

**ARTICLE 19**

Legal Analysis

**Indonesia: Regulation of the Minister of  
Communication and Informatics Number 5  
of 2020 on Private Electronic System  
Operators (Ministerial Regulation 5)**

September 2021

## ARTICLE 19

**E:** info@article19.org

**W:** www.article19.org

**Tw:** @article19org

**Fb:** facebook.com/article19org

First published by ARTICLE 19 in September 2021

Text and analysis Copyright ARTICLE 19, 2021 (Creative Commons License 3.0)

### © ARTICLE 19, 2021

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by power-holders for transparency good governance and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

About Creative Commons License 3.0: This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 license. You are free to copy, distribute and display this work and to make derivative works, provided you: 1) give credit to ARTICLE 19; 2) do not use this work for commercial purposes; 3) distribute any works derived from this publication under a license identical to this one. To access the full legal text of this license, please visit: <http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode>

## Executive Summary

In this analysis, ARTICLE 19 reviews the **Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators** (hereinafter ‘Ministerial Regulation 5’ or ‘the Regulation’), issued on 24 November 2020, for its compliance with international freedom of expression standards.

Ministerial Regulation 5 governs the functioning of private electronic systems operators (ESOs) accessible in Indonesia which include social media platforms, search engines, ecommerce platforms, games, and communications services. Ministerial Regulation 5 will affect Indonesian services and platforms as well as multinational companies such as Facebook, Twitter, Google, TikTok, and others.

The Regulation, promulgated in November 2020, despite concerns from civil society, grants the government overbroad authority to regulate Private ESO activity, gives authorities access to user data, and provides for sweeping notice and takedown orders. Ministerial Regulation 5 governs both local and international ESOs, requiring registration and designation of contact person(s) in Indonesia, who may be at risk of arbitrary reprisal for failure to comply with overbroad requests. It also introduces excessive penalties for non-compliance, from fines to full shutdown of services in Indonesia.

ARTICLE 19 highlights the following concerns regarding Ministerial Regulation 5:

- It includes overbroad and vague definitions;
- It requires data localisation;
- It grants authorities data access without adequate procedural safeguards;
- It introduces sweeping notice and takedown orders;
- It includes excessive penalties for failure to comply.

ARTICLE 19 calls on the Indonesian government to immediately revoke Ministerial Regulation 5.

# Contents

---

Introduction	5
International human rights standards	7
The protection of freedom of expression under international law	7
Limitations on the right to freedom of expression	7
Intermediary liability	8
Anonymity, encryption, and right to privacy	8
<hr/>	
Protection of human rights in domestic law	10
1945 Constitution of the Republic of Indonesia	10
Law No. 39 of 1999 (the Human Rights Law)	10
<hr/>	
Analysis of Ministerial Regulation 5	11
Overbroad scope	11
Prohibited content	11
Intermediary obligations and liability	12
Access to user data	13
Local Contact Person(s)	14
Excessive penalties for failure to comply	14
<hr/>	
About ARTICLE 19	16

## Introduction

On 24 November 2020, the Ministry of Communication and Information Technology of the Republic of Indonesia (hereinafter 'KOMINFO' or 'the Ministry') issued **Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators** (hereinafter 'Ministerial Regulation 5' or 'the Regulation'). This came about despite civil society objection. Initially, electronic systems operators were to register under the law by 24 May 2021 or be blocked in Indonesia. However, on 24 May the Ministry announced a six-month postponement until a national Single Sign-On (SSO) system is ready for implementation.

Ministerial Regulation 5 governs the functioning of 'Private Electronic Systems Operators' (Private ESOs) providing online services that are accessible in Indonesia. These include social media platforms, search engines, ecommerce platforms, games, and communications services. The Regulation will affect Indonesian services and platforms as well as multinational companies such as Facebook, Twitter, Google, and others.

Ministerial Regulation 5 is the latest addition to the legal arsenal used by the Indonesian government to crack down on freedom of expression. The most significant threat to freedom of expression online comes from the Electronic Information and Transactions Law (ITE Law), the main instrument for the regulation of online content, often used together with the Penal Code.<sup>1</sup> The Regulation also adds to a growing list of human rights concerns in Indonesia, which include threats to digital rights,<sup>2</sup> ongoing violence and extrajudicial killings in West Papua, and the targeting of civil society organisations and media groups. Lawyers and other human rights defenders have faced judicial harassment for their social media posts related to human rights abuses in Papua and West Papua.<sup>3</sup> With greater restrictions on online content, the targeting of social media users commenting on sensitive human rights issues is likely to increase.

Indonesia scored 48 out of 100 in the Freedom House Freedom on the Net 2021 report, a 'partly free' ranking.<sup>4</sup> Freedom House noted 'increased online harassment, as well as technical attacks against journalists, activists, and online news outlets further this environment of caution.'

Across the country, Indonesians have been imprisoned in response to exercising their rights to the freedom of expression or assembly. In its 2020 annual report, Amnesty International stated that 'unidentified parties digitally intimidated academics, students, activists, human rights defenders, social justice leaders and journalists, trying to silence their critical voices.'<sup>5</sup> As the COVID-19 pandemic raged through the country, authorities targeted individuals who discussed the official response, with police monitoring online platforms and taking action against 'hoax spreaders' and those accused of insulting the President and his administration.<sup>6</sup>

Widespread censorship has been reported.<sup>7</sup> This includes the blocking of lesbian, gay, bisexual, transgender, queer, and intersex (LGBTQI) websites, criticism of Islam, pornography, and other material deemed immoral.<sup>8</sup> Censors have targeted social media platforms, streaming media services, and other communications services, including at times YouTube, Netflix, Tumblr, and TikTok. In 2019, YouTube removed a satirical video about West Papua after receiving a complaint from the government.<sup>9</sup>

Content restriction and filtering has been on the rise in Indonesia, especially since KOMINFO slammed social media platforms for not filtering enough in 2019.<sup>10</sup> From January to June 2020, according to Facebook's transparency report, content restrictions based on local laws reached a three-year high, with 630 pieces of content blocked by Facebook in response to government requests.<sup>11</sup> In 2018, the Ministry submitted 8,903

---

<sup>1</sup> ARTICLE 19, [Navigating Indonesia's Information Highway](#), March 2013.

<sup>2</sup> SAFEnet, [Indonesia Digital Rights Situation Report 2019: The Rise of Digital Authoritarianism](#), July 2020; Association for Progressive Communication, [Uns#ackling expression Indonesia](#), November 2020.

<sup>3</sup> [Indonesian rights lawyer named suspect after sharing posts on Papua](#), *Reuters*, 4 September 2019; [Indonesian filmmaker named suspect after sharing posts on Papua](#), *Reuters*, 27 September 2019.

<sup>4</sup> Freedom House, [Freedom on the Net 2021](#).

<sup>5</sup> Amnesty International, [Indonesia 2020](#).

<sup>6</sup> *Ibid.*

<sup>7</sup> Open Observatory of Network Interference (OONI), [The State of Internet Censorship in Indonesia](#), 23 May 2017.

<sup>8</sup> Freedom on the Net 2020, *op.cit.*

<sup>9</sup> [Govt gets YouTube to block satirical West Papua 'advertisement'](#), *The Jakarta Post*, 29 August 2019.

<sup>10</sup> [Indonesia slams Facebook, Instagram for 'sluggish' efforts in filtering content](#), *The Jakarta Post*, 1 March 2019.

<sup>11</sup> Facebook, [Transparency Report for Indonesia](#).

requests for content removal to Facebook and Instagram, compared to 2,232 in 2017.<sup>12</sup> The Ministry has also demanded the removal of certain apps from app stores in Indonesia. According to Freedom House, in January 2020 the Ministry announced that it had ordered the removal of 1,085 FinTech apps and 1,356 other apps from the Google Play Store in 2019.<sup>13</sup>

Indonesia has also employed internet throttling and shutdowns and has ordered the blocking of social media platforms during periods of political unrest. In May 2019, the Indonesian government imposed social media restrictions during demonstrations around the national election.<sup>14</sup> Also in 2019, the Indonesian government ordered three internet shutdowns in Papua and West Papua.<sup>15</sup> In response, in December 2019, Indonesian human rights organisations the Alliance of Independent Journalists (AIJ) and Southeast Asia Freedom of Expression Network (SAFEnet) filed a lawsuit against KOMINFO challenging the use of internet throttling and shutdowns.<sup>16</sup> In June 2020, the Jakarta State Administrative Court ruled that the government's intentional internet shutdowns in 2019 had been illegal.<sup>17</sup>

In light of the above concerns, ARTICLE 19 finds that rather than addressing restrictions on freedom of expression and access to information online, Ministerial Regulation 5 will exacerbate existing freedom of expression challenges and introduce more severe restrictions on internet freedom. On 28 May 2021, a coalition of 25 Indonesian and international human rights organisations sent an open letter to Indonesia's Minister of Communication and Information Technology to express concerns about the Regulation's impact on the rights to freedom of expression and privacy.<sup>18</sup> This analysis elaborates on these concerns in greater detail and provides arguments as to why it fails to meet relevant human rights standards.

ARTICLE 19 calls on the Indonesian government to immediately revoke Ministerial Regulation 5.

---

<sup>12</sup> *The Jakarta Post*, 1 March 2019, *op.cit.*

<sup>13</sup> Freedom on the Net 2020, *op.cit.*

<sup>14</sup> [Indonesia curbs social media, blaming hoaxes for inflaming unrest](#), *Reuters*, 22 May 2019.

<sup>15</sup> SAFEnet, [The Rise of Internet Shutdown in Southeast Asia](#), 31 July 2020.

<sup>16</sup> [Civil society groups will face government in court over Papuan internet blackout](#), *The Jakarta Post*, 3 December 2019; Access Now, [Indonesians seek justice after internet shutdown](#), 13 May 2020.

<sup>17</sup> Access Now, [Court rules the internet shutdowns in Papua and West Papua were illegal](#), 3 June 2020; SAFEnet, [We Won The Case!](#), 4 June 2020.

<sup>18</sup> ARTICLE 19, [Indonesia: Repeal Ministerial Regulation 5 to protect digital rights](#), 31 May 2021.

## International human rights standards

### The protection of freedom of expression under international law

The right to freedom of expression is enshrined in Article 19 of the **Universal Declaration of Human Rights (UDHR)**<sup>19</sup> and Article 19 of the **International Covenant on Civil and Political Rights (ICCPR)**.<sup>20</sup>

Indonesia became a State Party to the ICCPR on 23 February 2006, and as such is obligated to ensure its laws, policies, and practices regarding the freedom of expression and access to information comply with Article 19 of the ICCPR. Article 7 of the 1999 Human Rights Law of Indonesia likewise states that ‘provisions set forth in international law concerning human rights ratified by the Republic of Indonesia, are recognised under this Act as legally binding in Indonesia.’<sup>21</sup>

**General Comment No. 34**,<sup>22</sup> adopted by the UN Human Rights Committee in September 2011, recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.<sup>23</sup>

The UN Human Rights Council (HRC) affirmed in 2018 that the ‘same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice.’<sup>24</sup>

In a 2019 **Joint Declaration on challenges to Freedom of Expression in the Next Decade**, the four special mandate holders on the right to freedom of expression reiterated that ‘the exercise of freedom of expression requires a digital infrastructure that is robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders.’ They called on States to ‘recognise the right to access and use the Internet as a human right as an essential condition for the exercise of the right to freedom of expression,’ ‘refrain from imposing Internet or telecommunications network disruptions and shutdowns,’ and ‘avoid measures that risk fragmenting the Internet and limiting access to the global Internet.’<sup>25</sup>

### Limitations on the right to freedom of expression

While the right to freedom of expression and access to information is a fundamental right, it is not absolute. Under strict circumstances, States may limit the right to freedom of expression but restrictions must be:

- **Provided for by law:** Any restriction must be formulated with sufficient precision so that any individual may regulate their conduct accordingly.<sup>26</sup> Vague or overbroad restrictions are never permissible.
- **In pursuit of a legitimate aim:** Legitimate aims for restricting the freedom of expression are expressed in Article 19(3)(a) and (b) of the ICCPR. Restrictions shall only be permitted for (a) respect of the rights or reputation of others and (b) the protection of national security or of public order (*ordre public*), or of public health or morals.
- **Necessary and proportionate:** Restrictions must have a direct and immediate connection between the expression and the protected interest. Proportionality requires that restrictions are not overbroad. They must be appropriate to achieve a protective function. The restriction must be specific, tailored, and the least intrusive means capable of achieving the same limited result.<sup>27</sup>

<sup>19</sup> UN General Assembly Resolution 217A(III), adopted 10 December 1948.

<sup>20</sup> UN General Assembly Resolution 2200A (XXI), adopted 16 December 1966, entry into force 23 March 1976.

<sup>21</sup> Indonesia: Law No. 39 of 1999 on Human Rights [Indonesia], 23 September 1999, available at: <https://www.refworld.org/docid/4da2ce862.html>

<sup>22</sup> Human Rights Committee, **General Comment No. 34**, CCPR/C/GC/34, adopted on 12 September 2011.

<sup>23</sup> *Ibid.*, para. 12.

<sup>24</sup> UN Human Rights Council (HRC), **The promotion, protection and enjoyment of human rights on the Internet**, A/HRC/38/L.10/Rev.1, July 2018.

<sup>25</sup> UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, **Joint Declaration on challenges to Freedom of Expression in the Next Decade**, 10 July 2019.

<sup>26</sup> UN Human Rights Committee, *L.J.M de Groot v. The Netherlands*, No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).

<sup>27</sup> UN Human Rights Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

In a 2011 **Joint Declaration on Freedom of Expression and the Internet**, the four special mandate holders on the right to freedom of expression noted that ‘restrictions on freedom of expression on the internet are only acceptable if they comply with established international standards.’<sup>28</sup> The UN Human Rights Committee has also made clear that limitations on electronic forms of communication or expression disseminated over the internet must be justified according to the same criteria as ‘offline’ communications, as set out above.<sup>29</sup>

## Intermediary liability

In their 2011 Joint Declaration, the Special Rapporteurs stated, ‘no one who simply provides technical internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services.’ They continued that ‘intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression.’<sup>30</sup>

In his June 2016 report to the HRC,<sup>31</sup> the UN Special Rapporteur on Freedom of Opinion and Expression encouraged States not to impose policies that would pressure businesses to interfere with freedom of expression unnecessarily or disproportionately. He further recognised that ‘private intermediaries are typically ill-equipped to make determinations of content illegality,’<sup>32</sup> and reiterated criticism of notice and takedown frameworks for ‘incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation,’ i.e., the danger of ‘self- or over-removal.’<sup>33</sup>

The Manila Principles on Intermediary Liability, furthermore, introduces a framework to assess laws, policies, and practices that govern liability of intermediaries for third-party content, which states:

*Intermediaries should be shielded from liability for third-party content. Content must not be required to be restricted without an order by a judicial authority. Requests for restrictions of content must be clear, be unambiguous, and follow due process. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality. Laws and content restriction policies and practices must respect due process. Transparency and accountability must be built into laws and content restriction policies and practices.*<sup>34</sup>

## Anonymity, encryption, and right to privacy

The protection of anonymity is vital to the enjoyment of the right to freedom of expression, the right privacy, and other human rights. A fundamental feature enabling anonymity online is encryption.<sup>35</sup>

In May 2015, the UN Special Rapporteur on Freedom of Opinion and Expression, David Kaye, published his report on encryption and anonymity in the digital age.<sup>36</sup> The report highlighted the following issues:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the right to freedom of expression and opinion in the digital age;<sup>37</sup>
- Attempts to ban or intercept anonymous communications during protests is an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.<sup>38</sup> Legislation and regulations

<sup>28</sup> [The Joint Declaration on Freedom of Expression and the Internet](#), 2011, issued by UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information.

<sup>29</sup> General Comment No. 34, *op.cit.*, paras. 12, 39, and 43.

<sup>30</sup> 2011 Joint Declaration on Freedom of Expression and the Internet, *op.cit.*

<sup>31</sup> HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (SR on FoE), [A/HRC/32/38](#), 11 May 2016, paras. 40–44.

<sup>32</sup> *Ibid.*

<sup>33</sup> *Ibid.*, para. 43.

<sup>34</sup> [Manilla Principles on Intermediary Liability](#).

<sup>35</sup> Encryption is a mathematical ‘process of converting messages, information, or data into a form unreadable by anyone except the intended recipient’ that protects the confidentiality of content against third-party access or manipulation; see for example, SANS Institute, [History of encryption](#), 8 August 2001.

<sup>36</sup> HRC, Report of the SR on FoE, [A/HRC/29/32](#), 22 May 2015.

<sup>37</sup> *Ibid.*, paras. 12, 16 and 56.

<sup>38</sup> *Ibid.*, para. 53.

protecting human rights defenders and journalists should include provisions that allow for technologies that would secure their communications;

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.<sup>39</sup> Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.<sup>40</sup>

The Special Rapporteur's report also addressed mandatory 'key disclosure' and 'decryption orders' from law enforcement. The Special Rapporteur noted that targeted decryption orders 'may be seen as more limited and less likely to raise proportionality concerns,' whereas key disclosure would expose an individual's 'private data well beyond what is required by the exigencies of a situation.' This is because the decryption key would grant authorities access to the individual's entire set of encrypted communication.<sup>41</sup>

In his 2018 Encryption and Anonymity follow-up research paper, the Special Rapporteur reiterated that, 'court-ordered decryption should only be permitted on a case-by-case basis applied to individuals pursuant to 'transparent and publicly accessible' legal criteria that meet the requirements of Article 19(3) and are subject to prior judicial authorisation and associated due process safeguards.'<sup>42</sup>

Article 12 of the UDHR and Article 17 of the ICCPR establish the right to privacy. The ICCPR holds that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence,' and that 'everyone has the right to the protection of the law against such interference or attacks.'<sup>43</sup>

The UN Human Rights Committee, in its General Comment No. 16 on the Right to Privacy, holds that 'even with regard to interferences that conform to [the ICCPR], relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.'<sup>44</sup>

In the 2018 'Right to privacy in the digital age' report, presented to the HRC, the High Commissioner for Human Rights recommended all States adopt strong and comprehensive privacy legislation, including on data privacy, in accordance with international human rights law covering safeguards, oversight, and remedy.<sup>45</sup>

---

<sup>39</sup> *Ibid.*, para. 56.

<sup>40</sup> *Ibid.*, paras. 31–35.

<sup>41</sup> *Ibid.*, para. 45.

<sup>42</sup> Mandate of the SR on FoE, [Research Paper, Encryption and Anonymity follow-up report](#), June 2018.

<sup>43</sup> ICCPR Article 17

<sup>44</sup> UN Human Rights Committee, [General Comment No. 16: Article 17 \(Right to Privacy\)](#), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

<sup>45</sup> HRC, Report of the UN High Commissioner for Human Rights, [A/HRC/39/29](#), 3 August 2018.

## Protection of human rights in domestic law

### 1945 Constitution of the Republic of Indonesia

The Constitution of Indonesia has been amended four times, in 1999, 2000, 2001, and finally 2002. Chapter XA, Articles 28a through 28j, enumerates a number of human rights protections.

The right to freedom of expression and access to information in particular is guaranteed in Article 28f of the Constitution: 'Every person shall have the right to communicate and to obtain information for the purpose of the development of his/her self and social environment, and shall have the right to seek, obtain, possess, store, process and convey information by employing all available types of channels.'<sup>46</sup> While the Constitution in Article 28j allows for restrictions 'established by law... based upon considerations of morality, religious values, security and public order in a democratic society,' any such restrictions still must comply with the three-part test noted above.

A right to privacy is not explicitly laid out in the Constitution but the Constitutional Court in *Anggara v Kominfo*<sup>47</sup> found that the Constitution implies a right to privacy at Article 28g: 'Every person shall have the right to protection of his/herself, family, honour, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right.'<sup>48</sup>

### Law No. 39 of 1999 (the Human Rights Law)

In addition to incorporating Indonesia's international human rights law obligations in Article 7, noted above, the 1999 Human Rights Law enumerates a number of protections for the right to freedom of opinion, expression, and access to information:

- 'Everyone has the right to communicate and obtain information they need to develop themselves as individuals and to develop their social environment. Everyone has the right to seek, obtain, own, store, process, and impart information using all available facilities,' Article 14(1-2).
- 'Everyone has the freedom to hold, impart and widely disseminate his beliefs, orally or in writing through printed or electronic media,' Article 23(2).
- 'Everyone has the right to peaceful assembly and association,' Article 24(1).
- 'Every citizen has the right to express his opinion in public, and this includes the right to strike, according to prevailing law,' Article 25.

And the right to privacy:

- 'Everyone has the right to integrity of the individual, both spiritual and physical, and as such shall not become the object of any research without his approval, Article 21.
- 'Everyone has the right to protection of the individual, his family, opinion, honour, dignity, and rights, Article 29.
- 'Everyone has the right to security and protection against the threat of fear from any act or omission,' Article 30.
- 'No one shall be subject to arbitrary interference with his home,' Article 31.
- 'No one shall be subject to arbitrary interference with his correspondence, including electronic communications, except upon the order of a court or other legitimate authority according to prevailing legislation,' Article 32.<sup>49</sup>

<sup>46</sup> [The 1945 Constitution of the Republic of Indonesia](#), as amended by the First Amendment of 1999, the Second Amendment of 2000, the Third Amendment of 2001 and the Fourth Amendment of 2002 Unofficial translation.

<sup>47</sup> Graham Greeneaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, Oxford University Press, 2017, p. 379-380.

<sup>48</sup> Constitution of the Republic of Indonesia, Article 28f.

<sup>49</sup> [Indonesia: Law No. 39 of 1999 on Human Rights \[Indonesia\]](#), 23 September 1999.

## Analysis of Ministerial Regulation 5

### Overbroad scope

Ministerial Regulation 5 governs the provision of a broad range of digital services by Private ESOs. Private ESOs are broadly defined as ‘any individual, business entity, or community’ that operates an ‘Electronic System’ involved in the ‘preparing, collecting, processing, analysing, saving, displaying, announcing, sharing and/or distributing’ of electronic information (Article 1(4) and (6)). Individuals and companies connected to websites, social media platforms, email services, search engines, messaging services, mobile applications, and nearly any other online service or application fall within the scope of the definition. As such, the Regulation extends the government’s regulatory powers to virtually any actor engaged in any online activity.

All Private ESOs are required to register with and obtain a registration certificate from the Minister of Communication and Information Technology before providing their services in Indonesia (Article 2). Those who do not register risk being blocked in Indonesia (Article 7), to the detriment of Indonesian citizens’ right to freedom of expression and access to information. The public is also permitted to submit complaints against Private ESOs who fail to register (Article 2(5)). As noted above, the original deadline for registration was May 2021 but this has been postponed until later in 2021.

The registration process requires Private ESOs to provide KOMINFO with information on the location of data management, processing, and storage and to guarantee and implement the requirement to provide access to their electronic systems and data in support of law enforcement and oversight efforts (Article 3(4)).

Registration requirements extend also to foreign companies or individuals if they provide services in Indonesia. The registration process for foreign Private ESOs requires providing the identity of the company’s chairman, information about residence or certificate of incorporation, the total number of users in Indonesia, and the value of its transactions in Indonesia (Article 4(2)).

ARTICLE 19 notes that under international human rights law, registration requirements constitute an interference with the right to freedom of expression. As such, they must be justified under the three-part test, i.e. be provided by law, in pursuit of a legitimate aim, and necessary and proportionate to that aim. In their 2011 Joint Declaration on Freedom of Expression and the Internet, the special mandates on freedom of expression stated that ‘Approaches to regulation developed for other means of communication – such as telephony or broadcasting – cannot simply be transferred to the Internet but, rather, need to be specifically designed for it.’<sup>50</sup>

More recently, the UN Special Rapporteur on Freedom of Opinion and Expression has noted that ‘smart’ regulation of platforms may be compatible with human rights if it is carefully defined, focuses on transparency and due process obligations, and falls under the supervision of an independent regulator whose powers should be carefully circumscribed.<sup>51</sup> This is plainly not the case with the registration requirement in Ministerial Regulation 5, which provides unrestricted access to user data in breach of international standards on privacy and can be enforced by blocking the entire service. These requirements are unjustified, unnecessary, and disproportionate.

### Prohibited content

Ministerial Regulation 5 requires Private ESOs to ensure that their ‘electronic systems’ do not contain prohibited electronic information or documents or facilitate the spreading of such prohibited content (Article 9(3)).

Article 9(4) defines prohibited information or documents as content that violates Indonesian law, ‘disturbs the community and public order,’ or ‘informs others how to access or provides access to’ prohibited content. Article 9(5) gives the government sole authority to determine what constitutes a disturbance to community and public order.

---

<sup>50</sup> The 2011 Joint Declaration on Freedom of Expression and the Internet, *op. cit.*

<sup>51</sup> HRC, Report of the SR on FoE, [A/HRC/38/35](#), 6 April 2018.

ARTICLE 19 finds that the overly broad definition of prohibited content stipulated by Article 9 does not provide the clarity necessary to allow Private ESOs to regulate their conduct in line with the law. The prohibition of content that may ‘disturb the community or public order’ implicates an extremely broad and poorly defined category of communication, including expression that is protected by international human rights law. Article 9(5) provides excessive discretion to authorities to interpret this vague terminology, increasing this risk of abusive application of the law and breaching the legality requirement under international human rights law.

Moreover, the general reference to content that violates Indonesian law, which here means any legal statute and not only activity covered under Ministerial Regulation 5, is extremely overbroad given the myriad different laws that could be relevant. This level of breadth makes it all the more difficult for an individual to regulate their conduct accordingly under the law, as required by the three-part test regarding restrictions on the freedom of expression. Even laws that are incompatible with international freedom of expression standards,<sup>52</sup> list the particular offences that fall within the scope of the law. Indonesian substantive law raises significant issues in its own right. In particular, free speech offences are generally overly broad and in breach of international human rights law.

Ministerial Regulation 5 imposes an ‘obligation of result’ by requiring that all prohibited content be blocked or removed by Private ESOs. As such, it strongly incentivises pervasive monitoring of online communications. In practice, Private ESOs will not be able to comply with the law without using automated filters, raising the risk of false negatives and false positives and the removal of content that does not violate the law. In addition, proactive monitoring by tech companies raises serious privacy concerns since it generally involves the use of privacy-invasive technology to identify ‘illegal’ content.

Finally, Article 9(4)(c) appears to ban access to circumvention tools such as virtual private networks (VPNs) despite the fact that these tools can be used for perfectly legitimate reasons, including to protect the right to privacy. As noted above, the UN Special Rapporteur on the Freedom of Opinion and Expression has stressed the importance of circumvention tools and encryption to exercise the right to seek, receive and impart information and emphasised that any restrictions on their use must meet the requirements of legality, necessity, proportionality, and legitimacy.

In summary, Articles 9(3) and (4) are overly broad in breach of the legality requirement under international human rights law. This is even more concerning given that failure to comply with these vague obligations can lead to disproportionate sanctions, including blocking of entire services, applications, etc. as explained in more detail below.

## Intermediary obligations and liability

Articles 10 and 11 establish obligations for Private ESOs concerning the removal of prohibited content in a way that does not comply with international standards concerning intermediary liability.

The proposed scheme contains some limited positive aspects, including the obligation for Private ESOs hosting user-generated content services to have a complaints mechanism in place in order to deal with requests to remove content, an obligation to respond to such complaints and notify users whose content is the target of a complaint, and a duty to set out users’ rights and obligations (Article 10(1) to (4)).

At the same time, the obligations imposed on Private ESOs are inconsistent with international standards on freedom of expression and due process online. These provisions delegate the responsibility for deciding the legality of content to private hosting services. Moreover, companies are required to interpret and apply broad content restrictions on their own rather than merely comply with court orders. Article 11(b) requires Private ESOs to hand over user data upon request from law enforcement as a condition in order to avoid liability for user generated content. As noted below, this introduces additional concerns relating to the right to privacy and the security of encryption. Failure to comply also leads to disproportionate sanctions, namely having online platforms blocked in Indonesia.

Chapter IV of the Regulation sets out a sweeping notice-and-takedown regime that gives broad powers to the government to order the swift removal of content at its discretion.

---

<sup>52</sup> See for example, ARTICLE 19, [At a glance: Does the EU Digital Services Act protect freedom of expression?](#), 11 February 2021, or ARTICLE 19, [Germany: Responding to ‘hate speech’](#), 30 March 2018.

The Regulation requires that Private ESOs rapidly comply with government orders to take down content. Private ESOs must comply with most orders for content removal within 24 hours of being notified by the Ministry, (Article 16(7)) and within four hours for 'urgent' take down requests (Article 16(9)). While Article 14(3) defines 'urgent cases' as those involving terrorism, child sexual abuse images, or 'content that disturbs the community or public order.' ARTICLE 19 finds that this language is vague and overbroad and does not provide individuals with the guidance necessary to regulate their conduct.

The Regulation does not define 'public order,' either in the context of urgent notice and takedown in Article 16 or as it relates to prohibited content described in Article 9 above. The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights offer guidance on permissible derogations in the name of 'public order.' Article 22 emphasises 'respect for human rights is part of public order,' and that public order 'shall be interpreted in the context of the purpose of the particular human right which is limited on this ground.'<sup>53</sup>

Short removal timeframes, such as four and 24 hours, inhibit the careful review of such notices and further increases the risk that legitimate and lawful expression may also be restricted. Ministerial Regulation 5 also empowers the Ministry to compel internet service providers (ISPs) to block access to specific content should the Private ESO not comply with takedown orders (Article 16(10)).

The public can also submit requests to the Ministry for takedown of prohibited content (Article 15). The Ministry may then issue an order to a Private ESO to take down the content within the same timeframe: 24 hours or four hours for 'urgent' cases. The Regulation does not require the Ministry to thoroughly assess public complaints, which leaves the public complaint mechanism open to abuse, including through the discriminatory targeting of minority groups, LGBTQI persons, and other marginalised communities. Public complaints and subsequent takedown orders could also facilitate the harassment of activists, human rights defenders, and journalists, including those reporting on human rights abuses in Papua and West Papua.

The obligations imposed on Private ESOs to proactively monitor and filter prohibited content, which includes third-party hosted content, and to comply with takedown orders from the Ministry violate international human rights standards. The Manila Principles on Intermediary Liability state that internet intermediaries should never be required to proactively monitor content and that orders to restrict content should come from judicial authorities.<sup>54</sup> The UN Special Rapporteur on the Freedom of Opinion and Expression has noted that failure to protect intermediary liability 'creates a strong incentive to censor'<sup>55</sup> and urged states to 'refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.'<sup>56</sup>

## Access to user data

As noted above, the registration process requires that Private ESOs guarantee to grant the Ministry and law enforcement access to their electronic system data, which includes any text and voice data, email records, and 'access codes,' which could mean private passwords, passphrases, or PIN numbers, for example. Article 21 clarifies that Private ESOs are obligated to grant access to the Ministry and law enforcement in the context of oversight in line with Indonesian law. The obligation to provide essentially unfettered access to user data and data systems is inconsistent with international standards on freedom of expression and privacy. Under those standards, access to user data should only be granted subject to a court order and only on a case by case basis.

The Ministry or law enforcement officials may demand access to electronic data or systems for the purpose of 'oversight' in line with Indonesian law (Articles 21-31). Although data obtained this way can only be used for 'oversight' purposes, such requests do not require a court order, which leaves them open to abuse. All orders for access to electronic data or systems, whether for oversight or law enforcement purposes, must be granted within five days. The Regulation provides no effective appeal process by which Private ESOs can challenge such requests for access.

---

<sup>53</sup> [The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights](#), April 1985, Article 23.

<sup>54</sup> Manila Principles, *op. cit.*

<sup>55</sup> HRC, Report of the SR on FoE, [A/HRC/35/22](#), 30 March 2017.

<sup>56</sup> HRC, Report of the SR on FoE, [A/HRC/38/35](#), 6 April 2018.

Ministerial Regulation 5 does not require authorities to obtain a court order to access privately held user data. Private ESOs are required to provide law enforcement officials access to user data related to investigations of crimes punishable by two or more years imprisonment (Article 32). A court order is only required for access to Private ESOs' 'electronic systems' if law enforcement is investigating crimes punishable with between two to five years imprisonment (Article 33).

Article 36 requires that Private ESOs grant law enforcement access to 'user information,' 'communications content,' and 'specific personal data.' 'Specific personal data' is defined broadly to include health data and information, biometric data, genetic data, sexual orientation and sex life data, political view data, children's data, personal financial data, and/or other data as regulated by law (Article 1(21)). Law enforcement must obtain judicial approval before requesting access to 'communication content' and 'specific personal data' (Article 36(3), (4e), and (5)).

The provisions in the Regulation further raise concerns about government sanctioned hacking and weakening of encryption. To comply with government requests to access electronic data and information, Private ESOs would need to break end-to-end encryption of communications. End-to-end encryptions ensure that only the sender and intended recipient of a message are able to read the content between them and the service provider has no way of accessing the content. Furthermore, requiring Private ESOs to grant authorities access to electronic data would make it impossible for users to secure their private information through asymmetric encryption, whereby they possess a unique decryption key known only to them. In other words, Ministerial Regulation 5 could force Private ESOs to create backdoors or introduce other vulnerabilities to comply with government orders.

### Local Contact Person(s)

Ministerial Regulation 5 requires Private ESOs to designate at least one local 'Contact Person' in Indonesia. In particular, Article 25 provides that the contact person(s) shall reside in Indonesia and be responsible for facilitating access requests from the Ministry and other institutions. The local contact person(s) is responsible for responding to requests for access to electronic data and systems for oversight purposes (Articles 22-33) and complying with law enforcement requests for 'user information,' 'communications content,' and 'specific personal data' (Article 36), in line with court orders as required for relevant sentencing limitations as noted above.

The requirement to designate a local contact person raises significant human rights concerns. Companies with local representatives may be more vulnerable to government pressure to comply with overbroad data access or content removal requests, resulting in self-censorship or pre-emptive content removal. Individuals designated as contact persons may face heightened risk of reprisal or judicial harassment. These risks are magnified by the lack of an effective appeal or remedy mechanism allowing companies to challenge official decisions or penalties or seek compensation.

Localisation requirements raise potential administrative or economic challenges and may privilege larger companies with the financial resources to comply, disadvantaging smaller firms. Such practices decrease competition and introduce risks to net neutrality.

### Excessive penalties for failure to comply

Failure to comply with the various obligations set out in the law can lead to heavy and disproportionate penalties.

In particular, Article 45 provides that Private ESOs that fail to grant access to their electronic data under Article 21 are at risk of administrative sanctions enforced by the Ministry. These may include a written warning, temporary termination, blocking of their services in Indonesia, and revocation of their operating license. Cloud computing operators who fail to grant access are only subjected to a written warning or revocation of their operating license (Article 46).

Similarly, failure to respond to notice and takedown orders on prohibited content will first receive a written warning, either once every 24 hours or four hours depending on the takedown window, and after three written warnings a fine will be issued. The fine amount is not explicitly established under the Regulation but is based on Indonesian Non-Tax State Revenue Law. It is highly concerning, however, that the exact amount does

not appear in the law and that the only guidance is provided by statements from the regulator reported in official media, as between 100 and 500 million IDR per piece of content (6,950 – 34,740 USD).<sup>57</sup>

The Ministry is empowered to block the online platforms of Private ESOs that fail to remove content or pay fines (Articles 15 and 16). Judicial institutions can also order the Ministry to take down forbidden content (Article 16).

Under international human rights standards, website blocking is almost always disproportionate since it penalises access to internet resources in circumstances where they might still contain legitimate content. Ministerial Regulation 5 allows the Ministry to block entire websites or online platforms without demonstrating that less severe measures could address the presence of unlawful content on those platforms. For example, the regulation prescribes access blocking for mere procedural violations or the presence of a single piece of 'prohibited' content without evidence of an overwhelming presence of illegal content on the platform. Moreover, service blocking can be imposed for failure to comply with overly vague obligations, violating the principle of legality under international human rights law.

In his 2011 report, the UN Special Rapporteur on Freedom of Opinion and Expression reiterated that States should provide full details regarding the necessity and justification for blocking a particular website and that the determination of what content should be blocked must be undertaken by a competent judicial authority or a body that is independent of any political, commercial or other unwarranted influences in order to ensure that blocking is not used as a means of censorship.<sup>58</sup> Finally, rather than sanctioning providers of digital services, service blocking ultimately penalises users who find themselves deprived of access to information and services and unable to meaningfully exercise their right to freedom of expression. In his 2016 report, the UN Special Rapporteur followed up that 'even if content regulations were validly enacted and enforced, users may still experience unnecessary access restrictions. For example, content filtering in one jurisdiction may affect the digital expression of users in other jurisdictions.'<sup>59</sup>

ARTICLE 19 has previously warned that online content blocking and filtering can restrict the right to freedom of expression. ARTICLE 19 advanced recommendations to protect the right, including that blanket filtering must be prohibited by law; filtering should be user-controlled and transparent; any requirement to block content must be provided by law; blocking should only be ordered by an independent and impartial court or adjudicatory body; and blocking orders must be strictly proportionate to the aim pursued.<sup>60</sup>

---

<sup>57</sup> [Gawat! Belum Daftarin PSE Bisa Kena Sanksi! Ini Prosedur Pendaftaran PSE 2021 Sumber: Gawat! Belum Daftarin PSE Bisa Kena Sanksi! Ini Prosedur Pendaftaran PSE 2021](#), Smart Legal, 8 March 2021; [PP 71/2019 \(PSTE\) Berlaku, Platform Akan Didenda Jika Membiarkan Konten Negatif](#), KOMINFO, 6 November 2019.

<sup>58</sup> Report of the SR on FoE, [A/66/290](#), 10 August 2011, para 82.

<sup>59</sup> A/HRC/32/38, *op. cit.*, para 47.

<sup>60</sup> ARTICLE 19, [Freedom of Expression Unfiltered: How blocking and filtering affect free speech](#), December 2016.

## About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information, and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of ARTICLE 19's analyses are available at <https://www.article19.org/law-and-policy/>.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law and Policy Team, you can contact them by e-mail at [legal@article19.org](mailto:legal@article19.org). For more information about ARTICLE 19's work in Indonesia, contact Michael Caster at [michaelcaster@article19.org](mailto:michaelcaster@article19.org).