (over-criminalization), which reduce the authority of the law.[36]

We recommend formulating a criminalization policy model in regulations as follows. The Criminal Code differentiates "general rules" for criminal acts in the form of "crimes" and "violations." This means that the qualification of an offense in the form of a "crime" or "violation" is a "juridical qualification" that will bring different "juridical consequences." Therefore, every criminal act formulated in Law Number 11 of 2008 must have its juridical qualifications stated. If it is not mentioned, it will give rise to juridical problems in applying the general rules of

[35] Zaka Firma Aditya and Sholahuddin Al-Fatih, 'Indonesian Constitutional Rights: Expressing and Purposing Opinions on the Internet', *International Journal of Human Rights*, 0.0 (2020), 1–25 https://doi.org/10.1080/13642987.2020.1826450

[36] Youngjae Lee, 'Proxy Crimes and Overcriminalization', *SSRN Electronic Journal*, 2022 https://doi.org/10.2139/ssrn.4051022

the Criminal Code to Law Number 11 of 2008. Then, in efforts to overcome information technology crimes, it can be expanded to include criminal acts in the form of "malicious conspiracy," "preparation," "relief," and "repetition" *(recidive)*.

Second, regarding criminal responsibility, in criminal law, two crucial things need attention: the commission of a criminal act *(actus reus)* relating to the subject or perpetrator of the criminal act and the error *(mens rea)* relating to the issue of responsibility. Criminal. About the principle of criminal law, namely "*Geen straf zonderschuld, actus non facit reum nisi mens sir rea*," that "not to be punished if there is no mistake," then the meaning of "criminal act" is separate from what is meant by "responsibility for a criminal act." It only refers to the prohibition and threat of a criminal act; whether the person who commits the act is also punished as threatened will depend significantly on whether the perpetrator also made a mistake in carrying out the act. Meanwhile, the basis for responsibility is the fault found in the perpetrator's soul about his behavior, which can be punished, and based on his mental state, the perpetrator can be blamed for his behavior. In other words, only with this inner connection can the perpetrator be held accountable for the prohibited act.[37]

This guilty mind *(guilty mind, mens rea)* is a mistake that is the subjective nature of a criminal act because it is within the perpetrator. Therefore, guilt has two aspects, namely, the psychological aspect and the normative aspect. The psychological element of error must be sought in the perpetrator's mind, namely the existence of an inner connection with the action he has committed so that he can be held accountable for his actions. The normative aspect is based on the measurements commonly used by society to determine whether there is an inner relationship between the perpetrator and his actions.

Criminal liability must first fulfill objective requirements, namely that the action must constitute a criminal act according to applicable law. In other words, for criminal accountability to exist, the principle of legality must first be met, namely that there must be a clear legal basis or source (source of legitimacy), both in material or substantive criminal law and formal criminal law. Apart from that, subjective requirements must also be met, namely the existence of an inner attitude within the perpetrator or the principle of culpability. About the principle of guilt, Moeljatno thinks that even though a criminal act has been committed, the author cannot always be punished (can be held accountable). Furthermore, in general, the maker can be held responsible, but this is not always the case. This was further emphasized by Honderic, who said: "punishment is not always the

[37] David Maimon and Eric R. Louderback, 'Cyber-Dependent Crimes: An Interdisciplinary Review', *Annual Review of Criminology*, 2.1 (2019), 191–216 https://doi.org/10.1146/annurev-criminol-032317-092057

case of an offender."[38] Furthermore, the law enforcement process aims to realize justice and order in social life through the criminal justice and punishment systems. The rights of citizens who are disturbed due to someone's unlawful actions will be rebalanced. Satjipto Raharjo stated that the law enforcement process also extends to law-making. The formulation of ideas for making laws (laws) as outlined in legal regulations will also determine how law enforcement is carried out.[39]

The performance of legal institutions naturally receives relatively high attention from the people because they are the ones who have the task of translating legal rules into practice to resolve disputes and conflicts that occur in society, especially the entire criminal justice system (if not, can be called a system because it seems to have a thicker non-system color), namely the police, prosecutor's office, courts, and correctional institutions as well as human resources, which are currently receiving extraordinary attention. Coupled with this spotlight, these institutions are simultaneously the source and object of societal neglect, disrespect, and distrust.

To increase the effectiveness and renew the orientation (reform or reconstruction) of criminal law enforcement in the face of cybercrime need to take several steps (efforts), including the following: 1) Increasing strategic commitment or national priorities in overcoming crime in the field of morality, which should be aligned with efforts to overcome criminal acts of corruption, drugs, terrorism and so on; 2) Carry out renewal of juridical thinking/construction (juridical construction reform). Efforts to renew or reconstruct juridical thinking should be carried out in all areas of criminal law enforcement. However, it is essential in dealing with cybercrime problems because cybercrime cannot be equated with conventional criminal acts, so it cannot be faced with law enforcement and traditional legal thinking or construction.[40]

Apart from that, law enforcement officials are doing several things to overcome information technology crimes in the future. Educating law enforcement officers in handling cybercrime cases requires specialization of investigative officers and public prosecutors, which can be considered as one way to carry out law enforcement against cybercrime. This specialization starts with education aimed at mastering technical and basic knowledge in the field of computers and hacker

[38] Jesper Ryberg, 'Punishment and Political Philosophy', in *Oxford Research Encyclopedia of Politics* (Oxford University Press, 2016) https://doi.org/10.1093/acrefore/9780190228637.013.200
[39] Benoit Dupont, 'Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime', *Crime, Law and Social Change*, 67.1 (2017), 97–116 https://doi.org/10.1007/s10611-016-9649-z
[40] Joanna Curtis and Gavin Oxburgh, 'Understanding Cybercrime in "Real World" Policing and Law Enforcement', *The Police Journal: Theory, Practice and Principles*, 96.4 (2023), 573–92 https://doi.org/10.1177/0032258X221107584

profiles.[41] Indonesia needs Cyber Police, Cyber Prosecutors, and Cyber Judges to enforce cybercrime law in Indonesia. Without law enforcers skilled in information technology, it will be challenging to ensnare cyber criminals because this cyber crime can be cross-linked. country. What is more important in law enforcement efforts is the existence of socialization in the form of upgrading, courses, or joint vocations between law enforcement officers in the context of equal perception in evidentiary procedures in criminal information technology cases. Building forensic computing facilities: The forensic computing facilities that the National Police will establish are expected to serve three important things, namely: 1) evidence collection, 2) forensic analysis, and 3) expert witness.[42]

Improving facilities or facilities in dealing with information technology crimes is not only limited to making every effort to update and upgrade the facilities and infrastructure already owned by law enforcement officials but also by completing these facilities or facilities by current technological developments. Therefore, skilled personnel and costs are needed, primarily to support the capabilities and skills of law enforcement officers in the computer field. This facility should not only involve the National Police, but the Government, through the communications and information department, should build its facility, which functions as an information center or laboratory, like a forensic laboratory, as a place for research for investigation and development of information technology.

It must be acknowledged that Indonesia has not taken significant steps in law enforcement to anticipate cybercrime by developed countries in Europe and the United States. In England and Germany, they formed a joint institution tasked with dealing with Cybercrime Investigation problems named the National Criminal Intelligence Service (NCIS), headquartered in London. In 2001, England launched the "Trawler Project" and formed the National Hi-tech Crime Unit, equipped with a particular budget for cyber cops. Meanwhile, the United States also created a Computer Emergency Response Team (CERT) based in Pittsburg in the 1990s, and the Federal Bureau of Investigation (FBI) has a Computer Crime Squad to tackle cybercrime.[43]

Along with the development of technology, Law No. 11 of 2008 aims to provide legal certainty regarding every action in cyberspace. However, implementing this regulation has caused much controversy and criticism—Law No. 11 of 2008 limits

[41] Myriam Dunn Cavelty, 'Cybersecurity Research Meets Science and Technology Studies', *Politics and Governance*, 6.2 (2018), 22–30 https://doi.org/10.17645/pag.v6i2.1385

[42] Mary-Jane Sule, Marco Zennaro, and Godwin Thomas, 'Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends', *Technology in Society*, 67 (2021), 101734 https://doi.org/10.1016/j.techsoc.2021.101734

[43] Ioannis Agrafiotis and others, 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity*, 4.1 (2018) https://doi.org/10.1093/cybsec/tyy006

the space for citizen expression within a democratic framework. One of the first steps in handling criminal acts related to freedom of expression in digital media can be done through preventive efforts, namely cyber patrol. Cyber patrol or virtual patrol is a monitoring effort carried out by the Police over activities in cyberspace to prevent law violations in cyberspace. Virtual patrols are carried out by the Police in collaboration with the Ministry of Communication and Information.[44]

Third, punishment, the development of forms and dimensions of crime, certainly requires handling; one way of dealing with this is using penalties or criminal sanctions. Criminal sanctions are one of the central issues in criminal law, therefore it is essential to study the appropriate form of punishment in dealing with cybercrime. The issue of punishment itself is an integral part of a sentencing policy which, according to Herbert L. Packer, is one of the current controversial issues in criminal law. The problem of criminalization is a problem that always requires reconsideration, considering that it is inherent in the nature and essence of crime itself, which is constantly changing and developing. Then, changes and developments in crime are always followed by changes and developments in crime itself.

Punishment can be interpreted as the stage of determining sanctions and giving sanctions in criminal law. If someone is guilty of violating the law, he must be punished. The issue of punishment is not just a matter of convicting someone by throwing him in prison; punishment must contain an element of loss or misery carried out by an authorized institution. Therefore, punishment is not revenge from the victim against the lawbreaker who causes suffering. The determination of types of crime by legislators is intended, among other things, to provide a set of tools for law enforcers in order to tackle crime. Apart from that, it is also intended to limit law enforcement officials from using the means in the form of criminal penalties that have been determined. They may not use criminal means that the legislator does not previously determine. Thus, the type of crime chosen and determined by the legislator binds and limits other law enforcers.[45]

Therefore, an essential part of the criminal system is determining the type of crime or sanction. Its existence will provide direction and consideration regarding what should be used as sanctions in a criminal act to enforce the enactment of norms. On the other hand, punishment is the most complex process in the criminal justice system because it involves many different people and institutions. Thus, if the set of criminal sanctions that have been determined result from inappropriate

[44] Toni Harmanto, Bagus Oktafian Abrianto, and Xavier Nugraha, 'Penal Mediation By Police Institution In Handling Hate Speech Through Electronic Media: A Legal Efforts To Resolve with A Restorative Justice Approach', *International Journal Of Artificial Intelligence Research*, 6.1.2 (2022). https://doi.org/10.29099/ijair.v6i1.388

[45] *Cyber Criminology*, ed. by K. Jaishankar (Routledge, 2011) https://doi.org/10.1201/b10718

choices or are no longer following the development of criminality, then it is natural that the response to the development of criminality will be disrupted.[46]

Determination of criminal sanctions, imposition of a crime, and execution of a crime are closely related to the purpose of punishment. Therefore, the purpose of punishment must be used as a benchmark before determining criminal sanctions. The punishment that will be selected is a crime expected to support achieving the objectives. The effectiveness of punishment must be measured based on the goals or results to be completed. Based on the definition above, the formulation, objectives, and guidelines for punishment start from the following thoughts: In essence, the law is a system (law) with a purpose (purposive system). The formulation of criminal penalties and punishment rules in law is essentially only a means to achieve goals.

Functionally and operationally, punishment is a series of processes and policies whose concretization is deliberately planned through several stages (formulation, application, execution). It is necessary to formulate objectives and guidelines for punishment to intertwine and integrate the three stages as a unified criminal system. A criminal system that departs from criminal individualization does not mean giving complete freedom to judges and other officers without guidance or control. The formulation of objectives and guidelines is intended as a "controlling function" and, at the same time, provides a philosophical basis, rationality, and motivation for punishment that is clear and directed.

Starting from the definition of the criminal system, L.H.C. Hulsman put forward the definition of the criminal system as statutory rules relating to criminal sanctions and punishment (the statutory regulations relating to penal sanctions and punishment). Therefore, all material or substantive criminal law, formal criminal law, and unlawful implementation law can be seen as one unified sentencing system (the sentencing system). To be implemented (operationalized or functional), the formulation of criminal sanctions must still be supported by other sub-subsystems, namely the sub-system of rules or guidelines and criminal principles contained in the general rules of the Criminal Code or special rules in the relevant special law.[47]

Therefore, in order for the formulation of criminal sanctions to be operational, it must pay attention to the general rules contained in the Criminal Code. Viewed from the perspective of *"strafsoort"* (types of criminal sanctions), all punishment regulations in the Criminal Code are oriented to the *"strafsoort"* that exists or is

[46] C. Schafers and J. Stephen Wormith, 'Criminality', in *Encyclopedia of Mental Health* (Elsevier, 2023), pp. 526–37 https://doi.org/10.1016/B978-0-323-91497-0.00161-2

[47] Annika Elisabet Suominen, 'What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?', *Bergen Journal of Criminal Law & Criminal Justice*, 2.1 (2014), 1 https://doi.org/10.15845/bjclcj.v2i1.615

mentioned in the Criminal Code, both in the form of basic penalties and additional penalties. Therefore, if a particular law says types of crimes or other actions that are not in the Criminal Code, then the special law must make special criminal regulations for those types of criminal sanctions. According to the Criminal Code pattern, the types of punishment that are formulated or threatened in the formulation of an offense are only the main punishment and/or additional punishment. The crime of "substitute imprisonment" is not formulated in the formulation of the offense (special rules), but is included in the general rules regarding the implementation of the crime *(strafmodus)*. Special laws do not need to have substitute imprisonment as a type of punishment that is threatened in the formulation of the offense, especially if the length of substitute imprisonment does not deviate from the general rules of the Criminal Code. Even if it is deviant, the formulation is not included as a *strafsoort* in the formulation of the offense, but is regulated separately in the rules regarding criminal implementation (*strafmode or strafmodus)*.

Viewed from the perspective of *"strafmaat"* (a measure of the amount or length of punishment), the punishment rules in the Criminal Code are oriented towards a general minimum and specific maximum system, not introduced towards a specific minimum system. This means that in the Criminal Code there are no sentencing regulations for specific minimum criminal threats. Therefore, if a particular law creates specific minimum criminal threats, it must also be accompanied by rules or guidelines for its implementation. The general criminal provisions in the Criminal Code are oriented towards "natural persons", not aimed at "corporations". Therefore, if a particular law states that there are criminal sanctions for corporations, it must also be accompanied by special regulations for punishment for corporations. Based on the things above, to be more effective in efforts to overcome information technology crimes, criminal sanctions should not be formulated in a cumulative manner which is imperative and rigid, but instead criminal sanctions should be formulated in alternative or optional ways or cumulatively-alternatively in order to provide leniency to application stage by looking at the problem casuistically.

By formulating alternative criminal sanctions, the perpetrator will be given the option of imposing a principal penalty in the form of imprisonment or a fine based on the motive and purpose of committing the criminal act, which will be considered by the judge in handing down the sentence. The only types of criminal offenses are prison fines and/or fines formulated cumulatively. Thus, no additional crimes or sanctions are integrated into the criminal system. Different types of crimes or actions should be regulated to overcome information technology crimes, such as 1) Prohibition of internet use during a specified time limit and 2) Payment of compensation for victims. The threat of criminal acts in Law No. 11 of 2008 does not recognize a minimum criminal threat. In the context

of reform, including minimum penalties for information technology crimes is entirely appropriate. However, regulations or guidelines are needed to operationalize the minimum criminal threat.[48]

The subject of criminal acts in the Criminal Code is only "people," so all criminal provisions in the Criminal Code are oriented towards "people," not corporations. Therefore, if Law No. 11 of 2008 expands the subject of criminal acts to corporations, it should also be accompanied by special criminal or liability regulations for corporations. Special provisions need to be made regarding implementing criminal penalties for non-payment by corporations. This is important because if a corporation is treated as the subject of a criminal offense but does not pay, the corporation can't undergo a substitute prison sentence.

Law Number 11 of 2008 has no special provisions regarding compensation for unpaid fines. This means that the general requirements of Article 30 of the Criminal Code apply. To make fines more effective, special requirements that deviate from Article 30 of the Criminal Code (regarding the implementation of penalties for unpaid fines or penalties instead of fines) must be made. There is a need for additional basic penalties for corporations. Draft Convention on Cybercrime Title 5, Art.13 states each party shall ensure that legal person shield liability by Article 12 (corporate liability) shall be subject to effective, proportionate, and dissuasive criminal or non-criminal sanctions or measures, including monetary sans. From this draft, the most suitable corporate punishments are fines and deprivation of liberty.

Eventually, internet use in various sectors will help interaction between society, businesses, government, and politics. However, cybercrime has become a consequence of an ecosystem, even though it cannot be justified. Various social media platforms are said to be one of the causes of the decline of democracy due to conflicts between internet users. However, it would help if you remembered the balance between freedom and the rights of other people and the applicable laws.[49] Therefore, regulatory formulation will be fundamental to strictly regulate the criteria for dangerous content that should be blocked. Without indicators, accusations of a decline in democracy and even issues of human rights to expression and opinion will continue to color the use of social media throughout the world, including countries with claims of a strong and good level of democracy. Apart from that, community participation and its culture need to be carried out to build or raise the sensitivity of citizens and law enforcement officials

[48] Krzysztof Szczucki, 'Ethical Legitimacy of Criminal Law', *International Journal of Law, Crime and Justice*, 53 (2018), 67–76 https://doi.org/10.1016/j.ijlcj.2018.03.002

[49] Barrie Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law', *European Journal of International Law*, 32.1 (2021), 159–93 https://doi.org/10.1093/ejil/chab022

to the problem of cybercrime and disseminate or teach the legal and ethical limits of internet use.

4. Conclusion

Blocking dangerous content by the government is to deal with increasingly widespread cyber crimes. The content becomes eligible to be restricted and blocked if it is deemed to cause social unrest because it can clash with social values or norms, religious norms, and public morality or even violate written laws made by the government. The right to access social media is part of the right to freedom of information. This means that accessing social media is a derogable right whose fulfillment can be limited by the government. However, blocking hundreds of sites or content deemed to violate often ignores the objectivity of criminalization so that it is accused of violating freedom of expression and opinion—human rights. However, this is still part of human rights, so restrictions on fulfillment must be based on the legal corridors stipulated in international covenants that regulate these restrictions. The limits must be carried out with a legitimate aim or have legitimacy, and the limits are considered to be something that needs to be done. Regulations for blocking dangerous content in electronic communications networks are currently spread across other laws and regulations. Restrictions on prohibited information or content have even emerged before the digital era, which can be seen from several prohibitions on disseminating certain information in the Criminal Code. Blocking dangerous content in electronic communications networks in the future will involve efforts to secure information systems so that cybercrime prevention, especially regarding dangerous content, can be prevented through technological channels or techno prevention. Examining regulations and policies in the Netherlands, the USA, and Singapore, they already have regulations and policy directions for blocking dangerous content, or at least regulations regarding law enforcement for cybercrime. The difference is in the level of sensitivity to the specifications of existing problems. Blocking harmful content with special arrangements outside the Criminal Code must be carried out non-repressively so that it does not become over-criminalized. Handling criminal acts related to freedom of expression in digital media can be carried out through preventive efforts with cyber patrols carried out by the Police. The policy model is based on the formulation stage of all crime prevention plans using the criminal law system, which pays attention to the problem of formulating criminal acts (criminalization), criminal responsibility, and criminal regulations and punishment.

References

Aditya, Zaka Firma, and Sholahuddin Al-Fatih, 'Indonesian Constitutional Rights: Expressing and Purposing Opinions on the Internet', *International Journal of Human Rights*, 0.0 (2020), 1–25 https://doi.org/10.1080/13642987.2020.1826450

Agrafiotis, Ioannis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton, 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks

and Understanding How They Propagate', *Journal of Cybersecurity*, 4.1 (2018) https://doi.org/10.1093/cybsec/tyy006

Ahdanisa, Dissa Syakina, and Steven B. Rothman, 'Revisiting International Human Rights Treaties: Comparing Asian and Western Efforts to Improve Human Rights', *SN Social Sciences*, 1.1 (2021), 16 https://doi.org/10.1007/s43545-020-00018-0

Akdeniz, Yaman, 'To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression', *Computer Law & Security Review*, 26.3 (2010), 260–72 https://doi.org/10.1016/j.clsr.2010.03.004

Aytac, Ugur, 'Digital Domination: Social Media and Contestatory Democracy', *Political Studies*, 72.1 (2024), 6–25 https://doi.org/10.1177/00323217221096564

Barnidge, Matthew, 'The Role of News in Promoting Political Disagreement on Social Media', *Computers in Human Behavior*, 52 (2015), 211–18 https://doi.org/10.1016/j.chb.2015.06.011

Castaño-Pulgarín, Sergio Andrés, Natalia Suárez-Betancur, Luz Magnolia Tilano Vega, and Harvey Mauricio Herrera López, 'Internet, Social Media and Online Hate Speech. Systematic Review', *Aggression and Violent Behavior*, 58 (2021), 101608 https://doi.org/10.1016/j.avb.2021.101608

Common, Mackenzie F., 'Beyond the Usual Suspects: A Taxonomy of Social Media Regulations in Countries with Human Rights Issues', *International Review of Law, Computers & Technology*, 37.1 (2023), 1–28 https://doi.org/10.1080/13600869.2022.2043093

Curtis, Joanna, and Gavin Oxburgh, 'Understanding Cybercrime in "Real World" Policing and Law Enforcement', *The Police Journal: Theory, Practice and Principles*, 96.4 (2023), 573–92 https://doi.org/10.1177/0032258X221107584

Dhawan, S.M., B.M. Gupta, and B. Elango, 'Global Cyber Security Research Output (1998–2019): A Scientometric Analysis', *Science & Technology Libraries*, 40.2 (2021), 172–89 https://doi.org/10.1080/0194262X.2020.1840487

Donalds, Charlette, and Kweku-Muata Osei-Bryson, 'Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach', *Computers in Human Behavior*, 92 (2019), 403–18 https://doi.org/10.1016/j.chb.2018.11.039

Dunn Cavelty, Myriam, 'Cybersecurity Research Meets Science and Technology Studies', *Politics and Governance*, 6.2 (2018), 22–30 https://doi.org/10.17645/pag.v6i2.1385

Dupont, Benoit, 'Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime', *Crime, Law and Social Change*, 67.1 (2017), 97–116

https://doi.org/10.1007/s10611-016-9649-z

Dupont, Benoît, and Chad Whelan, 'Enhancing Relationships between Criminology and Cybersecurity', *Journal of Criminology*, 54.1 (2021), 76–92 https://doi.org/10.1177/00048658211003925

Eftedal, Nikolai Haahjem, and Lotte Thomsen, 'Motivated Moral Judgments about Freedom of Speech Are Constrained by a Need to Maintain Consistency', *Cognition*, 211 (2021), 104623 https://doi.org/10.1016/j.cognition.2021.104623

Gallant, Kenneth S., *The Principle of Legality in International and Comparative Criminal Law* (Cambridge University Press, 2008) https://doi.org/10.1017/CBO9780511551826

Gambäck, Björn, and Utpal Kumar Sikdar, 'Using Convolutional Neural Networks to Classify Hate-Speech', in *Proceedings of the First Workshop on Abusive Language Online* (Stroudsburg, PA, USA: Association for Computational Linguistics, 2017), pp. 85–90 https://doi.org/10.18653/v1/W17-3013

Gordon, Sarah, and Richard Ford, 'On the Definition and Classification of Cybercrime', *Journal in Computer Virology*, 2.1 (2006), 13–20 https://doi.org/10.1007/s11416-006-0015-z

Hatano, Ayako, 'Regulating Online Hate Speech through the Prism of Human Rights Law: The Potential of Localised Content Moderation', *The Australian Year Book of International Law Online*, 41.1 (2023), 127–56 https://doi.org/10.1163/26660229-04101017

Holbig, Heike, 'Be Water, My Friend: Hong Kong's 2019 Anti-Extradition Protests', *International Journal of Sociology*, 50.4 (2020), 325–37 https://doi.org/10.1080/00207659.2020.1802556

Hunter, Lance Y., 'Social Media, Disinformation, and Democracy: How Different Types of Social Media Usage Affect Democracy Cross-Nationally', *Democratization*, 30.6 (2023), 1040–72 https://doi.org/10.1080/13510347.2023.2208355

Jaishankar, K., ed., *Cyber Criminology* (Routledge, 2011) https://doi.org/10.1201/b10718

Jørgensen, Rikke Frank, ed., *Human Rights in the Age of Platforms* (The MIT Press, 2019) https://doi.org/10.7551/mitpress/11304.001.0001

Karin, Alfina Faradisa, Moch. Syafrudin Dwi Sapto Laxamanahady, and Muhamad Alief Hidayat, 'The Right to Freedom of Expression in the Digital Age', in *Proceedings of the International Conference for Democracy and National Resilience 2022 (ICDNR 2022)* (Paris: Atlantis Press SARL, 2023), pp. 47–54 https://doi.org/10.2991/978-2-494069-75-6_8

Kim, Yonghwan, Shih-Hsien Hsu, and Homero Gil de Zúñiga, 'Influence of Social Media Use on Discussion Network Heterogeneity and Civic Engagement: The Moderating Role of Personality Traits', *Journal of Communication*, 63.3 (2013), 498–516 https://doi.org/10.1111/jcom.12034

Kocyigit, Emre, Mehmet Korkmaz, Ozgur Koray Sahingoz, and Banu Diri, 'Real-Time Content-Based Cyber Threat Detection with Machine Learning', 2021, pp. 1394–1403 https://doi.org/10.1007/978-3-030-71187-0_129

Lee, Youngjae, 'Proxy Crimes and Overcriminalization', *SSRN Electronic Journal*, 2022 https://doi.org/10.2139/ssrn.4051022

Leukfeldt, E. Rutger, Anita Lavorgna, and Edward R. Kleemans, 'Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime', *European Journal on Criminal Policy and Research*, 23.3 (2017), 287–300 https://doi.org/10.1007/s10610-016-9332-z

Lubin, Asaf mname, 'Cyber Law and Espionage Law as Communicating Vessels', *SSRN Electronic Journal*, 2018 https://doi.org/10.2139/ssrn.3099769

Lusthaus, Jonathan, Edward Kleemans, Rutger Leukfeldt, Michael Levi, and Thomas Holt, 'Cybercriminal Networks in the UK and Beyond: Network Structure, Criminal Cooperation and External Interactions', *Trends in Organized Crime*, 2023 https://doi.org/10.1007/s12117-022-09476-9

Maimon, David, and Eric R. Louderback, 'Cyber-Dependent Crimes: An Interdisciplinary Review', *Annual Review of Criminology*, 2.1 (2019), 191–216 https://doi.org/10.1146/annurev-criminol-032317-092057

Miró Llinares, Fernando, and Ana B. Gómez Bellvís, 'Freedom Of Expression In Social Media And Criminalization Of Hate Speech In Spain: Evolution, Impact And Empirical Analysis Of Normative Compliance And Self-Censorship', *Spanish Journal of Legislative Studies*, 1, 2019 https://doi.org/10.21134/sjls.v0i1.1837

Nave, Eva, and Lottie Lane, 'Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service?', *Computer Law & Security Review*, 51 (2023), 105884 https://doi.org/10.1016/j.clsr.2023.105884

Plotnek, Jordan J., and Jill Slay, 'Cyber Terrorism: A Homogenized Taxonomy and Definition', *Computers & Security*, 102 (2021), 102145 https://doi.org/10.1016/j.cose.2020.102145

Rizky Pratama Putra Karo Karo, 'Hate Speech: Penyimpangan Terhadap UU ITE, Kebebasan Berpendapat Dan Nilai-Nilai Keadilan Bermartabat', *Jurnal Lemhannas RI*, 10.4 (2023), 52–65 https://doi.org/10.55960/jlri.v10i4.370

Ryberg, Jesper, 'Punishment and Political Philosophy', in *Oxford Research Encyclopedia of Politics* (Oxford University Press, 2016) https://doi.org/10.1093/acrefore/9780190228637.013.200

Sander, Barrie, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law', *European Journal of International Law*, 32.1 (2021), 159–93 https://doi.org/10.1093/ejil/chab022

Schafers, C., and J. Stephen Wormith, 'Criminality', in *Encyclopedia of Mental Health* (Elsevier, 2023), pp. 526–37 https://doi.org/10.1016/B978-0-323-91497-0.00161-2

Siyuan, Chen, 'Regulating Online Hate Speech: The Singapore Experiment', *International Review of Law, Computers & Technology*, 2023, 1–21 https://doi.org/10.1080/13600869.2023.2295091

Spitzberg, Brian H., and Gregory Hoobler, 'Cyberstalking and the Technologies of Interpersonal Terrorism', *New Media & Society*, 4.1 (2002), 71–92 https://doi.org/10.1177/14614440222226271

Sule, Mary-Jane, Marco Zennaro, and Godwin Thomas, 'Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends', *Technology in Society*, 67 (2021), 101734 https://doi.org/10.1016/j.techsoc.2021.101734

Suominen, Annika Elisabet, 'What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?', *Bergen Journal of Criminal Law & Criminal Justice*, 2.1 (2014), 1 https://doi.org/10.15845/bjclcj.v2i1.615

Szczucki, Krzysztof, 'Ethical Legitimacy of Criminal Law', *International Journal of Law, Crime and Justice*, 53 (2018), 67–76 https://doi.org/10.1016/j.ijlcj.2018.03.002

Toni Harmanto, Bagus Oktafian Abrianto, and Xavier Nugraha, 'Penal Mediation By Police Institution In Handling Hate Speech Through Electronic Media: A Legal Efforts To Resolve with A Restorative Justice Approach', *International Journal Of Artificial Intelligence Research*, 6.1.2 (2022) https://doi.org/10.29099/ijair.v6i1.388

Wildana, Faiq, 'An Explorative Study on Social Media Blocking in Indonesia', *The Journal of Society and Media*, 5.2 (2021), 456–84 https://doi.org/10.26740/jsm.v5n2.p456-484

Yang, JungHwan, Matthew Barnidge, and Hernando Rojas, 'The Politics of "Unfriending": User Filtration in Response to Political Disagreement on Social Media', *Computers in Human Behavior*, 70 (2017), 22–29 https://doi.org/10.1016/j.chb.2016.12.079