350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

May 17, 2021

Mr. Johnny G. Plate
Minister of Communication and Information Technology
Ministry of Communication and Information Technology
Jl. Medan Merdeka Barat 9
Jakarta 10110
Indonesia

Re: Amendments to Ministerial Regulation 5 (MR5)

Dear Minister Plate,

Human Rights Watch is an international human rights organization that carries out monitoring and advocacy in more than 90 countries around the world. Our human rights engagement in Indonesia spans more than three decades. We have worked on a range of rights issues, including freedom of expression, the draft Criminal Code, and the Electronic Information and Transactions Law (Undang-Undang Informasi dan Transaksi Elektronik, or ITE Law).

We write to express serious concern about Ministerial Regulation 5 (MR5), issued on December 2, 2020. MR5 is deeply problematic, granting government authorities overly broad powers to regulate online content, access user data, and penalize companies that fail to comply. The regulation was also issued without adequate public consultation.

On February 16, 2021, President Joko "Jokowi" Widodo stated that he would ask the parliament to revise the ITE Law, saying that it had caused "multiple interpretations" and "must fulfill a public sense of justice." On April 28, Coordinating Minister Mahfud MD announced that the government would not amend the ITE Law, saying that the law is still needed to regulate the internet. Mahfud said the Attorney General, the Minister of Telecommunication, and the National Police would issue a joint decree.

We are concerned that the police will be involved in drafting internet-related regulations, which should be seen through a freedom of expression lens instead of as a criminal law matter.

We will send the government a separate letter outlining concerns with the ITE Law, but as you consider changes to MR5, we urge you to keep in mind President Jokowi's comments that any regulation of the internet "must fulfill a public sense of justice." It is also essential that the process includes sufficient public consultation.

With this in mind, below we offer our recommendations on amending MR5 so that it is consistent with Indonesia's obligations under international law.

Registration and Censorship

MR5, which was made retroactive to November 24, 2020, governs all private sector "electronic systems operators" (ESOs) that are accessible in Indonesia. These are broadly defined to include social media and other content-sharing platforms, digital marketplaces, search engines, financial services, data processing services, and communications services providing messaging or video calls and games.[1] The new regulation will affect many national and regional digital services and platforms, as well as multinational companies like Google, Facebook, Twitter, and TikTok.

MR5 requires all private sector ESOs to register with the Ministry of Communication and Information Technology (the "Ministry") and agree to provide access to their systems and data as specified in the regulation. Those that fail to register by May 24, 2021, will be blocked in Indonesia. Private sector ESOs are required to "ensure" that their platform does not contain or facilitate the distribution of "prohibited content," which would imply a general obligation to monitor content.[2] Failure to do so can lead to blocking of the entire service.[3]

MR5's requirement that private sector ESOs proactively monitor or filter content is both inconsistent with the right to privacy and likely to amount to pre-publication censorship.[4] When combined with the ITE Law, which permits the imposition of criminal penalties on those who "knowingly" permit access to a range of vaguely defined content,[5] MR5 incentivizes internet companies, particularly those that facilitate user-generated content

[1] Ministerial Regulation No. 5 (MR5), art. 2(2).
[2] MR5, art. 9.
[3] MR5, art. 9(6).
[4] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of freedom of opinion and expression, A/HRC/38/35, April 6, 208, para 67.
[5] ITE Law, arts. 27 and 45.

like Facebook, Instagram, TikTok, Twitter, YouTube, and WhatsApp, to unduly restrict freedom of expression and access to information.

The definition of prohibited content is extremely broad, including not only content in violation of Indonesia's already overbroad laws restricting speech, but also any material "causing public unrest or public disorder" or information on how to provide access to, or providing access to, prohibited material.[6] The prohibition of content "providing access to" prohibited material could be understood to prohibit the use of Virtual Private Networks (VPNs), which allow a user access to blocked content but are also routinely used by businesses and individuals to ensure privacy for legal activities. It could also be understood to prohibit providing instructions for gaining access to blocked content.

For "urgent" requests, the ESO must take down content within four hours and all other prohibited content within 24 hours of being notified by the Ministry. Failure to do so can lead to blocking of the service[7] or, in the case of service providers that facilitate user-generated content, substantial fines.[8] The time allocated for response is unrealistically short, particularly for companies that work in multiple time zones, and will impose onerous burdens on smaller ESOs with limited staff. "Urgent" requests are requests to take down material related to terrorism or "child pornography" or "causing public unrest or public disorder." The regulation contains no definition of what constitutes "terrorist" content, nor does it provide standards for determining what material is likely to cause public unrest. This lack of clarity opens the door to use of the regulation to censor opposition or dissenting views.

In addition to taking down the content, the ESO must provide the authorities with user data, including name, home address, email address, and subscriber information for the user who uploaded the prohibited content.[9] Unreasonably short timeframes for removing content would likely incentivize service providers to pre-emptively take down content to ensure compliance. It would possibly force the shutdown of smaller providers who do not have adequate staff available to respond to such requests.

Disproportionate sanctions, like heavy fines or blocking of services can have a significant chilling effect on freedom of expression.[10] Mandatory blocking of entire websites or services such as social networking sites is an extreme measure, which can only be

[6] MR5, art. 9(4).
[7] MR5, art. 15(9).
[8] MR5, art. 15(10).
[9] MR5, art. 11.
[10] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of freedom of opinion and expression, A/HRC/38/35 (2018), para. 66.

justified in accordance with international standards, for example where necessary to protect children against sexual abuse.[11]

MR5 does not appear to provide a mechanism for either the ESO or the person who posted the content to challenge the Ministry's determination to take down content, either before or after it is taken down. The lack of procedural safeguards and channels to appeal decisions only exacerbates the risk that the provisions to take down content will be abused.

Access to User Data

Under the regulation, private sector ESOs must provide access to both their "systems" and their "data" for "supervision" purposes whenever requested to do so. They must also allow law enforcement authorities to access electronic data for criminal investigations into any offense carrying a penalty of at least two years in prison.[12] For access to electronic "systems," law enforcement must obtain a court order when investigating offenses that carry a penalty of between two and five years, but not for those with a possible sentence of more than five years. We do not understand the basis for this distinction, since court orders are even more important when the possible criminal penalties are greater.[13]

Ministries or institutions can request "technical assistance" or other assistance needed to gain access to electronic systems from the private sector ESO, which is required to provide that assistance.[14] A company is still required to provide data even if that data is stored outside of Indonesia as long as it relates to Indonesian residents and businesses – an obligation that could violate data protection and privacy laws in the country in which the data is stored.[15] Allowing such access may also violate the rights of individuals entitled to the protection of those laws, whose data may be disclosed due to communications with the Indonesian resident or business whose data has been requested. A private sector ESO that fails to provide access for supervision and law enforcement faces penalties ranging from a written warning to revocation of their registration.[16]

---

[11] International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Freedom of Expression and the Internet, https://www.osce.org/files/f/documents/e/9/78309.pdf.

[12] MR5, art. 32. Electronic Data is defined to mean "data in electronic form, which is not limited to text, voice, image, map, design, photography, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the likes, alphabets, sign, number, access code, symbol, or perforation." MR5, art. 2(3).

[13] MR5, art. 33. Electronic Systems is defined to mean "a series of electronic devices and procedure having the function to prepare, collect, manage, analyze, store, display, announce, transmit, and/or distribute Electronic Information." MR5, art. 2(4).

[14] MR5, art. 29(3).

[15] MR5, art. 34.

[16] MR5, art. 45.

Requirements that authorities have direct access to systems or massive amounts of information collected and stored by private actors are of serious concern. They are particularly prone to abuse, tend to circumvent key procedural safeguards, and can exceed the limits of what can be considered necessary and proportionate.[17]

MR5 authorizes enforcement officers to demand access to traffic data and electronic user information, including names, home addresses, email addresses, and billing information, for any investigation, without the need for a court order.[18]

Appointment of Local Contact

To facilitate access requests, each private sector ESO must appoint a local contact person to receive and act on those requests.[19]

The requirement to appoint a local contact person in Indonesia would make companies much more susceptible to improper pressure to comply with overbroad content removal and take-down requests and will inevitably lead to an increase in unnecessary censorship, compromise people's privacy and right of access to information. While the establishment of local representatives for tech companies can help them navigate and better understand the different contexts in which they operate, this is dependent on the existence of a legal environment in which it is possible to challenge unfair removal or access requests before independent courts. MR5 provides no mechanism for appeal to the courts, and the presence of staff on the ground makes it much harder for companies to resist overbroad or unlawful requests.

International Standards

The restrictions on content in MR5 are inconsistent with international standards for protection of freedom of expression, notably as formulated in the International Covenant on Civil and Political Rights (ICCPR),[20] which make clear that governments may only impose restrictions on freedom of expression for reasons of national security or other pressing public need if they are provided by law and are strictly necessary and proportionate for achieving a legitimate state aim.[21] MR5 does not specify what content will be deemed likely to "cause public unrest or public disorder," leaving both users and the service providers uncertain what content is prohibited. In doing so, it fails to meet the requirement that

---

[17] UN Human Rights Council, Report of the UN High Commissioner for Human Rights, A/HRC/39/29, para. 18.

[18] MR5, art. 36.

[19] MR5, art. 25.

[20] International Covenant on Civil and Political Rights (ICCPR), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, *entered into force* March 23, 1976. Indonesia ratified the International Covenant on Civil and Political Rights in February 2006.

[21] UN Human Rights Committee, General Comment No. 34, UN Doc. CCPR/C/GC/34 (2011), paras. 21-36.

restrictions formulated with sufficient precision to enable an individual to regulate their conduct accordingly.[22] The lack of clarity is also likely to lead to over-censorship on the part of ESOs concerned about compliance with the regulation.

The MR5's use of a model that permits government agencies, rather than judicial authorities, to determine what content is impermissible is also inconsistent with international standards. The UN Special Rapporteur on freedom of opinion and expression advised that states should refrain from adopting models of regulation in which government agencies rather than judicial authorities become the arbiters of lawful expression.[23] They should also avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users.[24]

Finally, the imposition of liability on intermediaries such as ESOs for content posted by third parties is extremely problematic.[25] In reviewing the regulation's imposition of intermediary liability, the National Assembly should take into consideration the Manila Principles on Intermediary Liability, developed by a coalition of civil society experts and issued in 2015. Laws governing intermediary liability should be precise, clear, and accessible and intermediaries should be immune from liability for third-party content when they have not been involved in modifying that content.[26] The UN Special Rapporteur on freedom of opinion and expression advised that states should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on internet intermediaries, and from requiring the "proactive" monitoring or filtering of content.[27]

---

[22] UN Human Rights Committee, General Comment No. 34, UN Doc. CCPR/C/GC/34 (2011), para. 25.

[23] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of freedom of opinion and expression, A/HRC/38/35, para. 68.

[24] Ibid.

[25] UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," March 30, 2017, UN Doc. A/HRC/35/22, para. 49 (noting that "intermediary liability creates a strong incentive to censor; providers may find it safest not to challenge such regulation but to over-regulate content such that legitimate and lawful expression also ends up restricted."); UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," April 6, 2018, UN Doc. A/HRC/38/35, para. 66.

[26] Manila Principles on Intermediary Liability, March 24, 2015, https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf; UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," April 6, 2018, UN Doc. A/HRC/38/35, para. 66.

[27] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," April 6, 2018, UN Doc. A/HRC/38/35, paras. 66-67.

Recommendations

Human Rights Watch urges you to:

- Suspend implementation of Ministerial Regulation 5 before the May 24 deadline for registration.
- Fully consult with stakeholders and civil society groups to determine how to revise MR5 to meet the requirements of international law, the standards elaborated by United Nations experts, and the Manila Principles on Intermediary Liability to protect the rights to privacy and freedom of expression in Indonesia.
- Any new or revised regulation should:
    - Narrow the definition of Electronic Systems Operators covered by the regulation;
    - Narrow the definition of "prohibited content" to include only content that creates a clear threat to national security or public order, such as child sexual exploitation images or incitement to violence;
    - Require an order from an impartial and competent court before an ESO can be required to take down content;
    - Provide a realistic and flexible timeframe for an ESO to take down content pursuant to court order;
    - Provide a clear avenue of appeal of any take-down order to a competent judicial authority;
    - Limit intermediary liability to instances in which the ESO or relevant entity has failed to comply with a narrowly tailored take-down order from an impartial and competent court. Penalties should be proportionate, and should not include blocking of the entire service;
    - Ensure all requests for user data meet the standards of necessity and proportionality and respect due process;
    - Require a court order for requests for content data;
    - Remove the sections permitting government access to electronic data and electronic systems for "supervision" and law enforcement;
- Remove the requirement that ESOs appoint a local contact.

Thank you for your consideration. We are available to meet with you to discuss our concerns further and offer expert advice.

Sincerely,

Brad Adams
Executive Director
Asia Division

CC:
President Joko Widodo
House of Representative Speaker Puan Maharani
Coordinating Minister for Political, Legal, and Security Affairs Mohammad Mahfud MD
National Police Chief Listyo Sigit Prabowo
Attorney General Sanitiar Burhanuddin
Minister of Law and Human Rights Yasonna Laoly
Commission I, House of Representatives, chairwoman Meutya Viada Hafid
Commission III, House of Representatives, chairman Herman Herry