



Hak Digital untuk Demokrasi dan *Civic Space*:

Studi Pemetaan Regulasi
Internet di Indonesia

Southeast Asia
Freedom of
Expression Network
(SAFEnet)

Pusat Studi Hukum
dan Kebijakan
Indonesia
(PSHK)

April
2025

Southeast Asia
Freedom of
Expression Network
(SAFEnet)

Pusat Studi Hukum
dan Kebijakan
Indonesia
(PSHK)

**April
2025**

Hak Digital untuk Demokrasi dan Civic Space:

Studi Pemetaan Regulasi Internet di Indonesia

April 2025

Tim Penyusun

Tim Penulis:

Tessa Ardhia Maheswari
Shinta Ressmy CN
Dean Rizqullah
Balqis Zakkiyah Qonita
Asfinawati
Alviani Sabillah
Violla Reininda

Editor:

Violla Reininda

Desain & Tata Letak

Atsarina Kardina

Dengan Dukungan Kedutaan
Belanda

Penerbit

SAFEnet
Jl. Gita Sura III No 55
Denpasar, Bali 80115

 +62 817 9323 375

 info@safenet.or.id

 safenet.or.id

 @safenetvoice



Laporan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di <https://creativecommons.org/licenses/by-nc/4.0/>

Ringkasan Eksekutif

Ruang gerak masyarakat sipil (*civic space*) tak hanya terbentuk di ruang fisik semata, tetapi dalam perkembangannya, juga meluas ke ruang digital. Ruang digital menjadi wadah bagi masyarakat sipil untuk dapat berpartisipasi mengekspresikan kebebasan sipil dan politik dalam tatanan masyarakat demokratis. Peluasan ini berdampak pada perlunya negara memberikan jaminan pemenuhan, penghormatan, dan perlindungan atas hak digital bagi masyarakat sipil. Interaksi dan aktivitas di ruang digital yang diatur dengan pendekatan hak asasi manusia memungkinkan masyarakat untuk dapat berkomunikasi, menjalankan kebebasan sipil, dan memengaruhi

kebijakan tanpa takut akan penindasan, diskriminasi, atau kriminalisasi.

Southeast Asia Freedom of Expression Network (SAFEnet) bersama Pusat Studi Hukum dan Kebijakan Indonesia (PSHK) menilik seberapa jauh negara memberikan jaminan pemenuhan, penghormatan, dan perlindungan atas hak digital tersebut dalam tatanan negara demokrasi dan peluasan ruang gerak masyarakat sipil (*civic space*), yang dituangkan dalam **Laporan Penelitian “Hak Digital untuk Demokrasi dan Civic Space: Studi Pemetaan Regulasi Internet di Indonesia”**. Pada laporan penelitian ini, SAFEnet dan PSHK memetakan regulasi internet dan ruang digital di

Indonesia serta mengidentifikasi celah pada tiap pengaturan untuk mewujudkan regulasi tata kelola internet yang berbasis hak asasi manusia. Tolok ukur analisis regulasi tata kelola internet tersebut merujuk pada *The Charter of Human Rights and Principles for the Internet* (ICRP), terutama untuk menghasilkan pengaturan tata kelola internet yang memperhatikan aspek akses internet, aspek proteksi dan keamanan digital, serta aspek kebebasan (*liberty*). Studi ini menggunakan tiga metode penelitian, yaitu *regulatory gap analysis* (analisis kesenjangan kebijakan), studi literatur, dan studi kasus selektif.

Berdasarkan temuan dan analisis dari SAFEnet dan PSHK, dapat disimpulkan sebagai berikut.

01

saat ini terdapat 13 (tiga belas) undang-undang dan 153 (seratus lima puluh tiga) pasal yang mengatur tata kelola internet di Indonesia. Dari jumlah tersebut, ditemukan terdapat 51 (lima puluh satu) norma yang mengatur aspek akses internet atau setara dengan 33.3% (tiga puluh tiga koma tiga persen), 80 (delapan puluh) ketentuan yang mengatur aspek proteksi dan keamanan digital atau

setara dengan 52.3% (lima puluh dua koma tiga persen), dan 22 (dua puluh dua) ketentuan yang mengatur aspek kebebasan (*liberty*) atau setara dengan 14.4% (empat belas koma empat persen). Dari data tersebut, terlihat bahwa orientasi pengaturan tata kelola internet yang tersebar pada 13 (tiga belas) undang-undang tersebut memiliki kecenderungan proteksionis (*protection*

heavy). Artinya, negara memiliki kecenderungan untuk mengontrol warga negara dalam beraktivitas di ruang digital. Paradigma ini diperkuat dengan minimnya jaminan kebebasan dalam undang-undang-undang yang menjadi objek riset,

02

implementasi peraturan perundang-undangan yang sudah dibahas sebelumnya tidak cukup melindungi masyarakat sipil dalam beraktivitas di ruang digital. Dalam temuan ini, upaya *controlling* dari negara tidak hanya terlihat dari banyaknya aspek proteksi yang diatur, kecenderungan ini terlihat hingga pada tahap implementasi. Pada aspek akses internet, masih seringkali terdapat pembatasan dengan tidak proporsional, transparan, dan sesuai dengan kebutuhan. Di sisi lain, pasal-pasal yang mengatur

dalam hal ini, jaminan kebebasan hanya ditemukan dalam sembilan undang-undang saja. Sementara pada aspek akses, pengaturan lebih banyak kaitannya dengan keterbukaan informasi.

mengenai proteksi justru masih banyak yang dijadikan sebagai justifikasi untuk melindungi pandangan mayoritas saja atau hanya menguntungkan kepentingan individu yang timpang kuasanya dengan mengkriminalisasi masyarakat, terutama kelompok rentan. Pada aspek kebebasan, selain jaminan perlindungan yang minim, dalam implementasinya, pasal-pasal yang mengatur mengenai jaminan kebebasan berpendapat dan berekspresi jarang digunakan.

03

kendati pengaturan tata kelola internet cenderung bersifat proteksionis, tidak terdapat penekanan pada akuntabilitas negara untuk bertanggung jawab dan memberikan pemulihan atas kesalahan atau kelalaian instansi negara yang berujung pada kerugian bagi masyarakat. Kasus-kasus yang diteliti juga menunjukkan tidak berjalannya akuntabilitas, baik dalam kasus-kasus individual maupun pelanggaran HAM oleh negara.

04

pengaturan tata kelola internet bukan merupakan isu sektoral, sehingga terdapat pertautan antara aspek pengaturan pada norma di satu undang-undang dengan undang-undang lainnya.

05

undang-undang yang berusia lebih dari lima tahun harus diperbarui agar lebih relevan dan sesuai dengan konteks perkembangan

pemanfaatan ruang digital dan perlindungan pengguna ruang digital dewasa ini. Misalnya, UU Pers agar dapat melindungi kebebasan jurnalis yang membagikan informasi melalui *platform* media sosial, serta UU

Pemilu dan UU Pilkada, misalnya agar terdapat aturan kampanye yang lebih relevan dengan pemanfaatan sosial media saat ini.

06

pengaturan tentang tata kelola internet yang ada saat ini belum cukup efektif memberikan perlindungan kepada kelompok rentan, yaitu kelompok perempuan, kelompok minoritas kepercayaan, kelompok keberagaman gender, jurnalis, dan masyarakat sipil yang kritis terhadap kekuasaan. Alih-alih memberikan perlindungan, ketentuan yang ada malah mengekang kebebasan dan mengancam keselamatan kelompok rentan tersebut, seperti kriminalisasi menggunakan UU ITE dan UU Pornografi.

07

jangkauan ketentuan hukum yang ada saat ini belum cukup untuk mendorong akuntabilitas *platform* media sosial. Belum terdapat pengaturan di level undang-undang yang menjadi dasar pertanggungjawaban dan transparansi bagi *platform* media sosial dalam mengeset algoritma dan memoderasi konten untuk dicermati pengguna media sosial.

“

pengaturan tentang tata kelola internet yang ada saat ini belum cukup efektif memberikan perlindungan kepada kelompok rentan, yaitu kelompok perempuan, kelompok minoritas kepercayaan, kelompok keberagaman gender, jurnalis, dan masyarakat sipil yang kritis terhadap kekuasaan.

Hukum tentang tata kelola internet yang ada saat ini belum menggunakan pendekatan untuk mengakomodasikan hak asasi manusia, terutama hak digital masyarakat. Hal ini menggambarkan jelas bahwa terdapat potensi ancaman terhadap demokrasi dan penyempitan ruang gerak masyarakat sipil di ruang digital, termasuk pemenuhan hak-hak digital. Celaknya, kebebasan di ruang digital terkait dan tidak dapat dipisahkan dari kebebasan di ruang fisik. Artinya, hilangnya kebebasan di ruang digital dapat berarti kehilangan berganda.

Pada penelitian ini, SAFEnet dan PSHK menghadirkan dua rekomendasi, yaitu **rekomendasi penyempurnaan kebijakan** dan **rekomendasi riset lanjutan**. Pada **rekomendasi penyempurnaan kebijakan,**

berikut hal yang perlu dipertimbangkan untuk menciptakan regulasi internet yang memenuhi hak digital:

1. Pemerintah dan DPR melakukan revisi komprehensif terhadap pengaturan terkait tata kelola internet yang lebih menjamin aspek akses, aspek proteksi dan keamanan digital, serta aspek kebebasan dengan seimbang. Komitmen ini dimulai dengan membentuk tim lintas sektor yang melibatkan masyarakat sipil untuk melakukan pemetaan regulasi dan membentuk naskah akademik tata kelola internet yang berbasis hak asasi manusia dan memperluas ruang gerak masyarakat sipil;

2. Sebagai upaya pendahuluan dalam melakukan revisi komprehensif tersebut di atas, kami mendorong para pihak untuk melakukan langkah-langkah sebagai berikut:

a. Mahkamah Agung untuk membentuk Peraturan/Surat Edaran Mahkamah Agung untuk menangani kasus terkait dengan tata kelola internet dan kaitannya dengan aspek akses, aspek proteksi dan keamanan digital, serta aspek kebebasan;

b. Peningkatan kompetensi dari pelaksana teknis dan membentuk mekanisme pengawasan untuk mengurangi human error dan memastikan implementasi prosedur yang mempengaruhi hak digital masyarakat;

c. Meningkatkan transparansi dan akuntabilitas pemerintah dan sektor bisnis digital tentang pemutusan dan pelambatan akses, kebocoran data, dan penyensoran konten;

d. Aparat penegak hukum menjalankan akuntabilitas penegakan hukum di ruang digital kepada masyarakat melalui keterbukaan

laporan penanganan kasus;

e. Presiden melakukan pengawasan ketat kepada Kepolisian dan Kejaksaan agar memiliki perspektif hak asasi manusia dan perlindungan korban dalam penegakkan hukum di ruang digital; dan

f. DPR menjalankan fungsi pengawasan terhadap penegakan hukum di ruang digital termasuk meminta laporan secara berkala terhadap Presiden, Jaksa Agung dan Kapolri setidaknya mengenai penegakan hukum dan penggunaan anggaran di ruang digital.

Pada rekomendasi riset lanjutan, kami menyadari bahwa penelitian ini tak terhindarkan dari kekurangan. Sejumlah hal yang dapat menjadi objek penelitian lanjutan, yaitu:

a. Meneliti lebih lanjut tentang singgungan antara hak digital dengan hak-hak asasi manusia di ruang fisik, terutama hak ekonomi, sosial, dan budaya (ekosob). Dalam hal ini, penelitian lebih lanjut dapat menyibak bagaimana hak sipil dan politik di ruang digital memengaruhi pengejawantahan hak sipil dan politik di ruang fisik, bagaimana hak sipil dan politik di ruang digital memengaruhi hak ekosob di ruang fisik, bagaimana hak ekosob di ruang digital memengaruhi hak sipil dan politik di ruang fisik, dan bagaimana hak ekosob di ruang fisik memengaruhi hak ekosob di ruang digital;

b. Meneliti lebih lanjut tentang identifikasi peran aktor terkait dalam tata kelola internet, sehingga dapat membentuk pengaturan tata kelola internet yang berbasis hak asasi manusia dan memperluas ruang gerak masyarakat sipil.

Daftar Isi

Ringkasan Eksekutif	04
Daftar Isi	08
Kata Pengantar	09-10
1. Latar Belakang	12
A. Perkembangan Internet	14
B. Ruang Digital sebagai Ruang Baru	15
C. Langkah awal Indonesia Mengatur Ruang Digital	17
D. Aktivisme dan Ruang Digital di Indonesia	18
2. Metode Penelitian	22
3. Paradigma Pengaturan Tata Kelola Internet dan Ruang Digital	26
A. Paradigma Umum	27
B. Model Pengaturan Intenet Berdasarkan Sejarah	36
4. Prinsip Tata Kelola Internet dalam The Charter of Human Right and Principles for the Internet	38
5. Pemetaan Regulasi Internet di Indonesia dan Perkembangannya	44
A. Pengaturan tentang Tata Kelola Internet	45
1. Akses Internet	47
2. Proteksi dan Keamanan Digital	56
3. Kebebasan Berekspresi (<i>Liberty</i>)	65
6. Implementasi Penegakan Hukum dalam Ruang Digital	76
1. Akses Internet	77
2. Proteksi dan Keamanan Digital	80
3. Kebebasan Berekspresi (<i>Liberty</i>)	84
7. Kesimpulan dan Rekomendasi	86
A. Kesimpulan	87
B. Rekomendasi Penyempurnaan Kebijakan	90
C. Rekomendasi Riset Lanjutan	91
DAFTAR PUSTAKA	92

Kata Pengantar

Ruang digital memainkan peran kunci dalam memperluas partisipasi dan memperkuat proses demokratisasi. Ia tidak lagi hanya berfungsi sebagai saluran komunikasi atau pertukaran informasi, tetapi telah berkembang menjadi ruang partisipasi publik, pengorganisasian gerakan sosial, serta ekspresi politik warga negara. Ruang digital merupakan perluasan dari ruang-ruang di mana masyarakat sipil dapat menyuarakan pendapat, memperjuangkan hak, dan mengawasi jalannya kekuasaan.

Namun, perluasan ruang ini belum sepenuhnya diimbangi dengan kerangka regulasi dan aturan yang adil dan berbasis hak asasi manusia. Alih-alih melindungi, beberapa regulasi justru membatasi kebebasan berekspresi dan berisiko mempersempit ruang sipil digital. Karena itu, sangat penting hadirnya regulasi yang menjamin kebebasan, memberikan akses yang setara, memberikan perlindungan, serta mendorong akuntabilitas para aktor.

Penelitian ini disusun sebagai upaya untuk menelaah kondisi tata kelola ruang digital di Indonesia saat ini, khususnya bagaimana negara menjamin hak digital masyarakat sipil dalam kerangka demokrasi. SAFEnet dan PSHK melakukan pemetaan terhadap regulasi internet yang berlaku, menganalisis kesenjangan normatif, dan mengidentifikasi pola serta kecenderungan pengaturan yang berdampak langsung pada kebebasan sipil di ruang digital.

Analisis terhadap 13 undang-undang dan 153 pasal menunjukkan bahwa regulasi tata kelola internet masih sangat dominan dalam aspek proteksi dan kontrol, dengan jaminan kebebasan yang sangat terbatas. Ketimpangan ini berdampak pada menyempitnya ruang digital yang aman dan setara, terutama bagi kelompok-kelompok rentan dan masyarakat sipil yang kritis terhadap kekuasaan. Selain itu, akuntabilitas negara dan tanggung jawab platform digital masih belum diatur secara memadai.

Laporan ini tidak hanya menyajikan potret regulatif yang ada, tetapi juga menawarkan rekomendasi kebijakan yang konkret untuk perbaikan tata kelola internet yang lebih adil dan demokratis. Rekomendasi riset lanjutan juga disampaikan guna memperdalam kajian terkait relasi antara hak digital dan hak-hak asasi lainnya di berbagai konteks sosial.

Kami berharap laporan ini dapat menjadi rujukan bagi pembuat kebijakan, penegak hukum, masyarakat sipil, dan aktor-aktor digital dalam mendorong arah regulasi yang lebih berpihak pada hak asasi manusia dan memperkuat demokrasi di era digital.

Nenden Sekar Arum

Direktur Eksekutif

**Southeast Asia Freedom of Expression Network
(SAFEnet)**

Kata Pengantar

Pusat Studi Hukum dan Kebijakan

Tak bisa dimungkiri, ruang digital telah menjelma menjadi bagian penting dari kehidupan demokratis kita hari ini. Ia bukan sekadar ruang baru, tetapi perpanjangan dari ruang fisik tempat masyarakat sipil mengekspresikan pendapat, berkumpul, berserikat, dan mempengaruhi kebijakan publik. Maka, sebagaimana ruang fisik, ruang digital pun seharusnya dijamin oleh hukum untuk menjadi ruang yang aman, setara, dan bebas dari ancaman.

Sayangnya, arah regulasi ruang digital di Indonesia justru menunjukkan kecenderungan yang mengkhawatirkan. Alih-alih memberikan jaminan atas hak-hak digital warga negara, pengaturan hukum yang ada hari ini lebih banyak berorientasi pada kontrol dan pembatasan. Pendekatan semacam ini bukan saja melahirkan ketimpangan dalam beraktivitas di ruang digital, tetapi juga memperlihatkan pola lama yang kini menjalar ke medium baru: pembungkaman atas nama hukum, dengan konsekuensi serius bagi demokrasi dan ruang gerak masyarakat sipil.

Pusat Studi Hukum dan Kebijakan Indonesia (PSHK) telah lama memberikan perhatian pada kualitas peraturan perundang-undangan dan ruang gerak masyarakat sipil. Studi ini merupakan bagian dari kelanjutan perhatian tersebut, kali ini berfokus pada tata kelola ruang digital. Bersama SAFEnet, kami memetakan berbagai pengaturan hukum terkait internet di Indonesia, menelaah celah-celah regulatornya, serta mengkaji sejauh mana pengaturan tersebut mengakomodasi hak-hak digital warga negara.

Temuan dari laporan ini menunjukkan bahwa kerangka hukum kita masih timpang. Aspek kebebasan berekspresi dan jaminan akses belum menjadi perhatian utama, sementara aspek proteksi cenderung digunakan sebagai dalih untuk mengontrol, bahkan mengkriminalisasi, terutama terhadap kelompok rentan dan masyarakat sipil yang kritis terhadap kekuasaan. Minimnya akuntabilitas negara dan belum adanya mekanisme pengawasan yang memadai terhadap platform digital memperparah situasi ini. Semua ini menjadi pertanda bahwa ruang digital pun mengalami penyempitan, sebagaimana yang telah lama terjadi di ruang fisik.

Studi ini hadir sebagai bentuk kontribusi PSHK dan SAFEnet dalam menghadirkan pemahaman yang lebih utuh tentang kondisi tata kelola internet di Indonesia hari ini. Harapannya, laporan ini dapat menjadi dasar untuk advokasi kebijakan yang lebih kuat—yang tak hanya mendorong pembaruan regulasi, tetapi juga membentuk kerangka kerja yang menjamin kebebasan, akses, dan perlindungan digital secara seimbang dan berperspektif hak asasi manusia.

Kami mengucapkan terima kasih kepada tim peneliti PSHK dan SAFEnet atas kerja keras dan kolaborasi dalam menyusun laporan penting ini. Secara khusus, kami menyampaikan apresiasi kepada SAFEnet yang telah mengajak PSHK untuk terlibat dalam riset ini dan terus mendorong agenda advokasi kebijakan ke depan. Semoga hasil studi ini menjadi pijakan penting dalam memperluas ruang demokrasi, tak hanya secara fisik, tetapi juga dalam lanskap digital Indonesia.

Rizky Argama

Direktur Eksekutif

**Pusat Studi Hukum dan Kebijakan Indonesia
(PSHK)**

Southeast Asia
Freedom of
Expression Network
(SAFEnet)

Pusat Studi Hukum
dan Kebijakan
Indonesia
(PSHK)

**April
2025**

Hak Digital untuk
Demokrasi dan
Civic Space:

Studi Pemetaan Regulasi
Internet di Indonesia

01

Latar Belakang

1. Latar Belakang

“
Ruang gerak masyarakat sipil (*civic space*) merupakan ruang bagi masyarakat sipil untuk dapat berpartisipasi mengekspresikan kebebasan sipil dan politik dalam tatanan masyarakat demokratis.

Dalam perkembangannya, ruang gerak masyarakat sipil tidak hanya terbentuk di ruang fisik, tetapi juga meluas ke ruang digital. Ruang digital menjadi wadah bagi masyarakat sipil untuk berpartisipasi mengekspresikan kebebasan sipil dan politik dalam tatanan masyarakat demokratis. Tempat ini menjadi peluasan ruang untuk menginiasi percakapan tentang diskursus kebijakan publik, memengaruhi kebijakan publik, mengekspresikan opini dan jati diri, atau sekadar melakukan interaksi sosial.

Peluasan ini berdampak pada perlunya negara memberikan jaminan pemenuhan, penghormatan, dan perlindungan atas hak digital bagi masyarakat sipil. Jaminan tersebut dituangkan dalam beragam peraturan perundang-undangan, baik secara sektoral maupun pengaturan khusus. Interaksi dan aktivitas di ruang digital yang diatur dengan pendekatan hak asasi manusia memungkinkan masyarakat untuk dapat berkomunikasi, menjalankan kebebasan sipil, dan memengaruhi kebijakan tanpa takut akan penindasan, diskriminasi, atau kriminalisasi. Melalui penelitian ini, Southeast Asia Freedom of Expression Network (SAFEnet) bersama Pusat Studi Hukum dan Kebijakan Indonesia (PSHK) menilik seberapa jauh negara memberikan jaminan pemenuhan, penghormatan, dan perlindungan atas hak digital tersebut dalam tatanan negara demokrasi dan peluasan ruang gerak masyarakat sipil (*civic space*).

Studi ini menitikberatkan pada pemetaan dan analisis terhadap ragam peraturan yang mengatur tentang ruang digital dan tata kelola internet di Indonesia, khususnya di level undang-undang. Tak hanya substansi undang-undang, objek penelitian juga ditujukan pada implementasi undang-undang tersebut dalam penggunaan ruang digital dan penegakan hukum. Landasan analisis

yang digunakan dalam penelitian ini adalah *The Charter of Human Rights and Principles for the Internet* (ICRP), terutama untuk menghasilkan pengaturan tata kelola internet yang memperhatikan aspek akses internet, aspek proteksi dan keamanan digital, serta aspek kebebasan (*liberty*). Penelitian ini menggunakan tiga metode, yaitu *regulatory gap analysis* (analisis kesenjangan kebijakan), studi literatur, dan studi kasus selektif.

Studi dilakukan dengan terlebih dahulu mengupas tentang perkembangan internet dan ruang digital sebagai ruang baru. Disajikan pula bagaimana langkah awal Indonesia mengatur ruang digital dan gambaran aktivisme dan ruang digital di Indonesia. Kemudian, dipaparkan tentang paradigma pengaturan tata kelola internet dan ruang digital secara umum dan dengan pendekatan historis perkembangannya. Selanjutnya, studi menggariskan tolok ukur landasan analisis yang digunakan, yaitu prinsip tata kelola internet dalam ICRP. Setelah menentukan landasan analisis, paparan dilanjutkan dengan pemetaan regulasi internet di Indonesia dan perkembangannya pada tiga aspek, yaitu aspek akses internet, aspek proteksi dan keamanan digital, serta aspek kebebasan berekspresi (*liberty*). Studi ini juga dilengkapi dengan pendekatan studi kasus yang menganalisis tentang implementasi dari tiap-tiap undang-undang terhadap ketiga aspek di atas. Studi ini pun menghasilkan rekomendasi untuk penyempurnaan kebijakan tentang tata kelola internet yang berbasis hak asasi manusia dan rekomendasi untuk pengembangan riset lanjutan tentang tata kelola internet dan hak digital.

A.

Perkembangan Internet

Perkembangan internet yang semakin pesat pada periode 1990-an memunculkan berbagai istilah baru untuk menyebutnya, seperti “ruang siber”, “ruang digital”, dan “dunia maya”. Berbagai istilah ini muncul karena anggapan bahwa internet memiliki sifat yang unik dan menawarkan alternatif pergerakan politik di dunia modern. Keberadaan internet dianggap memunculkan ruang baru untuk melakukan kegiatan komunal sebagai bentuk partisipasi politik. Keberadaan internet tentunya telah membentuk pola interaksi baru untuk meningkatkan kolaborasi dalam kehidupan demokrasi. Paul M. Schwartz, dengan mengutip dari berbagai ahli, menjelaskan bahwa internet telah menjanjikan ruang baru bagi forum demokrasi yang penuh pertimbangan. Keberadaan internet dianggap sebagai jawaban atas pencarian terhadap ruang baru yang ramah untuk mendiskusikan demokrasi.¹ Laura J. Gulak juga menjelaskan bahwa internet, sebagai ruang elektronik, secara cepat dan simultan memungkinkan individu-individu dengan nilai yang sama untuk berkumpul mendiskusikan suatu permasalahan dan mengambil tindakan politik yang efektif.²

B.

Ruang Digital sebagai Ruang Baru

Ruang sipil merujuk pada lingkungan yang memungkinkan individu dan kelompok untuk menjalankan hak mereka atas kebebasan berekspresi, berasosiasi, dan berkumpul secara damai. Ruang sipil adalah aspek mendasar dari masyarakat demokratis tempat orang dapat berpartisipasi dalam kehidupan politik, sosial, dan ekonomi. Apabila berfungsi dengan baik, ruang sipil

memungkinkan warga negara untuk mengatur, berkomunikasi, dan mempengaruhi kebijakan yang mempengaruhi kehidupan mereka tanpa takut akan penindasan atau diskriminasi. Dalam arti yang lebih luas, ruang sipil mencakup ruang fisik dan digital tempat keterlibatan warga terjadi, seperti alun-alun, *platform* media sosial, dan pusat komunitas. Ruang sipil menjadi objek penting untuk perlindungan hak asasi manusia, promosi keadilan sosial, dan akuntabilitas pemerintah dan lembaga. Dalam konteks Indonesia, ruang sipil sangat dipengaruhi oleh sejarah politik, perubahan sosial, dan perkembangan teknologi.

Ruang digital memainkan peran penting dalam perkembangannya. Platform media sosial, misalnya, berkembang pesat di ruang digital dengan bantuan akses internet yang dapat diakses oleh publik. Ruang digital membantu menciptakan ruang untuk perdebatan publik, termasuk di dalamnya berbagai bentuk komunikasi publik yang melibatkan warga dari berbagai kalangan dan lapisan kelas. Ruang digital memungkinkan warga untuk saling bertemu tanpa ada pertemuan secara fisik, dapat diartikan pula bahwa pertemuan di ruang digital lebih efektif dan efisien.

Lebih dari itu, saat ini ruang digital dapat mengkonseptualisasikan sebagai ruang yang lebih dasar; bisa menjadi pasar, sekolah, tempat kencan, bioskop portable, ruang olah raga, instalasi seni hingga ruang sipil daring. Dalam konteks bisnis dan ekonomi, misalnya, platform digital menyediakan banyak pilihan kepada warga untuk menjalankan bisnis atau transaksi jual beli, mulai dari platform jual-beli lintas negara seperti Amazon, maupun platform kecil seperti Usaha Mikro Kecil dan Menengah (UMKM) berbasis aplikasi atau yang dikendalikan secara digital oleh warga.

Selain berinteraksi secara personal, warga dapat berinteraksi secara massal seperti

apabila ada perdebatan politik, siapa pun dapat ikut serta dalam perdebatan tersebut. Ruang digital menjadi salah satu alternatif bagi warga yang merasa bahwa ruang publiknya telah direnggut oleh negara. Mereka dapat dengan mudah, murah dan bebas untuk berekspresi dan mengakses informasi.³

Pada masa awal kemerdekaan hingga masa Orde Baru, ruang sipil di Indonesia didominasi oleh perjuangan untuk mengonsolidasikan kekuasaan negara dan identitas nasional. Kebebasan berserikat dan berekspresi relatif terbatas, terutama di bawah pengaruh ideologi yang kuat seperti nasionalisme dan komunisme. Di bawah pemerintahan Presiden Soeharto, ruang sipil mengalami penekanan yang signifikan. Rezim Orde Baru menerapkan kontrol ketat terhadap media, organisasi masyarakat, dan aktivitas politik. Pembatasan kebebasan berekspresi dan pengawasan ketat terhadap aktivitas masyarakat sipil adalah ciri khas periode ini.

Jatuhnya Soeharto pada tahun 1998 membuka jalan bagi era reformasi, yang menempatkan ruang sipil mengalami peluasan yang signifikan. Kebebasan pers meningkat, masyarakat sipil mulai berperan lebih aktif dalam politik, dan munculnya organisasi non-pemerintah yang beragam. Namun demikian, ruang sipil tetap menghadapi tantangan, seperti ancaman terhadap kebebasan berekspresi dan tindakan represif dari aparat negara dalam situasi tertentu.

Mengacu pada data V-Dem Institute, demokrasi di berbagai belahan dunia telah mengalami penurunan secara terus menerus sejak 1986. IDEA International juga melaporkan hal serupa, separuh dari seluruh negara yang ada di dunia sedang mengalami kemunduran demokrasi. Demokrasi tidak selalu dikategorikan sebagai praktik langsung seperti halnya pemilihan umum (pemilu), melainkan juga apa yang

terjadi di ruang publik digital. Secara signifikan, demokrasi digital mengalami penyusutan di ruang sipil digital sehingga masyarakat sipil kehilangan banyak kesempatan dalam berkumpul di ruang digital karena kebebasan yang tidak dijamin oleh negara.

Demokrasi digital erat kaitannya dengan gerakan aktivisme publik. Aktivisme yang dilakukan oleh masyarakat dewasa ini tidak hanya terbatas di ruang fisik saja, melainkan juga sudah dilakukan di ruang digital. Aktivisme digital dapat dikategorikan sebagai salah satu bentuk aktivisme modern yang merujuk pada partisipasi seseorang atau sekelompok individu pada berbagai kegiatan yang membawa perubahan dan dampak positif di lingkungan tertentu. Sementara itu, aktivisme digital atau biasa juga dikenal sebagai *e-activism* adalah bentuk aktivisme yang dilakukan dengan bantuan internet sebagai pendukung dalam gerakan, baik digunakan sebagai sarana komunikasi, agitasi dan propaganda, maupun mobilisasi gerakan dari berbagai isu sosial.⁴

Berkembangnya isu politik di ruang digital dan berbaurnya masyarakat sipil dalam ruang tersebut menjadikan makna politik menjadi lebih cair dan pengertian aktivisme tidak lagi menunjukkan kekakuan seperti periode sebelumnya. Saat ini, dengan bantuan internet, semua orang dapat berpartisipasi dengan metode yang paling sederhana sekalipun, yaitu *clicktivism*. *Clicktivism* dipahami sebagai aktivisme daring yang menggunakan internet dan media sosial sebagai medium penyebaran ide atau gagasan (Cambridge Dictionary).

Kehidupan kolektif warga dalam ruang digital juga mengalami pergeseran. Arab Spring, misalnya, pada periode 2011 gerakan masyarakat sipil dalam melawan rezim diktator menggunakan media sosial Twitter sebagai sarana komunikasi, koordinasi hingga mengagitasi masyarakat dunia mengenai apa yang terjadi di Mesir. Pada

“
Demokrasi digital erat kaitannya dengan gerakan aktivisme publik. Aktivisme yang dilakukan oleh masyarakat dewasa ini tidak hanya terbatas di ruang fisik saja, melainkan juga sudah dilakukan di ruang digital.

periode yang berdekatan, 2014, misalnya, di Hong Kong, ribuan orang melakukan gerakan “Revolusi Payung” atau “Umbrella Revolution” selama berbulan-bulan. Gerakan ini memprotes sistem Pemilu di Hong Kong yang dianggap membatasi pilihan warga negara dengan memperketat calon kepala negara Hong Kong. Gerakan ini juga memanfaatkan ruang sipil digital melalui berbagai platform untuk mengorganisasi gerakan masyarakat sipil dan mengagitasi warga dunia terkait dengan isu yang sedang diperjuangkan.

Penggunaan ruang digital dan *platform* media sosial sebagai medium untuk mobilisasi kelompok kepentingan mendapat sorotan dari pemerintah dan negara. Tentu saja hal tersebut berimbas pada reaksi pemerintah untuk membuat peraturan atau regulasi yang memperketat penggunaan ruang digital. Misalnya saja Pemerintah Thailand yang akan memblokir Facebook untuk tidak lagi beroperasi di Thailand karena menilai Facebook berperan sebagai medium kritik kepada raja Thailand. Pemerintah Thailand mengumumkan bentuk hukuman pidana hingga 15 (lima belas) tahun hingga diasingkan apabila terdapat orang yang mengkritik, menghina maupun

memfitnah keluarga kerajaan. Tentu ini berlawanan dengan prinsip kebebasan berekspresi. Facebook mengakui bahwa kritik yang ditujukan kepada pemerintah atau raja Thailand tersebut merupakan bagian dari kebebasan berekspresi, sehingga tidak seharusnya dilarang. Di sisi lain, misalnya, warga Thailand juga memanfaatkan platform media sosial untuk menyebarkan kesadaran dan menaikkan pentingnya isu reformasi monarki Thailand. Hal tersebut membuat ribuan warga Thailand melakukan demonstrasi di jalanan selama beberapa hari.⁵

Tidak jauh berbeda dari Thailand, Indonesia juga beberapa kali memanfaatkan media sosial sebagai sarana untuk mengkonsolidasikan warga ke dalam gerakan yang sama, misalnya adalah gerakan #ReformasidiKorupsi pada tahun 2019 lalu. Aksi tersebut adalah bagian dari penolakan publik terkait dengan agenda legislasi DPR dan pemerintah terkait dengan tujuh tuntutan di antaranya adalah Revisi Undang-Undang Komisi Pemberantasan Korupsi yang dinilai dapat dilemahkan secara sistemik. Selain itu juga terdapat tuntutan untuk DPR segera mengesahkan RUU Perlindungan Pekerja Rumah Tangga dan RUU Penghapusan Kekerasan Seksual. Akibat hal tersebut, terdapat gejolak perlawanan yang dilakukan di berbagai kota di Indonesia, seperti di Jakarta, Bandung, Yogyakarta, Makassar, dan berbagai kota lainnya. Gelombang aksi kian membesar akibat adanya brutalitas aparat di berbagai kota di Indonesia, salah satunya di Kendari, Sulawesi Tenggara, dan menimbulkan dua korban jiwa dan menangkap ribuan demonstran di berbagai daerah.⁶

Tentu permasalahan tersebut juga berimbas pada kualitas demokrasi yang kian menurun. Bangkitnya otoritarianisme dan matinya demokrasi dalam sebuah negara menurut Levitsky dan Ziblatt (2018) setidaknya dicirikan melalui empat karakteristik atau

gejala, di antaranya adalah **(1)** negara atau pemerintah tidak memiliki komitmen untuk mempertahankan demokrasi; **(2)** penyerangan dan pemberangusan kelompok oposisi; **(3)** melegitimasi kekerasan dan brutalitas kepada masyarakat sipil; dan **(4)** pembatasan kebebasan terhadap masyarakat sipil.



Langkah awal Indonesia Mengatur Ruang Digital

Kenyataan saat ini hal yang terkait dengan penggunaan teknologi informasi tidak lagi dapat dilakukan pendekatan melalui sistem hukum konvensional. Hal ini mengingat aktivitas di ruang digital tidak bisa dibatasi oleh teritorial suatu negara, aksesnya dengan mudah dapat dilakukan dari belahan dunia manapun, kerugian dapat terjadi baik pada pelaku internet maupun orang lain yang tidak pernah berhubungan sekalipun.⁷

Memasuki tahun 2000an, Indonesia mulai mengatur serangkaian hal-hal yang menjadi hak ataupun perbuatan-perbuatan hukum. Pada awalnya, pengaturan ini berangkat dari perhatian mengenai penggunaan *e-commerce* dan keamanan data. Hubungan keperdataan dan *e-commerce* sebagai jalur niaga baru mengakibatkan diperlukannya perlindungan hukum yang progresif. Namun demikian, hal ini juga mengakibatkan bentuk pelanggaran hukum dalam transaksi perdagangan elektronik yakni tindakan seperti *carding*, *hacking*, *cracking*, *phishing*, *booting*, *viruses*, *cybersquatting*, pornografi, perjudian, penipuan, terorisme, dan penyebaran informasi destruktif (cara pembuatan dan penggunaan bom) telah menjadi bagian dari aktivitas perbuatan pelaku kejahatan internet dan Information and Communication Technology (ICT).⁸

Pemerintah Indonesia akhirnya membentuk pengaturan khusus untuk mengatur ruang

digital, yakni Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini berangkat dari rumusan masalah mengenai prinsip-prinsip regulasi internet, model pengaturan, materi muatan, instrumen internasional yang relevan, dan bentuk-bentuk pelanggaran di ruang digital.⁹ Akan tetapi, berjalannya implementasi undang-undang menghadapi tantangan dalam situasi demokrasi dan penjaminan hak asasi manusia karena penggunaannya yang berbeda dengan paradigma awal.

Di tahun yang sama, Indonesia juga membentuk undang-undang khusus yang mengatur mengenai pornografi, yaitu Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi (UU Pornografi). Undang-undang ini dibentuk dengan salah satu alasan bahwa aktivitas pembuatan, penyebarluasan dan penggunaan produk pornografi semakin mudah dengan perkembangan teknologi informasi dan komunikasi. Materi pornografi sebelumnya hanya diatur dalam konteks konvensional pada Kitab Undang-Undang Hukum Pidana (KUHP Lama), Undang-Undang Nomor 43 Tahun 1999 tentang Pers (UU Pers) berkaitan dengan kebebasan berekspresi dan menyatakan pendapat, Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak (UU Perlindungan Anak), Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran (UU Penyiaran), Undang-Undang Nomor 8 Tahun 1992 tentang Perfilman (UU Perfilman), Undang-Undang Nomor 32 Tahun 2004 tentang Pemerintahan Daerah (UU Pemerintahan Daerah Lama), Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (UU Kesehatan Lama), Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional (UU Sisdiknas), Undang-Undang Nomor 17 Tahun 2008 tentang Pelayaran (UU Pelayaran), dan Undang-Undang Nomor 17 Tahun 2006 tentang Kepabebean (UU Kepabebean).¹⁰

Seiring berkembangnya zaman, pengaturan di ruang digital juga ikut berkembang karena semakin variatifnya aktivitas di ruang *online*. Hingga saat ini, UU ITE mengalami perkembangan revisi sebanyak dua kali. Lalu, muncul juga undang-undang lainnya yang spesifik mengatur mengenai perlindungan data pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Undang-undang lain mengatur mengenai perlindungan kekerasan seksual yang meliputi ranah digital, yakni Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS). Selain itu, pembaruan hukum pidana juga mengakomodasikan kejahatan siber di Undang-Undang Nomor 1 tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru).

D. **Aktivisme dan Ruang Digital di Indonesia**

Peraturan mengenai penggunaan internet di Indonesia yang dianggap merepresi kebebasan masyarakat sipil membawa Indonesia pada kondisi demokrasi yang separuh bebas menurut Freedom House selama setidaknya tiga tahun terakhir. Indonesia mendapat skor sebesar 47 dari 100, berada di bawah Malaysia, Singapura, dan Filipina. Adapun yang memengaruhi skor tersebut di lingkup digital antara lain adalah hambatan akses informasi, batasan konten dan pelanggaran hak pengguna. Hal tersebut dibuktikan setidaknya dalam beberapa peristiwa, misalnya gangguan internet yang terus terjadi di Papua akibat dianggap aktivitas yang dianggap mengganggu keamanan dan stabilitas nasional. Selain itu, pada tahun 2022, pemerintah memblokir beberapa *platform* digital yang ada di Indonesia karena dianggap tidak memenuhi Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun

2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat (Permenkominfo tentang Penyelenggara Sistem Elektronik Lingkup Privat) yang mengatur tentang moderasi konten dan pembagian data pengguna kepada pemerintah.

Kemudian, pada akhir tahun 2022, pemerintah resmi mengesahkan KUHP Baru yang akan berlaku di tahun 2026 dengan menetapkan berbagai hukuman yang berkaitan dengan kampanye pada isu tertentu, misalnya adalah promosi aborsi, penghinaan hingga penyebaran informasi yang dianggap palsu. Pemerintah Indonesia juga tercatat melakukan manipulasi informasi dengan menggunakan *buzzer* (pendengung) atau *cyber troops* (pasukan siber) yang kian meningkat dan justru melakukan represi kepada masyarakat sipil melalui ujaran kebencian. Bahkan hingga saat ini, komitmen pemerintah hanya sebatas pada memblokir situs yang dianggap terlarang dan melakukan kriminalisasi kepada masyarakat sipil yang dianggap mengganggu keamanan dan stabilitas nasional.

Tidak berbeda dengan tahun sebelumnya, pada tahun 2023, demokrasi di ruang sipil digital juga mengalami penyusutan yang secara signifikan berpengaruh pada kondisi masyarakat sipil. Freedom House menyatakan pada tahun 2023, skor kebebasan di Indonesia hanya menyentuh 58 dari 100 dengan rincian hak politik mencapai skor 30 dari 40 dan kebebasan sipil yang hanya berada di angka 28 dari 60 poin. Angka tersebut menempatkan Indonesia berada pada kategori *partly free* atau demokrasi separuh bebas. Hal tersebut diakibatkan oleh beberapa faktor, di antaranya adakah pembatasan kebebasan berekspresi oleh berbagai regulasi, misalnya oleh UU ITE yang cakupannya juga merujuk pada pencemaran nama baik, tetapi rentan disalahgunakan oleh berbagai pihak. UU ITE juga dapat digunakan untuk mengkriminalisasi orang yang menyebarkan

informasi sensitif, bertentangan dengan moral dan norma bangsa, hingga dianggap mengancam keamanan dan stabilitas nasional. Selama lima tahun terakhir, Indonesia mengalami ancaman nyata, misalnya pembatasan akses internet di berbagai daerah, mulai di Papua pada 2019 dengan pemadaman internet secara total, disusul di beberapa daerah lain seperti Jakarta di tahun yang sama dan di Wadas, Purworejo pada tahun 2022 dengan model pembatasan internet secara parsial. Pembatasan di berbagai daerah tersebut dilakukan karena aktivitas yang dianggap mengancam stabilitas dan keamanan nasional dan mencegah penyebaran berita bohong.

“
Freedom House menyatakan pada tahun 2023, skor kebebasan di Indonesia hanya menyentuh 58 dari 100 dengan rincian hak politik mencapai skor 30 dari 40 dan kebebasan sipil yang hanya berada di angka 28 dari 60 poin. Angka tersebut menempatkan Indonesia berada pada kategori *partly free* atau demokrasi separuh bebas.

Berdasarkan laporan Amnesty Internasional, di Indonesia terjadi kriminalisasi pada 225 jurnalis sepanjang tahun 2019-2023. Padahal, jurnalis memainkan peran penting dalam ruang sipil, baik sebagai saluran informasi maupun sebagai alat untuk mengawasi pemerintah. Namun, media juga menghadapi tantangan seperti tekanan politik dan ekonomi, serta ancaman fisik.

Permenkominfo tentang Penyelenggara Sistem Elektronik Lingkup Privat juga memperjelas bagaimana negara melakukan pengawasan kepada masyarakat sipil dengan mengharuskan berbagai *platform* mendaftarkan layanannya kepada Kementerian Komunikasi dan Informasi.¹¹ Apabila *platform* tidak tunduk pada aturan tersebut, maka platform dan berbagai layanannya akan diblokir di Indonesia. Tentu ini berpotensi mengancam privasi masyarakat sipil di ruang digital. Berdasarkan laporan yang dibuat oleh Kepolisian Republik Indonesia (POLRI), di masa pandemi COVID-19, polisi virtual berhasil menjatuhkan sanksi kepada 200 netizen terkait dengan penyebaran informasi di ruang digital. Lebih jauh, apabila dikaitkan dengan kebebasan berekspresi, tentu ini adalah hal yang berlawanan dengan rasa aman dan hak mengemukakan pendapat di muka umum. Sanksi yang dijatuhkan beragam, mulai dari permintaan *takedown* hingga yang terparah adalah penjemputan paksa dan dijadikan tersangka, seperti pada kasus JERinx, vokalis grup musik Superman is Dead.

Pada tahun 2024, gangguan sistem Pusat Data Nasional Sementara yang diakibatkan oleh peretasan dan mengakibatkan kebocoran data secara masal dan masif di berbagai instansi. Respon pemerintah dalam menghadapi situasi tersebut cenderung menganggap remeh, sehingga data pribadi masyarakat diperjualbelikan di forum *dark web* dan pemulihan data pribadi yang berhasil dilakukan hanya mencapai 2% (dua persen) dari keseluruhan data yang bocor

tersebut. Kasus-kasus dugaan kebocoran data yang melibatkan institusi pemerintahan seperti registrasi prabayar nomor layanan telekomunikasi seluler, hingga kebocoran 34 juta data paspor Indonesia yang diperjualbelikan di situs daring, menjadi bagian pertanyaan besar mengenai kemampuan tata kelola PDN dalam menjaga keamanan data-data yang disimpan secara sepihak oleh pemerintah pusat.

Regulasi internet yang ideal masih belum dapat dicapai dalam waktu yang singkat apabila dikaitkan dengan konteks di Indonesia. Bukan tanpa alasan, pasalnya pemerintah Indonesia belum memiliki komitmen sungguh-sungguh terkait dengan berbagai aspek, misalnya perlindungan data pribadi. SAFEnet (2024) menemukan imbas dari gangguan dan kebocoran data Pusat Data Nasional (PDN) terdapat setidaknya 32 (tiga puluh dua) insiden kebocoran data yang terjadi di lembaga pemerintah, di antaranya adalah BPJS Kesehatan, POLRI, Komisi Pemilihan Umum, dan Kementerian Pertahanan. Pun demikian, pemerintah seolah tidak memiliki mekanisme pemulihan dan penanganan yang jelas. Hal ini membuktikan tidak adanya komitmen dan konsistensi pemerintah dalam niatnya untuk membangun infrastruktur digital yang sebelumnya diklaim menerapkan standar yang tinggi. Padahal, akibat dari gangguan dan kebocoran PDN tersebut berimbas kepada jutaan masyarakat, misalnya adalah keterlambatan pengumuman Beasiswa KIP-K kepada sekitar 800ribu penerima beasiswa, sehingga di beberapa perguruan tinggi, mereka harus mengurus dan menyiapkan berkas secara luring.¹²

Legitimasi pemerintah melalui undang-undang terkait pembatasan kebebasan berekspresi masyarakat di ruang sipil merupakan bagian dari otoritarianisme digital. Hal ini menjadi catatan penting, pasalnya, tren otoritarianisme digital juga bisa dilakukan di negara demokrasi seperti

Indonesia. Secara umum, praktik otoritarianisme digital ditandai dengan empat taktik yang paling umum dilakukan, *pertama*, pengawasan atau *surveillance*, hal ini ditandai dengan adanya teknologi digital yang digunakan untuk mengawasi masyarakat dan difasilitasi oleh pemerintah. *Kedua*, serangan siber, secara teknis seperti peretasan, *phishing*, *malware*, *ransomware*, dan gangguan jaringan internet. *Ketiga*, pembatasan akses internet, teknik ini dapat dilakukan secara parsial atau dilakukan dengan membatasi akses internet secara total. Pembatasan internet juga berkaitan dengan pembatasan masyarakat terhadap sumber data. *Keempat* adalah manipulasi dan propaganda, teknik ini biasanya digunakan dengan memproduksi dan mereproduksi misinformasi, disinformasi, atau malinformasi, sehingga opini publik dapat dikendalikan dan dialihkan dari isu substansi.¹⁵

Dengan serangkaian permasalahan yang diuraikan di atas, studi ini akan mencoba menjawab memetakan peta regulasi internet atau ruang digital yang sudah ada di Indonesia, implementasi peta regulasi tersebut apabila ditinjau dari prinsip tata kelola internet dan The Charter of Human Rights and Principles for the Internet (ICRP), serta menghasilkan rekomendasi bagaimana secara ideal tata kelola internet diatur.

Hak Digital untuk
Demokrasi dan
Civic Space:

Studi Pemetaan Regulasi
Internet di Indonesia

02

Metode Penelitian

2. Metode Penelitian

“
Penelitian ini menggunakan tiga metode, yaitu regulatory gap analysis (analisis kesenjangan kebijakan), studi literatur, dan studi kasus selektif.

Analisis kesenjangan kebijakan dilakukan untuk menilai kesesuaian antara regulasi internet Indonesia dengan acuan ICRP yang fokus pada hak untuk hidup, kebebasan, dan keamanan (*the right to life, liberty, and security*). Pendekatan ini membantu untuk mengidentifikasi area pengaturan yang sudah baik dan yang perlu diperbaiki. Analisis kesenjangan kebijakan dilakukan dengan terlebih dahulu melakukan inventarisasi terhadap peraturan perundang-undangan yang mengatur tentang internet dan ruang digital, dalam hal ini, kami membatasi pada level undang-undang. Kemudian, kami melakukan analisis pasal per pasal undang-undang yang telah diinventarisasi, dengan terlebih dahulu mengelompokkan pengaturan yang mengandung materi yang melindungi, menjamin, dan menghormati hak asasi manusia pada aspek: (1) akses internet; (2) proteksi dan keamanan digital; dan (3) kebebasan berekspresi. Peneliti menyadari bahwa tiga aspek ini saling terkait karena suatu ketentuan kerap berisi lebih dari satu aspek. Ketentuan tersebut kemudian dikelompokkan berdasarkan aspek yang paling dominan melekat pada ketentuan tersebut. Ketiga aspek tersebut merupakan aspek mendasar tata kelola internet yang dikristalkan dari ICRP. Berdasarkan ketiga aspek tersebut, kami menentukan prinsip-prinsip ideal dari tiap pengaturan. Kemudian, berdasarkan pasal-pasal yang telah dikelompokkan dianalisis sesuai dengan prinsip-prinsip ideal yang telah ditentukan. Hasil analisis pasal per pasal menjadi rekomendasi bagi pembentukan aturan ideal tata kelola internet. Pada studi literatur, kami menganalisis sumber hukum sekunder, seperti buku, artikel jurnal, laporan studi lembaga riset, berita, dan sebagainya. Pada studi kasus selektif, kami memilih sejumlah kasus yang relevan

dengan implementasi hukum terkait tata kelola internet dan perlindungan terhadap hak asasi manusia di ruang digital maupun eskalasi kasus di ruang digital yang berdampak pada ruang fisik. Studi kasus selektif ditujukan untuk memperoleh

gambaran yang lebih mendalam tentang jaminan dan perlindungan hak digital dan proses penegakan hukumnya. Riset dilakukan dengan menjalankan alur sebagai berikut:

1. Identifikasi Masalah

Tahap yang pertama dalam penelitian ini adalah mengidentifikasi persoalan yang tengah dihadapi pada pengaturan hukum di ruang digital. Tahap ini dilakukan dengan cara mengamati, memahami, dan menganalisis masalah yang ada hingga menentukan topik penelitian agar relevan dan menjawab persoalan penting pada realitas hari ini.

2. Penyusunan Kajian Awal

Setelah mengidentifikasi masalah, dilakukan sebuah tinjauan awal untuk memahami konsep dasar dan penyatuan pandangan mengenai topik penelitian yang diangkat. Tinjauan awal ini dilakukan melalui studi literatur dan *focus group discussion* sebanyak satu kali bersama organisasi masyarakat sipil dan konsinyering sebanyak dua kali dengan para ahli di bidang tata kelola internet.

3. Penentuan batasan dan benchmark penelitian

Tahap ini menentukan batasan-batasan penelitian yang dipertimbangkan berdasarkan informasi dan pemahaman konsep serta keterbatasan yang didapatkan pada tahap penyusunan kajian awal. Batasan tersebut mencakup pemetaan terhadap regulasi pada tingkat undang-undang, cakupan tata kelola internet yang dianalisa dalam laporan ini, dan penentuan analisis data dengan melandaskan pada tiga prinsip tata kelola internet pada *The Charter of Human Rights and Principles for the Internet* (ICRP).

4. Pengumpulan dan pengolahan data

Pengumpulan dan pengolahan data dilakukan dengan memetakan peraturan perundang-undangan terkait tata kelola internet dan memilah kasus untuk melihat implementasi prinsip-prinsip tata kelola internet, yaitu (1) akses internet; (2) proteksi dan keamanan digital; dan (3) kebebasan berekspresi.

5. Analisis Data

Analisis data yang dilakukan pada penelitian ini menggunakan *mix method* (metode campuran). Metode ini menggabungkan metode kualitatif dan metode kuantitatif.

6. Paparan temuan awal untuk memperoleh masukan ahli dan masyarakat sipil

Temuan awal ini dipaparkan pada sebuah forum diskusi yang mengundang ahli akademisi dan praktisi mengenai tata kelola internet yang berkaitan dengan hak asasi manusia dan *civic space* (ruang gerak masyarakat sipil). Forum ini juga mengundang masyarakat sipil lintas sektor untuk mengumpulkan tanggapan serta masukan pada sektor masing-masing yang berkaitan dengan tata kelola internet.

7. Perbaikan Naskah

Pada tahap ini, kami menganalisis kembali masukan dan temuan pasca forum terbuka untuk menyempurnakan draf penelitian.

8. Merumuskan kesimpulan dan rekomendasi

Pada tahap ini, kami merumuskan kesimpulan dan rekomendasi untuk perbaikan regulasi tata kelola internet ke depan.

Hak Digital untuk
Demokrasi dan
Civic Space:

Studi Pemetaan Regulasi
Internet di Indonesia

03

Paradigma Pengaturan Tata Kelola Internet dan Ruang Digital

3. Paradigma Pengaturan Tata Kelola Internet dan Ruang Digital

A. Paradigma Umum

Secara umum terdapat dua pandangan terhadap pengaturan dunia digital, yaitu tidak mungkin diatur dan dapat diatur. Paradigma *pertama* memandang internet memiliki banyak lapisan dan jejaring jaringan yang kompleks, sehingga mengatur internet sepenuhnya mustahil karena hukum dan peraturan hanya dapat menysasar perilaku individu manusia.¹⁴ Oleh karena itu, pengaturan internet adalah jalan pintas linguistik untuk menggambarkan sebuah upaya berkelanjutan dan fokus untuk mengubah tindakan individu yang terkait dengan internet, termasuk penetapan standar, pengumpulan informasi, dan modifikasi perilaku.¹⁵

Paradigma *kedua* memandang internet dapat diatur karena mengartikan pengaturan tidak sekedar legislasi, melainkan mencakup semua jenis standar pengaturan (*standard settings*), insentif, dan pengaturan mandiri.¹⁶ Stuart Biegler mengatakan dalam menanggapi masalah perlu mempertimbangkan pendekatan-pendekatan pengaturan (*regulatory*) termasuk litigasi, legislasi, perubahan kebijakan, aktivitas badan

administrasi, kerja sama internasional, perubahan arsitektur, pengaturan swasta, dan pengaturan mandiri.¹⁷

Pembedaan paradigma juga dapat melalui melalui intensi pembuat aturan, mekanisme dalam peraturan dan intensitas peraturan.¹⁸ Intensi atau maksud pembuat aturan terbagi dalam dua kategori. *Pertama*, mencoba menegakkan tujuan regulasi yang telah ada sebelumnya di dunia luring. Bentuknya antara lain mencoba mentransfer atau memperluas kategori regulasi sebelum internet, atau menarget bentuk-bentuk perilaku tertentu di dunia digital. Contohnya adalah mengenai perlindungan hak milik, yaitu menganggap nama domain, akun Facebook (Meta), atau informasi pribadi seseorang sebagai hak milik seperti halnya rumah.¹⁹ Pendekatan yang berkebalikan adalah mencoba menemukan hak individu yang khusus untuk era digital seperti hak-hak individu untuk privasi digital, keamanan teknologi informasi, dan netralitas jaringan, bentuk-bentuk penyaringan juga pemblokiran internet dan teknologi.²⁰

Paradigma terkait mekanisme²¹ terdiri dari tiga bentuk sebagai berikut:

- a.** Pengaturan langsung: negara memberi wewenang kepada sebuah organ hukum untuk membuat peraturan, merawat, memantau, dan menegakkannya;

- b.** Pengaturan bersama: suatu badan negara, yang memiliki wewenang pengaturan menurut undang-undang, mendelegasikan tanggung jawab kepada industri yang relevan untuk memelihara dan menerapkan kode etik yang telah disetujui oleh regulator menurut undang-undang, dan terus mengawasi pengaturan bersama, dengan tetap memiliki wewenang untuk melakukan intervensi jika diperlukan; dan

- c.** Pengaturan mandiri: Sekelompok perusahaan atau individu memiliki kendali atas keanggotaan dan perilaku mereka sendiri. Keanggotaan bersifat sukarela, dan para peserta menyusun aturan mereka sendiri dengan menggunakan perangkat seperti kode etik, serta solusi dan standar teknologi. Para anggota bertanggung jawab penuh atas pemantauan dan kepatuhan tanpa mengacu pada otoritas pengatur hukum.

“
Untuk menyingkirkan kemungkinan miskonsepsi, tata kelola internet tidak hanya tentang nama domain ataupun institusi dan *United Nations Internet Governance Forum (IGF)*.²³ Tata kelola internet pada umumnya merujuk pada kebijakan atau koordinasi teknis atas pertukaran informasi yang terjadi di internet.”

Cakupan tentang pengaturan internet dapat berbeda-beda antara satu penulis dengan lainnya. Laura De Nardis dalam *The Emerging Field of Internet Governance* mengenalkan lima topik untuk pengaturan internet, yaitu **(1)** sumber daya internet yang penting; **(2)** protokol internet; **(3)** hak kekayaan intelektual terkait tata kelola internet; **(4)** keamanan dan manajemen infrastruktur; dan **(5)** hak komunikasi.²² Untuk menyingkirkan kemungkinan miskonsepsi, tata kelola internet tidak hanya tentang nama domain ataupun institusi dan *United Nations Internet Governance Forum (IGF)*.²³ Tata kelola internet pada umumnya merujuk pada kebijakan atau koordinasi teknis atas pertukaran informasi yang terjadi di internet.²⁴

William H. Dutton dan Malcolm Peltu membuat kategori tentang isu pengaturan internet sebagai berikut:²⁵

No	Jenis	Isu Penting	Contoh
1.	Internet sebagai pusat	Pengembangan infrastruktur teknis inti internet serta standar dan protokol web. Mempertahankan operasi internet yang efisien dan andal serta kemampuan beradaptasi yang tepat waktu terhadap perubahan teknologi dan perubahan lainnya yang terus berlanjut dan sering kali cepat yang memengaruhi internet.	Penetapan standar untuk internet dan <i>World Wide Web</i> , menetapkan alamat Internet, menentukan rute pesan antara pengirim dan penerima operasi internet yang lancar dan aman, serta pengembangan sistem dan layanan inti.
2.	Pengguna internet sebagai pusat	Bagaimana penggunaan atau penyalahgunaan Internet oleh individu, kelompok, dan organisasi (baik yang legal maupun ilegal, perilaku yang pantas maupun tidak pantas) didefinisikan dan diatur. Berhubungan dengan kebijakan yang umumnya ditetapkan oleh yurisdiksi lokal, regional, dan nasional, dengan aspek internasional yang dikembangkan melalui komunikasi dan negosiasi di antara yurisdiksi.	Email " <i>spam</i> " yang tidak diminta, pelanggaran privasi pengguna, perlindungan data, penipuan dan kejahatan siber lainnya, serangan jahat terhadap stabilitas atau keamanan sistem di Internet, penggunaan " <i>chat room</i> " di internet oleh para pedofil untuk menghubungi anak-anak muda, paparan yang tidak diinginkan terhadap konten web yang berbau pornografi.
3.	Internet bukan sebagai pusat	Kebijakan dan praktik yang ada di badan dan yurisdiksi tidak secara khusus menangani masalah-masalah yang berhubungan dengan internet. Menyediakan konteks kebijakan lokal dan internasional, yaitu perkembangan infrastruktur dan penggunaan internet bersinggungan dengan proses tata kelola yang lebih luas yang membentuk kebijakan yang lebih rinci terkait internet.	Ekspresi politik, penyensoran, hak cipta, hak kekayaan intelektual (HAKI), merek dagang, menutup kesenjangan digital, memenuhi MDGs, keragaman budaya dan bahasa, serta menyebarkan konten melalui operator telekomunikasi.

Desain internet dan prinsip-prinsip tata kelola yang baik dapat merujuk pada pemetaan di bawah ini:²⁶

No	Prinsip	Desain Internet	Tata kelola yang Berpusat pada Internet	Aspek Tata Kelola yang Lebih Luar
1.	Optimalisasi untuk adaptasi apabila terjadi perubahan yang tidak terprediksi	Arsitektur inti minimal untuk mengakomodasi aplikasi dan inovasi teknologi	Tidak membahayakan arsitektur inti, prinsip-prinsip lembaga yang lincah untuk tanggapan yang tepat waktu terhadap perubahan pengguna dan teknologi komunikasi internet	<ul style="list-style-type: none"> • Sentuhan regulasi ringan yang tidak mengancam pertumbuhan Internet. • Tanggapan yang tepat waktu terhadap perubahan sosial, ekonomi, budaya, dan teknis
2.	Independen	Tidak ada kontrol pusat atau penjaga gerbang komunikasi yang dominan	Pengambilan keputusan yang dilimpahkan, mandiri, dari bawah ke atas, bertanggung jawab kepada komunitas internet, dan tidak ada pemangku kepentingan yang dominan	<ul style="list-style-type: none"> • Tidak ada pemangku kepentingan yang dominan • Dukungan untuk otonomi pengguna dan keragaman kreatif, budaya, bahasa, dan aplikasi
3.	Terbuka	Ketersediaan standar dan protokol inti internet, serta aplikasi dan konten independen	Pluralistik, transparan, kolaboratif, proses bersama ragam <i>stakeholder</i> publik dan privat, keterbukaan terhadap pasar terkait internet	<ul style="list-style-type: none"> • Proses multipihak yang transparan • Akses internet yang luas dengan biaya yang wajar • Peningkatan kapasitas manusia • Konsep <i>open society</i>, seperti kebebasan berpendapat

4. Interoperabilitas ujung ke ujung (End-to-end interoperability)

Transfer paket data tanpa batas dari pengirim ke penerima, serta konten, aplikasi, pengguna, dan teknologi independen

Pelindungan *end-to-end* secara global dan menghindari sekat interoperabilitas secara teknis dan regulasi

Memprioritaskan prinsip *end-to-end* dalam tata kelola internet internasional, sembari mengakui hak dan tanggung jawab nasional

5. Subsidiaritas: keputusan pada tingkat yang paling tepat dan efisien

Kepemilikan bersama atas arsitektur inti oleh komunitas internet secara keseluruhan

Koordinasi yang efisien untuk proses kolaboratif yang terdesentralisasi

Berbagai model untuk berbagai isu dan koordinasi global yang efisien untuk menghindari fragmentasi mosaik tata kelola

6. Secara operasional pragmatis

Pengoperasian arsitektur inti yang stabil, aman, dan efisien

Fokus pada apa yang berhasil dalam mempertahankan integritas dan kinerja arsitektur inti

Tidak ada ancaman terhadap operasi internet yang berkelanjutan dan tata kelola dengan dukungan dari yang diatur

Terdapat pula ketegangan yang timbul dari prinsip-prinsip tata kelola dan kepentingan yang saling bersaing, yaitu:²⁷

No	Jenis	Deskripsi	Contoh/Potensi Solusi
1.	Demokrasi-kecepatan	Upaya untuk membuat tata kelola internet menjadi lebih demokratis, akuntabel, dan transparan dapat menangkal kebutuhan akan tanggapan yang tepat waktu terhadap perubahan teknologi komunikasi internet dan internet yang cepat	Dahulu, beberapa ahli dapat memutuskan standar internet dan menerapkannya dengan cepat. Sekarang, seratus kelompok kerja IETF dan ribuan ahli terlibat. Kesulitan dalam mengimplementasikan perubahan yang menantang investasi pengguna dan industri teknologi komunikasi internet yang substansial ditunjukkan oleh penundaan dalam memperkenalkan versi Internet terbaru, IPv6 (Dutton 2004b)
2.	Privasi-kepercayaan	Desain terbuka memungkinkan kreativitas pengguna yang memberikan nilai khusus pada internet, tetapi juga merusak kepercayaan dunia maya dengan memungkinkan penyusupan jahat. Mekanisme perlindungan pengguna dapat menghambat inovasi dan mengancam privasi pribadi	Katz berpendapat bahwa peningkatan identifikasi pengguna sebagai mekanisme perlindungan harus disertai dengan pembatasan yang kuat dalam menghubungkan identitas pengguna dengan sumber informasi lain. Crocker menyarankan sebuah kompromi: membatasi jumlah identifikasi yang diperlukan untuk kegiatan yang berbeda untuk memungkinkan respon yang proporsional, tergantung pada jenis ancaman
3.	Subsidiaritas-fragmentasi	Fragmentasi antara para ahli dan lembaga dapat terjadi akibat pengambilan keputusan yang didelegasikan oleh pihak-pihak yang paling dekat dengan suatu masalah, yang mengarah pada koordinasi dan pengawasan yang tidak efisien dan ancaman terhadap kedaulatan nasional	Proses Uniform Domain-Name Dispute-Resolution Policy (UDRP) untuk cybersquatting yang dirumuskan oleh World Intellectual Property Organization (WIPO) dan diimplementasikan oleh Internet Corporation for Assigned Names and Numbers (ICANN) mengilustrasikan bagaimana proses tata kelola dapat disepakati meskipun terdapat fragmentasi tanggung jawab (Jones 2005). Meningkatnya jumlah Kelompok Kerja Internet Engineering Task Force (IETF) mengindikasikan meningkatnya fragmentasi di tingkat Tipe I yang berpusat pada Internet

4. **Konsensus- persaingan**

Proses multipemangku kepentingan dan multikelembagaan dapat menciptakan ketegangan di antara para pelaku yang memiliki tujuan yang berbeda ketika mereka bersaing dan bekerja sama untuk mencapai tujuan mereka sendiri sambil menegosiasikan konsensus tentang tujuan yang lebih luas

Bradner menyoroti ketegangan yang muncul dari model bisnis operator telekomunikasi yang mencari keuntungan dari konten yang berjalan di jaringan mereka. Lucinda Jones dari WIPO menunjukkan manfaat yang diperoleh dari tujuan bersama, seperti keinginan penyedia konten untuk menyediakan konten secara aman melalui jaringan yang diperluas untuk menjangkau lebih banyak konsumen

5. **Komunal- perdagangan**

Konsep awal dari “informasi global bersama” yang dapat diakses secara terbuka di internet ditantang oleh meningkatnya komersialisasi konten di pasar internet terbuka

Melindungi dan mengenakan biaya untuk konten telah menjadi semakin umum seiring dengan meningkatnya nilai internet sebagai sumber daya global. Namun demikian, bentuk-bentuk baru “lisensi permisif” mulai bermunculan di mana pengarang dan pencipta membuat karya mereka tersedia secara lebih terbuka dengan tetap mempertahankan beberapa kepemilikan dan kontrol (Uhlir 2005: 60-61)

Berikut merupakan gambaran aktor-aktor terkait, objek yang dikelola, serta tujuan dan sasaran yang akan dicapai dari tiap-tiap “pemain”:²⁸

No	Jenis	Lingkup Permainan	Pemain Utama	Tujuan (<i>Goal</i>) dan Sasaran (<i>Objectives</i>)
1.	Berpusat pada internet (<i>Internet centric</i>)	Yurisdiksi trans-nasional berupa “perebutan wilayah”	Pemerintah, entitas regional (misalnya, European Union), lembaga tata kelola pemerintah (misalnya, ICANN, ITU, UN, WIPO, WGIG), ahli-ahli	Aktor nasional dan aktor lain berpartisipasi dalam badan tata kelola untuk mendapatkan atau mempertahankan, membatasi, atau memperluas kendali atas sumber daya internet, seperti atas <i>server root</i>
		Nama-nama dan angka	Ahli-ahli individu, ICANN, Pendaftar (<i>registries</i>), <i>Internet Service Providers</i> (ISPs), pengguna	Mendapatkan, menjual, dan mengalokasikan nama domain, dll. untuk mengidentifikasi situs, <i>server</i> , dan pengguna
		Standar	Badan-badan yang mengatur standar, IETF, W3C	Menetapkan dan menyebarkan standar internet
2.	Berpusat pada pengguna internet (<i>internet user centric</i>)	Pelindungan konsumen	konsumen, kelompok konsumen, <i>supplier</i> , pembuat peraturan, <i>spammers</i> , telemarketers	Legislator, regulator menanggapi pandangan dan kepentingan yang saling bersaing dan saling melengkapi
		Privasi dan perlindungan data	Pemerintah, warga negara, pembuat peraturan, firma swasta, pengacara, jurnalis, aktivis kebebasan sipil	Pemain mencegah atau mengupayakan pengungkapan data pribadi tergantung pada kriteria yang dinegosiasikan atau diberlakukan

3.

**Tidak berpusat
pada Internet
(non-internet
centric)**

Hak cipta, hak digital, manajemen

DPR dan pembuat peraturan, penyedia konten, penyedia (supplier) media dan telekomunikasi, penyedia layanan akses online ke konten, vendor ICT

Konsumen mencari akses online berbiaya rendah ke konten. Pencipta, pemasok mencoba memanfaatkan aset mereka. Pemilik konten, pemasok, pengguna, legislator menegosiasikan persyaratan akses dan hak

Kemerdekaan berekspresi

Aktivis politik dan keagamaan, penulis, seniman, pembela hak media, media berita, blogger, pemerintah, penyensor

Individu, kelompok, organisasi bertujuan untuk memfasilitasi atau membatasi ekspresi dan pertukaran sudut pandang tertentu

Kesenjangan digital

Pemerintah, ornop, aktivis lokal, kelompok kepentingan khusus, komunitas lokal, investor

Para pemain berusaha untuk menutup kesenjangan sosial, ekonomi, dan lainnya dengan bantuan infrastruktur terkait teknologi komunikasi internet, penggunaan, dan pengembangan kapasitas manusia

B.

Model Pengaturan Internet Berdasarkan Sejarah

Pengaturan internet berdasarkan kesejarahan dapat dibagi dalam empat fase.²⁹ Fase pertama adalah masa keterbukaan internet (*open internet*) dari kelahiran internet hingga tahun 2000. Fase kedua adalah penolakan terhadap akses (*access denied*) hingga tahun 2005. Fase ketiga adalah kontrol terhadap akses (*access controlled*) hingga tahun 2010. Terakhir adalah kontestasi akses (*access contested*), yaitu masa sekarang.

Fase pertama yaitu keterbukaan internet memiliki makna deskriptif, prediktif, dan normatif.³⁰ Pemikiran dominan dalam fase ini adalah internet merupakan ruang yang terpisah, sering disebut *cyberspace*. Dalam makna deskriptif, hingga akhir 1990-an, sebagian besar negara cenderung mengabaikan aktivitas *online* atau mengaturnya dengan sangat sedikit. Mereka juga cenderung memikirkan dan memperlakukannya dengan sangat berbeda dari aktivitas di ruang nyata. Dalam makna prediksi, istilah keterbukaan internet terbukti tidak akurat, sedangkan sebagai definisi normatif, tetap penting mempertahankan konsep ini. Masih ada hal penting dari konsep internet terbuka yang perlu terus diingat.³¹

Makna deskriptif internet terbuka sudah lama lewat, tetapi unsur-unsur penting dari teori dibaliknya terus bertahan. Contohnya adalah internet memungkinkan kita untuk mendengar lebih banyak pernyataan dari lebih banyak orang daripada sebelumnya. Internet memberikan kebebasan yang lebih besar daripada sebelumnya, terutama dalam rezim tertutup, negara mengontrol apa yang dapat didengar atau tidak oleh warganya. Pemerintah juga dapat menggunakan teknologi ini untuk menjadi lebih terbuka dan

lebih transparan dalam kerjanya.³²

Fase kedua kira-kira terjadi pada tahun 2000-2005. Pada masa ini, negara dan pihak-pihak lain mulai berpikir bahwa aktivitas dan ekspresi di internet merupakan sesuatu yang perlu diblokir atau diatur dengan berbagai cara. Pemikirannya adalah bahwa tindakan-tindakan tertentu dalam berbicara dan berorganisasi secara *online* perlu diatur seperti hal lainnya.³³

Penyaringan di internet dengan cakupan serta tingkat efektivitas yang berbeda-beda terjadi secara luas di berbagai negara. Tiongkok adalah rezim penyaringan yang paling rumit di dunia, dengan pemblokiran yang terjadi di berbagai tingkat jaringan dan mencakup konten yang menjangkau berbagai bidang topik. Singapura memblokir akses hanya ke beberapa situs-situs salinan elektronik, yang semuanya bersifat pornografi.³⁴

Beberapa negara menerapkan aplikasi perangkat lunak. Penyaringan ini ada yang berdasarkan hukum dan untuk negara lain melalui otoritas keamanan nasional. Peraturan penyaringan ini terkadang hanya menyebutkan sebagai hal yang diperbolehkan. Konten yang diblokir mencakup berbagai macam informasi sosial, agama, dan politik.³⁵

Fenomena penyaringan ini menunjukkan bahwa penyaringan internet tidak hanya terjadi di negara-negara otoriter. Negara-negara demokratis juga melakukan pengaturan internet yang luas, seperti di Eropa Utara terhadap pengaturan pornografi. Amerika Serikat mengatur apa yang bisa dilihat anak-anak di perpustakaan dan sekolah, sebagai salah satu cara untuk membatasi akses ke informasi yang

dianggap berbahaya bagi mereka.³⁶ Pemblokiran untuk alasan perlindungan anak berbeda dengan penyaringan terhadap kebebasan berpendapat, tetapi mekanisme teknis keduanya serupa.³⁷

Fase ketiga adalah kontrol terhadap akses yang terjadi sekitar 2005 hingga 2010. Ciri periode ini adalah negara telah membuat peraturan yang berfungsi tidak hanya seperti filter atau blok, tetapi juga sebagai kontrol variabel. Gagasan utama periode ini adalah ada serangkaian besar mekanisme, di berbagai titik kontrol, yang dapat digunakan untuk membatasi akses terhadap pengetahuan dan informasi.³⁸ Negara kemudian menyadari tidak dapat menerapkan tingkat kontrol yang mereka cari atas aktivitas jaringan secara langsung. Akibatnya, negara memperluas cakupan strategi kontrolnya kepada pihak swasta.³⁹

Fase keempat adalah kontestasi akses yang dimulai dari tahun 2010 hingga saat ini. Gagasan utama tahap ini adalah bahwa ada, dan akan ada lebih banyak lagi, penolakan terhadap beberapa kontrol. Ada pertarungan yang sedang berlangsung tentang seperti apa lingkungan digital ini nantinya. Ada perdebatan politik yang berkembang tentang cara peraturan yang dilakukan oleh negara-negara di seluruh dunia. Pada tingkat negara ke negara, proses militerisasi dunia maya yang telah terjadi selama beberapa tahun terakhir adalah bagian penting dari bagian penting dari narasi yang muncul ini. Meningkatnya aktivitas online sebagai hal penting dalam kehidupan secara umum adalah pendorong utama dari fase ini.⁴⁰

Masa ini ditandai munculnya tanggapan yang kuat dari sektor swasta dan dari negara bagian lain yang tidak setuju dengan peraturan yang mengontrol internet. Perusahaan-perusahaan menerapkan strategi baru untuk mengatasi banyaknya regulasi dan tanggung jawab yang mereka hadapi sebagai perantara internet. Dalam

menanggapi tekanan yang meningkat dari negara-negara, termasuk Tiongkok dan Vietnam, perusahaan-perusahaan seperti Google, Microsoft, dan Yahoo! telah bergabung bersama dengan kelompok-kelompok hak asasi manusia dan akademisi untuk mendirikan sebuah organisasi, Global Network Initiative. Organisasi ini membantu menerapkan kode etik untuk menangani tuntutan terhadap internet dengan cara yang menjunjung tinggi kebebasan sipil.⁴¹

Kontestasi ini juga terlihat dari cara pandang dan aktivitas negara-negara. Para pejabat militer semakin menganggap lingkungan digital sebagai domain strategis dan zona peperangan yang potensial.⁴² Reaksi publik terhadap regulasi internet juga menunjukkan kontestasi di arena publik di seluruh dunia. Salah satu kasusnya adalah para demonstran di Pakistan pada tahun 2010 menyatakan dengan jelas ketidaksetujuan mereka terhadap keputusan negara untuk meningkatkan pemblokiran internet.⁴³

“
Pertanyaan tentang masa depan regulasi internet adalah tidak menanyakan apakah Internet dapat diatur. Pertanyaan seharusnya adalah apakah internet akan diatur dengan cara yang persis sama, atau lebih luas, daripada dunia offline sebagai akibat dari kontestasi yang meningkat di era perebutan akses.”⁴⁴

04

**Prinsip Tata
Kelola Internet
dalam The
Charter of Human
Rights and
Principles for the
Internet**

4. Prinsip Tata Kelola Internet dalam The Charter of Human Rights and Principles for the Internet

“*The Charter of Human Rights and Principles for the Internet (Piagam Hak Asasi Manusia dan Prinsip-prinsip untuk Internet / ICRP) disusun oleh Internet Rights & Principles Dynamic Coalition (Koalisi IRP), yaitu sebuah jaringan internasional yang bekerja untuk menjunjung tinggi hak asasi manusia (HAM) di lingkungan online (dalam jaringan) dan di seluruh domain pengambilan kebijakan internet.*”

Koalisi ini didasarkan pada United Nations Internet Governance Forum untuk membahas hal-hal yang berkaitan dengan tata kelola internet bersama-sama.⁴⁵

Selama tahun 2009 dan 2010, draf awal piagam ini disempurnakan dan ditinjau oleh sekelompok pakar HAM untuk memastikan bahwa piagam tersebut sesuai dengan standar HAM internasional. Draft akhir versi yang ada saat ini (disebut versi 1.1), dibuka untuk konsultasi yang lebih luas dalam Internet Governance Forum (IGF) dan oleh komentator eksternal beberapa bulan setelah draft pertama (versi 1.0) yang dirilis pada pertemuan IGF 2010 di Vilnius, Lithuania. Pada pertemuan ini, sebuah kelompok kerja dibentuk untuk meringkas piagam yang awalnya panjang dan rumit secara hukum, menjadi format yang lebih mudah diakses untuk penjangkauan, pendidikan, dan advokasi. Hasilnya adalah “*Ten Punchy Principles*” atau “Sepuluh Prinsip yang Menonjol” yang diluncurkan secara *online* pada tahun 2011. Prinsip-prinsip tersebut selanjutnya disebut sebagai “*10 Internet Rights and Principles*” (IRP) Charter.⁴⁶

Piagam ini menyadarkan bahwa banyak sekali orang di seluruh dunia yang saat ini bergantung pada internet, termasuk dalam mengekspresikan dirinya serta sebagai sarana untuk melindungi hak asasi manusia mereka. Oleh karena itu, hak untuk mengakses dan menggunakan internet harus dipertimbangkan sebagai bagian dari HAM. Pemerintah maupun pihak swasta yang

menghambat kemampuan orang untuk mengakses dan/atau menggunakan internet tidak hanya menghilangkan kemudahan bagi mereka, tetapi juga merampas sesuatu yang jauh lebih mendasar. Internet adalah milik seluruh umat manusia, dan merupakan hak bagi setiap orang untuk memiliki tempat di dalamnya.⁴⁷

Piagam tersebut mencakup keseluruhan langkah-langkah terkait hak asasi manusia yang diambil dari Deklarasi Universal Hak Asasi Manusia (DUHAM) dan kovenan-kovenan lainnya yang membentuk “The International Bill of Human Rights at the United Nations”. Piagam tersebut didasarkan pada HAM yang sudah ada dan dalam praktiknya, sebagian besar ketentuan di dalamnya hanya akan mengikat negara. Namun, terdapat pengakuan yang semakin berkembang bahwa sektor swasta mempunyai kewajiban berdasarkan hukum HAM.

Penelitian ini menggunakan ICRP sebagai tolok ukur analisis atas sejumlah pertimbangan. *Pertama*, ICRP secara khusus mengonstruksikan jaminan, perlindungan, dan pemenuhan hak asasi manusia dengan hak digital yang merupakan turunan dari *Universal Declaration of Human Rights* (UDHR), *International Covenant on Civil and Political Rights* (ICCPR), *International Covenant on Economic, Social, and Cultural Rights* (ICESCR), *Convention on the Rights of the Child* (CRC), dan *Convention on the Rights of Persons with Disabilities* (CPRD). *Kedua*, penyusunan ICRP diinisiasi oleh komunitas masyarakat sipil global, sektor bisnis, dan pemerintah pada UN Internet Governance Forum, yang mengangkat perspektif dan orientasi pada perlindungan HAM ketika berbicara tentang tata kelola dan interaksi manusia di internet. Pendekatan tersebut merupakan perspektif yang berbeda dengan pendekatan sektor privat (*private sector*) yang memiliki kecenderungan memprioritaskan kepentingan bisnis, ataupun

aktor negara (*state actor*) yang cenderung proteksionis terhadap kepentingan nasional, khususnya dalam konteks tata kelola internet di Indonesia. Oleh karena itu, kepentingan yang diangkat dalam ICRP juga meliputi kepentingan masyarakat sebagai pengguna (*user*) dan menempatkan masyarakat sebagai subjek yang harus diperhatikan pemenuhan, penghormatan, dan perlindungan haknya. *Ketiga*, dokumen ICRP merupakan dokumen yang otoritatif untuk dirujuk dalam pengambilan kebijakan dan pembentukan hukum, serta menjadi alat advokasi untuk mengembangkan prinsip berbasis hak untuk tata kelola internet.

Piagam ICRP memuat 10 Hak dan Prinsip Internet, tetapi penelitian ini fokus menggunakan prinsip *accessibility* (aksesibilitas) serta *life, liberty, and security* (kehidupan, kebebasan, dan keamanan) sebagai tolok ukur analisis. Dari prinsip tersebut, kami mengelompokkan pembagian analisis menjadi aspek akses, aspek proteksi dan keamanan, dan aspek kebebasan. Hal ini dilakukan karena prinsip-prinsip tersebut merupakan fondasi dalam pengelolaan tata kelola internet. Dalam analisis ini, kami menempatkan ketiga aspek yang tersebut sebagai aspek yang tidak berdiri sendiri, melainkan berkelindan antara satu sama lain. Sebab suatu ketentuan dapat saja mengandung unsur yang memenuhi kualifikasi lebih dari satu aspek pisau analisis.

Aspek akses menjadi lapis yang paling mendasar untuk dapat melandasi keterpenuhan dan jangkauan hak dasar lain—terhadap internet. Aspek akses bagi setiap orang untuk dapat mengakses internet beririsan dengan aspek kebebasan, serta aspek proteksi dan keamanan. Dalam kaca mata penghormatan dan pemenuhan HAM, pemenuhan tiga aspek dalam tata kelola internet akan berdampak pada situasi demokrasi dan civic space. Pada akhirnya, prinsip-prinsip tersebut menciptakan ekosistem digital yang baik dan berbasis hak

asasi manusia dengan penekanan pada pemerintah dan sektor privat dibanding pengguna yang lebih terikat pada etika dan tanggung jawab.

Selanjutnya, yang dimaksud dengan aksesibilitas dalam piagam tersebut adalah bahwa setiap orang mempunyai hak yang sama untuk mengakses dan menggunakan internet secara aman dan terbuka. Prinsip ini menggarisbawahi hak untuk mengakses internet (*right to access to the internet*). Setiap orang berhak untuk mengakses dan memanfaatkan Internet. Hak ini merupakan dasar dari semua hak-hak lain yang dalam piagam ini. Hak ini mengalir terutama dari hak atas kebebasan berekspresi yang dijamin dalam Pasal 19 UDHR dan ICCPR. Yang dimaksud mengakses internet dalam hal ini tidak hanya terbatas dalam hal menumbuhkan kemampuan individu untuk menyampaikan informasi dan ide, tetapi juga untuk mencari dan menerimanya. Hak untuk mengakses internet ini tidak hanya berlaku dalam konteks penggunaan internet dengan tujuan pendidikan atau politik, tetapi juga termasuk penggunaan internet untuk sarana hiburan, jejaring sosial, dan sebagainya.⁴⁸

Saat ini, akses dan penggunaan internet semakin diperlukan untuk menikmati hak asasi manusia secara penuh, termasuk hak atas kebebasan berekspresi, hak atas pendidikan, hak atas kebebasan berkumpul dan berasosiasi secara damai, hak untuk mengambil bagian dalam pemerintahan suatu negara, hak untuk bekerja, dan hak untuk beristirahat dan bersantai. Hak untuk mengakses dan menggunakan internet berasal dari hubungan integralnya dengan semua hak asasi manusia ini. Oleh karena itu, piagam ini menyebutkan bahwa hak untuk mengakses dan memanfaatkan Internet harus dijamin bagi semua orang dan tidak boleh tunduk pada pembatasan apapun, kecuali yang ditetapkan oleh undang-undang, yang diperlukan dalam masyarakat demokratis untuk melindungi

keamanan nasional, ketertiban umum, kesehatan atau moral masyarakat, atau hak dan kebebasan orang lain, dan sesuai dengan hak-hak lain yang diakui dalam piagam ini.⁴⁹

Hak untuk mengakses dan memanfaatkan internet meliputi:⁵⁰

- a. Kualitas layanan. Kualitas layanan yang dapat diakses oleh masyarakat harus berkembang sejalan dengan kemajuan teknologi;
- b. Kebebasan memilih penggunaan sistem dan perangkat lunak. Akses dalam hal ini juga harus mencakup kebebasan dalam memilih penggunaan sistem, aplikasi, dan perangkat lunak. Untuk memfasilitasi hal ini dan menjaga interkoneksi dan inovasi, infrastruktur dan protokol komunikasi harus dapat dioperasikan dan standar harus terbuka. Selain itu, setiap orang harus dapat berinovasi dalam konten, aplikasi, dan layanan tanpa harus menjalani prosedur otorisasi dan validasi terpusat;
- c. Memastikan inklusi digital. Inklusi digital ini mengharuskan semua orang untuk memiliki akses, dan dapat menggunakan secara efektif, berbagai media digital, *platform* komunikasi, dan perangkat untuk pengelolaan dan pemrosesan informasi. Untuk tujuan ini, harus ada dukungan aktif, termasuk dalam penyediaan fasilitas dan layanan yang dikelola sendiri maupun yang berbasis komunitas. Titik akses internet publik harus disediakan, seperti di *telecenter*, perpustakaan, pusat komunitas, klinik, dan sekolah. Selain itu, akses ke internet melalui media seluler juga harus didukung. Inklusi digital juga mencakup aspek persamaan semua kelompok manusia dalam mengakses layanan internet, termasuk kelompok disabilitas; dan
- d. Netralitas jaringan dan kesetaraan jaringan. Internet adalah milik bersama global. Internet harus dilindungi dan dipromosikan agar dapat menjadi sarana pertukaran informasi, komunikasi, dan budaya yang bebas, terbuka, setara, dan tanpa diskriminasi. Tidak boleh ada hak istimewa khusus atau hambatan terhadap pihak atau konten mana pun atas dasar ekonomi, sosial, budaya, atau politik.

Hak atas hidup, kebebasan, dan keamanan (sebagaimana tertuang dalam Pasal 3 DUHAM) dalam jaringan harus dihormati, dilindungi, dan dipenuhi secara *online*. Hak-hak ini tidak boleh dilanggar, atau digunakan untuk melanggar hak-hak lain, di lingkungan online. Pada awalnya, seringkali hak atas kehidupan hanya dikaitkan dengan hukuman mati. Lebih dari itu, hak untuk hidup mencakup banyak isu lain seperti kemampuan generasi sekarang dan masa depan untuk menikmati hak tersebut (UN Human Rights) dan menikmati teknologi modern. Hak untuk hidup tentu fundamental mengingat individu dapat menikmati hak-hak lainnya apabila hak ini telah terpenuhi.

Hak atas kehidupan (*life*) menyangkut kehidupan layak pengguna internet yang harus dijamin pada ruang digital, termasuk segala aspek yang berkenaan atau berhubungan dengan hidup, kualitas hidup, serta lingkungan yang menjamin kehidupan. Pada konteks kehidupan di ruang digital, pengguna harus terpenuhi haknya untuk kebebasan berekspresi dan berpendapat tetapi juga mendapat perlindungan dari segala bentuk risiko serangan hak digital yang mungkin terjadi. Hak ini kemudian memayungi hak lainnya, seperti hak atas kebebasan (*liberty*) dan keamanan (*security*). Hak atas kebebasan (*liberty*) adalah hak yang melindungi tiap individu dari perampasan kebebasan secara sewenang-wenang, yang dalam hal ini dapat dimaknai sebagai kebebasan dalam menggunakan internet dan kebebasan berekspresi. Singgungan kuat lain antara hak atas kebebasan dengan hak atas rasa aman (*right to security*). Hal ini mengacu kepada setiap individu, berhak menikmati koneksi aman ke dan di internet. Semua tindakan pembatasan harus berdasarkan hukum dan standar hak asasi manusia internasional. Hal ini berarti bahwa tindakan pembatasan akan menjadi ilegal jika tindakan tersebut membatasi hak asasi manusia lainnya, misalnya hak atas privasi

atau hak atas kebebasan berekspresi, kecuali dalam keadaan luar biasa.

Pada tata kelola internet, hak untuk hidup, kebebasan, dan keamanan (*the right to life, liberty and security*) meliputi:

- a.** Perlindungan terhadap segala bentuk kejahatan. Setiap orang harus dilindungi terhadap segala bentuk kejahatan yang dilakukan yang menggunakan internet atau di dalam internet, termasuk pelecehan, *cyberstalking*, perdagangan manusia, serta penyalahgunaan identitas dan data digital seseorang;
- b.** Keamanan Internet. Setiap orang berhak untuk menikmati koneksi yang aman ke dan di Internet. Hal ini termasuk perlindungan dari layanan dan protokol yang mengancam fungsi teknis internet, seperti virus, malware, dan phishing.⁵¹



Aspek akses menjadi lapis yang paling mendasar untuk dapat melandasi keterpenuhan dan jangkauan hak dasar lain–terhadap internet. Aspek akses bagi setiap orang untuk dapat mengakses internet beririsan dengan aspek kebebasan, serta aspek proteksi dan keamanan.

**Hak Digital untuk
Demokrasi dan
Civic Space:**

Studi Pemetaan Regulasi
Internet di Indonesia

05

Pemetaan Regulasi Internet di Indonesia dan Perkembangan nya

5. Pemetaan Regulasi Internet di Indonesia dan Perkembangannya

A ● Pengaturan tentang Tata Kelola Internet

Pada dasarnya, sejumlah peraturan perundang-undangan di Indonesia mengatur tentang pengelolaan internet dan interaksi masyarakat di ruang digital, kendati tak seluruh pengaturan secara eksplisit ditujukan untuk meregulasi interaksi di ruang digital. Pengaturan tersebut bersinggungan secara langsung maupun tidak langsung dengan prinsip-prinsip tata kelola internet yang terkandung dalam ICRP, khususnya berkaitan dengan akses internet, proteksi dan keamanan digital, dan kebebasan berekspresi. Kami memetakan, setidaknya terdapat 13 (tiga belas) undang-undang yang memuat pasal terkait dengan tata kelola internet dan perlindungan hak-hak digital. Pada riset ini, kami membatasi objek analisis pada peraturan perundang-undangan di level undang-undang dengan pertimbangan bahwa substansi undang-undang pada umumnya menggariskan pengaturan fundamen tentang tata kelola serta pemenuhan dan perlindungan hak-hak digital.

Undang-undang tersebut, yaitu sebagai berikut:

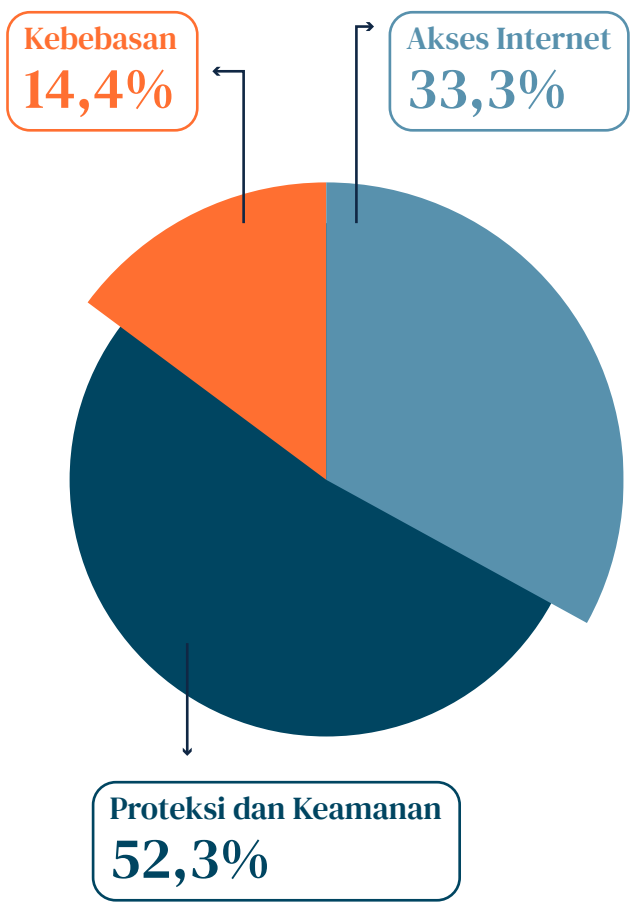
- 1. Undang-Undang Nomor 27 Tahun 2022** tentang Pelindungan Data Pribadi (“UU Pelindungan Data Pribadi”);
- 2. Undang-Undang Nomor 11 Tahun 2008** tentang Informasi dan Transaksi Elektronik, sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 (“UU ITE”);
- 3. Undang-Undang Nomor 4 Tahun 2023** tentang Pengembangan dan Penguatan Sektor Keuangan (“UU Pengembangan dan Penguatan Sektor Keuangan”);
- 4. Undang-Undang Nomor 44 Tahun 2008** tentang Pornografi (“UU Pornografi”);
- 5. Undang-Undang Nomor 44 Tahun 2008** tentang Pornografi (“UU Pornografi”);
- 6. Undang-Undang Nomor 1 Tahun 2023** tentang Kitab Undang-Undang Hukum Pidana (“KUHP Baru”); tentang Pornografi (“UU Pornografi”);

- 7. Undang-Undang Nomor 12 Tahun 2022** tentang Tindak Pidana Kekerasan Seksual (“UU TPKS”);
- 8. Undang-Undang Nomor 7 Tahun 2017** tentang Pemilihan Umum (“UU Pemilu”);
- 9. Undang-Undang Nomor 40 Tahun 1999** tentang Pers (“UU Pers”);
- 10. Undang-Undang Nomor 1 Tahun 2015** tentang Penetapan Perppu Pemilihan Gubernur, Bupati, dan Walikota Menjadi Undang-Undang, sebagaimana diubah dengan Undang-Undang Nomor 8 Tahun 2015, Undang-Undang Nomor 10 Tahun 2016, dan Undang-Undang Nomor 6 Tahun 2020 (“UU Pilkada”);
- 11. Undang-Undang Nomor 14 Tahun 2008** tentang Keterbukaan Informasi Publik (“UU Keterbukaan Informasi Publik”);
- 12. Undang-Undang Nomor 8 Tahun 1999** tentang Perlindungan Konsumen (“UU Perlindungan Konsumen”); dan
- 13. Undang-Undang Nomor 12 Tahun 2011** tentang Pembentukan Peraturan Perundang-undangan, sebagaimana diubah dalam Undang-Undang Nomor 15 Tahun 2019 dan Undang-Undang Nomor 13 Tahun 2022 (“UU Pembentukan Peraturan Perundang-Undang”).

Mayoritas isu yang diatur dalam undang-undang di atas bersifat sektoral, artinya pengelolaan ruang digital serta perlindungan dan pemenuhan hak-hak digital menjadi salah satu bagian pengaturan pelengkap di dalam undang-undang

tersebut. Bahkan terhadap undang-undang yang disahkan sebelum UU ITE, aspek digital tidak menonjol, tetapi pengaturan umum yang terdapat dalam undang-undang tersebut relevan untuk mengikat pengelolaan dan interaksi pengguna di ruang digital. Di sisi lain, pengaturan dalam UU ITE dan UU PDP secara khusus diperuntukkan bagi pengelolaan ruang digital dalam hal pendistribusian informasi dan transaksi elektronik serta perlindungan data pribadi pengguna ruang digital.

Persentase Pengaturan Tiap Aspek Tata Kelola Internet pada Legislasi



Pemetaan dan analisis dilakukan terhadap 13 (tiga belas) undang-undang dan 153 (seratus lima puluh tiga) ketentuan yang mengatur terkait tata kelola internet di Indonesia. Dari jumlah tersebut, seperti yang tergambarkan pada diagram di atas, ditemukan terdapat 51 (lima puluh satu) norma yang mengatur tentang aspek internet atau setara dengan 33.3% (tiga puluh tiga koma tiga persen), 80 (delapan puluh) ketentuan yang mengatur aspek proteksi dan keamanan digital atau setara dengan 52.3% (lima puluh dua koma tiga persen), dan 22 (dua puluh dua) ketentuan yang mengatur aspek kebebasan (*liberty*) atau setara dengan 14.4% (empat belas koma empat persen).

Dari data tersebut, terlihat bahwa orientasi pengaturan tata kelola internet yang tersebar pada 13 (tiga belas) undang-undang tersebut memiliki kecenderungan proteksionis (*protection heavy*). Artinya, negara memiliki kecenderungan untuk mengontrol warga negara dalam beraktivitas di ruang digital. Paradigma ini diperkuat dengan minimnya jaminan kebebasan dalam undang-undang-undang yang menjadi objek riset, dalam hal ini, jaminan kebebasan hanya ditemukan dalam sembilan undang-undang saja. Pengaturan dalam setiap undang-undang tersebut pun ditemukan dalam jumlah yang minim, misalnya paling banyak terdapat enam jaminan perlindungan dalam KUHP, lima jaminan dalam UU ITE, tiga jaminan dalam UU Pornografi dan UU Keterbukaan Informasi Publik, dan satu jaminan dalam UU Pemilu, UU Pers, UU Pilkada, UU Perlindungan Konsumen, dan UU Pembentukan Peraturan Perundang-Undangan. Bandingkan dengan pengaturan terkait proteksi dalam UU ITE yang berjumlah 25 (dua puluh lima) ketentuan, atau dalam UU Perlindungan Konsumen terdapat 20 (dua puluh) ketentuan.

Sementara itu, ketentuan tentang akses internet menempati posisi terbanyak kedua,

yaitu sebanyak 51 (lima puluh satu) ketentuan. Temuan terhadap pengaturan tentang akses internet terkait dengan bagaimana pengguna dapat memperoleh ruang aman dalam berinteraksi di internet dan tidak dibatasi oleh pilihan teknologi tertentu serta tidak dihalangi untuk memperoleh, mengolah, dan mendistribusikan informasi tertentu. Akses dalam hal ini tidak termasuk pada pemerataan jangkauan internet, sebab pada 13 (tiga belas) undang-undang yang telah dipetakan, tak ada satupun yang mengatur jaminan terhadap pemerataan jangkauan akses internet.

Ketiga belas undang-undang yang dianalisis mengandung jaminan perlindungan kebebasan yang sangat minim, yaitu terdapat 22 (dua puluh dua) ketentuan pengaturan atau setara dengan 14.4% (empat belas koma empat persen). Persentase ini menguatkan tesis terhadap tendensi pengaturan ruang digital yang proteksionis, sebab orientasi pengaturan ditujukan untuk memperketat pengawasan kepada pengguna, bukan mengakomodasikan dan menjamin hak kebebasan berekspresi di ruang digital.

Pemaparan lebih lanjut tentang analisis masing-masing aspek dapat disimak pada bagian di bawah ini.

1. Akses Internet

Akses terhadap internet dalam beragam undang-undang bermaksud untuk memberikan aksesibilitas dan keterbukaan informasi bagi pengguna internet. Di satu sisi, secara normatif, regulasi terkait akses internet memastikan dan menjamin bahwa pengguna dapat memperoleh akses terhadap internet secara wajar, terlindungi, dan memperoleh ruang aman dalam berinteraksi di internet, dan tidak dibatasi

oleh pilihan teknologi tertentu serta tidak dihalangi untuk memperoleh, mengolah, dan mendistribusikan informasi tertentu.

Seperti yang terjadi pada UU Pelindungan Data Pribadi, subjek diberikan pelindungan agar data pribadi yang bersangkutan tidak secara ilegal diakses dan disalahgunakan oleh pihak lain ketika memberikan informasi pribadinya saat beraktivitas di ruang digital. Contoh lain adalah UU Pers yang tetap memastikan jurnalis memiliki hak untuk mengakses, mengolah, dan memperoleh informasi untuk kegiatan jurnalistik. Di sisi lain, UU Keterbukaan Informasi Publik dan UU Pemilu juga memberikan jaminan atas akses informasi publik di ruang digital yang dapat dinikmati oleh masyarakat. Pelindungan juga dapat dilakukan dengan memberikan pembatasan terhadap akses informasi, seperti yang diatur dalam UU TPKS, yang fungsinya untuk menghindari reviktimisasi penyintas akibat penyebaran konten elektronik.

Namun demikian, terdapat pula norma yang kontraproduktif terhadap pelaksanaan kebebasan berserikat, berkumpul, berpendapat, dan berekspresi, sebab memberikan kewenangan yang besar bagi Pemerintah untuk menentukan secara sepihak, kapan informasi dapat dibatasi, melakukan moderasi konten, hingga memutus sama sekali akses internet, seperti yang diatur di dalam UU ITE. Analisis di bawah ini mengupas ragam orientasi pengaturan dan tujuan pengaturan terkait akses internet dari tiap-tiap legislasi terkait.

a. UU ITE

UU ITE mengamanatkan bahwa dalam mengakses internet atau ruang digital, pengguna memiliki kebebasan memilih teknologi atau netral teknologi,⁵² yang artinya tidak terfokus pada penggunaan teknologi tertentu, sehingga dapat

mengikuti perkembangan pada masa yang akan datang.⁵³

Aksesibilitas terhadap internet tersebut ditujukan untuk:⁵⁴

- mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
- mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
- meningkatkan efektivitas dan efisiensi pelayanan publik;
- membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan teknologi informasi seoptimal mungkin dan bertanggung jawab; dan
- memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi.

Dalam konteks akses terhadap internet, UU ITE mengenakan sanksi atas tindakan yang mengakibatkan terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya,⁵⁵ serta ganjaran pidana bagi perlakuan yang dilarang Pasal 27-Pasal 36 yang meliputi yurisdiksi sistem elektronik di luar Indonesia.⁵⁶

Perihal akses, Pasal 20 ayat (2a), (2b), (2c), dan (2d) UU ITE memberikan kewenangan yang signifikan bagi Pemerintah untuk melakukan pencegahan

penyebarluasan dan penggunaan informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang dilarang ketentuan peraturan perundang-undangan, dengan cara melakukan pemutusan akses, melakukan moderasi konten, dan memerintahkan penyelenggara sistem elektronik untuk melakukan pemutusan akses dan melakukan moderasi konten.⁵⁷ Namun demikian, pasal-pasal tersebut memberikan kewenangan sepihak bagi Pemerintah, dalam hal ini Kementerian Komunikasi dan Digital (Komdigi), untuk melabeli muatan konten tanpa basis yang jelas. Pasal tersebut tidak dilengkapi dengan sistem checks and balances yang memungkinkan adanya keterlibatan pihak ketiga untuk memberikan perspektif penyeimbang. Oleh karena itu, Pemerintah dapat secara serta-merta melakukan pembatasan atau pemblokiran konten, hingga akses internet terhadap aktivitas apapun yang dianggap menyimpangi undang-undang, termasuk aktivitas dan konten terkait kebebasan berpendapat, berserikat, berkumpul, dan berekspresi. Kondisi tersebut sejatinya merupakan pelanggaran atas Pasal 28F UUD 1945, sebab telah mereduksi, bahkan meniadakan hak masyarakat untuk memperoleh akses dan informasi.

Kondisi konkret pernah terjadi ketika Pemerintah, melalui Kementerian Komunikasi dan Informatika (Kominfo), melakukan pemblokiran akses internet di

Papua.⁵⁸ Pada 21 Agustus - 6 September 2019, Pemerintah melakukan pemblokiran atau pelambatan (*throttling*) koneksi internet di Papua sebagai respon terhadap aksi demonstrasi di Papua Barat. Demonstrasi besar-besaran tersebut dilatarbelakangi oleh adanya tindakan rasisme terhadap sejumlah mahasiswa Papua di Surabaya. Tindakan Pemerintah didasari oleh Pasal 40 ayat (2a) dan (2b) UU ITE. Pengadilan Tata Usaha Negara Jakarta kemudian memutus bahwa Presiden Joko Widodo dan Kominfo melakukan perbuatan melanggar hukum, sebab pemutusan akses hanya terhadap informasi elektronik dan/atau dokumen elektronik yang “bermuatan melanggar hukum”, tidak mencakup pemutusan akses jaringan internet.⁵⁹

b. UU Pengembangan dan Penguatan Sektor Keuangan

UU Pengembangan dan Penguatan Sektor Keuangan merupakan omnibus perubahan regulasi pada sektor keuangan. Ketentuan yang berkenaan dengan akses terhadap internet pada Undang-Undang ini bersinggungan dengan perubahan atas Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal, terutama berkenaan dengan *securities crowdfunding*. Pada perubahan tersebut, Otoritas Jasa Keuangan (OJK) diberikan kewenangan untuk mengatur penyelenggaraan penghimpunan dana masyarakat melalui penawaran Efek dengan

menggunakan jasa penyelenggara sistem elektronik (*securities crowdfunding*),⁶⁰ termasuk perluasan akses bagi Usaha Mikro, Kecil, dan Menengah untuk mendapatkan pendanaan dari Pasar Modal.⁶¹

c. UU Perlindungan Data Pribadi

Pada UU Pelindungan Data Pribadi, aspek akses internet berkelindan pada dua hal, yaitu: (1) memastikan pelindungan data pribadi pengguna; dan (2) menerapkan kewajiban bagi pemroses data pribadi dan pengendali data pribadi untuk menjaga dan memastikan keamanan data pribadi pengguna. Hal tersebut ditujukan untuk menciptakan ruang aman bagi pengguna internet dan menghindari penyalahgunaan data pribadi untuk kepentingan yang tidak dapat dipertanggungjawabkan. Perihal kepastian pelindungan data pribadi pengguna, UU Pelindungan Data Pribadi memastikan bahwa pengguna mendapat akses dan memperoleh salinan data pribadi tentang dirinya sendiri.⁶² Sementara itu, pemroses data pribadi dan pengendali data pribadi diberikan kewajiban untuk:

- melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, dan penghilangan data pribadi;⁶³
- menolak memberikan akses data dalam hal: (a) membahayakan keamanan,

kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/ atau orang lain; (b) berdampak pada pengungkapan Data Pribadi milik orang lain; dan/ atau; (c) bertentangan dengan kepentingan pertahanan dan keamanan nasional;⁶⁴

- mencegah data pribadi diakses secara tidak sah.⁶⁵

d. KUHP

Pengaturan dalam KUHP baru lebih banyak bersinggungan dengan aspek proteksi dan keamanan digital dan kebebasan berekspresi. Dalam hal ini, kami tidak memperoleh temuan signifikan tentang persinggungan antara KUHP dengan akses internet.

e. UU Pembentukan Peraturan Perundangan-Undangan

Pada UU Pembentukan Peraturan Perundang-Undangan, aspek akses internet berkenaan pada penyebarluasan informasi legislasi kepada masyarakat melalui kanal-kanal elektronik milik DPR dan Pemerintah di level nasional, dan pemerintah daerah untuk level peraturan daerah.⁶⁶ Selain itu, pengaturan juga terkait dengan pembentukan peraturan perundang-undangan secara elektronik, sejak perencanaan sampai dengan penggunaan. Aksesibilitas di sini dalam hal penggunaan tanda tangan elektronik pada setiap tahap pembentukan undang-undang.⁶⁷

Pengaturan aksesibilitas dalam undang-undang ini berkaitan

dengan pemenuhan asas transparansi dan akuntabilitas pembentukan peraturan perundang-undangan serta pemenuhan hak publik atas informasi pembentukan peraturan perundang-undangan pada setiap tahap pembentukan. Akses yang dimaksud ditujukan terhadap dokumen-dokumen pembentukan peraturan perundang-undangan, seperti rancangan undang-undang, naskah akademik, jadwal pembahasan undang-undang, daftar hadir anggota legislatif dalam rapat pembahasan, dokumen risalah rapat pembahasan, dan sebagainya.

Kendati telah diamanatkan untuk menyebarluaskan informasi pembentukan peraturan perundang-undangan, pada praktiknya, akses publik terhadap dokumen pembentukan tak selalu terbuka dan tak terus dipermudah. Pada sejumlah undang-undang kontroversial seperti UU Cipta Kerja (tahun 2020 dan perppu), Perubahan Ketiga UU Mahkamah Konstitusi, UU Pertambangan Mineral dan Batu Bara, Perubahan UU Kementerian Negara, Rancangan Undang-Undang Polri, dan Rancangan Undang-Undang TNI, sulit untuk memperoleh dokumen mendasar pembentukan undang-undang seperti rancangan undang-undang dan naskah akademik.

Terhadap pembahasan rancangan undang-undang yang kontroversial dan kontraproduktif dengan kepentingan publik, *website* resmi DPR dan

Pemerintah tidak menyediakan informasi secara cukup, terbuka, dan aktual pada momentum yang tepat saat pembahasan dilakukan. Kelompok masyarakat sipil kerap memperoleh informasi tersebut melalui kanal informal, yaitu melalui jejaring personal dengan anggota legislatif atau tenaga ahli DPR, maupun awak jurnalis. Hal ini menjadi tantangan besar untuk mewujudkan pembentukan peraturan perundang-undangan yang memenuhi prinsip *meaningful participation*, sebab partisipasi tersebut tak akan bermakna jika tak dimulai dengan transparansi dan keterbukaan akses bagi publik terhadap dokumen perancangan peraturan secara wajar.

f. UU TPKS

Pada UU TPKS, aspek akses internet ditujukan pada penghapusan dan/atau pemutusan akses informasi dan/atau dokumen yang bermuatan tindak pidana kekerasan seksual.⁶⁸ Penghapusan dan/atau pemutusan akses tersebut diajukan oleh Jaksa kepada Ketua Pengadilan Negeri untuk kemudian memerintahkan Komdigi untuk menghapus dan/atau memutus akses tersebut.⁶⁹ Ketentuan tersebut menunjukkan bahwa orientasi aspek akses internet dalam UU TPKS cenderung pada pembatasan akses. Hal tersebut ditujukan agar akses dan pemanfaatan internet dapat dilakukan secara aman dan terbuka serta memberikan proteksi

kepada korban dari viktimisasi yang berulang.

UU Pemilu

Pada UU Pemilu, akses dan pemanfaatan internet berkelindan pada penyebaran gagasan partai politik dan kandidat peserta pemilu melalui kegiatan kampanye yang dapat dilakukan pada media daring,⁷⁰ serta penyediaan dan penyebaran informasi elektronik ke pemilu melalui sistem informasi yang dimiliki oleh masing-masing penyelenggara pemilu,⁷¹ termasuk pula larangan mendistorsi sistem informasi penghitungan suara.⁷²

Pasal tentang kampanye membuka kemungkinan bagi peserta pemilu untuk berinteraksi dengan konstituen, baik secara langsung maupun melalui media elektronik, dalam menyampaikan gagasan dan menampung aspirasi konstituen. Hal tersebut merupakan bagian dari pendidikan politik bagi peserta pemilu dan masyarakat untuk membentuk orientasi interaksi peserta pemilu dan konstituen yang berbasis gagasan visioner.

Sementara itu, penyebaran informasi elektronik melalui penyelenggara pemilu merupakan perwujudan transparansi dan akuntabilitas penyelenggara pemilu atas keterbukaan informasi ke pemilu bagi konstituen. Sistem informasi yang dimiliki oleh penyelenggara pemilu saat ini, misalnya:

- KPU menyediakan kanal informasi, di antaranya Sistem Informasi Penghitungan Suara

(SITUNG), Sistem Informasi Rekapitulasi Suara (SIREKAP), Sistem Informasi Partai Politik (SIPOL), Sistem Informasi Daerah Pemilihan (SIDAPIL), Sistem Informasi Pencalonan (SILON), Sistem Informasi Logistik (SILOG), Sistem Informasi Kampanye dan Dana Kampanye (SIKADEKA);

- Bawaslu menyediakan kanal informasi, di antaranya Sistem Informasi Penyelesaian Sengketa (SIPS), SiGapLapor (sistem untuk melaporkan pelanggaran pemilu), Jaringan Dokumentasi dan Informasi Hukum (JDIH); dan
- Dewan Kehormatan Penyelenggara Pemilu menyediakan kanal informasi, di antaranya untuk mengakses pengaduan pelanggaran etik penyelenggara pemilu, jadwal persidangan, risalah persidangan, dan putusan etik.

Pengaturan terhadap sistem informasi tersebut dilengkapi dengan pidana pemilu bagi siapapun yang mendistorsi sistem informasi penghitungan suara, sebab dapat mencoreng kemurnian hasil pemilu.

Secara normatif, kedua dasar pengaturan tersebut dapat menjadi acuan bagi publik untuk memperoleh informasi ke pemilu secara resmi dan utuh dari penyelenggara pemilu dan peserta pemilu. Namun demikian, pada praktiknya, akses atas informasi elektronik masih menghadapi tantangan akibat kerangka hukum UU Pemilu yang belum dapat merespon dinamika

perkembangan pemanfaatan internet dan teknologi informasi kini. Misalnya, masih terdapat kekosongan hukum terkait disinformasi pemilu, pengaturan hanya dilekatkan pada manajemen bagi pelaksana kampanye, peserta pemilu, dan tim kampanye.⁷³ Kendati UU Pemilu telah mengatur norma larangan menyinggung isu suku, agama, ras, dan antargolongan (SARA), aturan tersebut belum dapat melindungi kelompok rentan, yaitu perempuan, kelompok penyandang disabilitas, minoritas beragama dan ras, serta minoritas gender, yang menjadi objek target disinformasi pemilu, ujaran kebencian, *trolling*, dan *doxing*.⁷⁴

Selain itu, tidak terdapat dorongan regulasi dan *political will* KPU dan Bawaslu untuk meminta akuntabilitas dan transparansi *platform* media sosial dalam melakukan penayangan konten kampanye pemilu yang mengandung unsur disinformasi dan misinformasi,⁷⁵ serta mendorong kebijakan efektivitas algoritma dan responsivitas terhadap pengaduan.⁷⁶ Aturan turunan tentang kampanye dalam Peraturan KPU Nomor 15 Tahun 2023 tentang Kampanye Pemilu juga tidak cukup untuk merespon hal tersebut, isu khusus yang diatur di dalamnya terkait dengan pembatasan akun peserta pemilu di setiap *platform* media sosial maksimal 20 (dua puluh) akun dan keterlibatan Kominfo/Komdigi untuk menerima formulir pendaftaran akun media sosial peserta pemilu.

Kondisi tersebut kontraproduktif untuk menghadirkan ruang yang aman dan bermanfaat bagi masyarakat untuk terlibat dalam pendidikan politik dan akses informasi kepiluan. Sebab distorsi informasi kepiluan menjadi penghambat dalam mengakses informasi kepiluan yang benar dan tidak mengandung kekerasan dan ujaran kebencian. Selain itu, hal ini juga menjadi tantangan untuk menghadirkan forum deliberasi daring yang konstruktif dan inklusif untuk tujuan pendidikan politik yang baik bagi peningkatan kualitas demokrasi elektoral.

h. UU Pilkada

Pada UU Pilkada, aspek akses internet jauh lebih minim dibandingkan dengan UU Pemilu. Pengaturan tersebut dititikberatkan pada aspek penyampaian materi kampanye dengan cara yang sopan, tertib, dan edukatif yang dapat dilakukan melalui media elektronik,⁷⁷ serta sanksi pidana terhadap tindakan mendistorsi sistem informasi penghitungan suara.⁷⁸ UU Pilkada juga memiliki tantangan yang serupa dengan UU Pemilu, sebab belum terdapat pembaruan terhadap konteks kampanye di ruang digital, disinformasi dan misinformasi pemilu di internet, kewenangan KPU dan Bawaslu dalam penanganan disinformasi dan misinformasi pemilu, dan moderasi konten oleh *platform* media sosial.

i. UU Hak Cipta

Pada UU Hak Cipta, tidak terdapat ketentuan yang berkaitan dengan penormaan dan penjaminan atas akses internet. Ketentuan UU Hak Cipta relevan dengan aspek proteksi dan keamanan digital.

j. UU Pornografi

Pada UU Pornografi, pengaturan mengenai akses internet serupa dengan pengaturan dalam UU TPKS. Orientasi pengaturan mengarah pada pembatasan akses terhadap konten. Pada UU Pornografi, Pemerintah Pusat dan Pemerintah Daerah berwenang melakukan pemutusan jaringan pembuatan dan penyebarluasan produk pornografi atau jasa pornografi, termasuk pemblokiran pornografi melalui internet.⁷⁹ Hal tersebut ditujukan agar akses dan pemanfaatan internet dapat dilakukan secara aman dan terbuka serta memberikan proteksi kepada korban konten pornografi dari viktimisasi yang berulang, maupun masyarakat pengguna internet dari paparan konten pornografi.

k. UU Keterbukaan Informasi Publik

UU Keterbukaan Informasi Publik adalah undang-undang yang memiliki pengaturan tentang akses internet terbanyak, mengingat Undang-Undang *a quo* menjadi dasar yang pemberian hak bagi masyarakat untuk memperoleh informasi publik⁸⁰ dan kewajiban bagi badan publik untuk menyebarluaskan dan

memberikan informasi publik kepada masyarakat secara umum dan yang memohon keterbukaan informasi publik.⁸¹ Undang-Undang ini mengamanatkan agar informasi publik bersifat terbuka dan dapat diakses oleh setiap pengguna informasi publik, serta dapat diperoleh siapapun yang memohon informasi publik dengan cepat dan tepat waktu, biaya ringan, dan cara sederhana.⁸² Informasi tersebut wajib disediakan, diberikan, dan/atau diterbitkan secara akurat, benar, dan tidak menyesatkan. Selain itu, untuk meningkatkan aksesibilitas publik terhadap informasi publik, badan publik wajib untuk mengembangkan sistem informasi dan dokumentasi untuk mengelola informasi publik secara baik dan efisien.

Kendati badan publik memiliki hak untuk menolak memberikan informasi publik, dalam hal informasi publik tak sesuai dengan ketentuan peraturan perundang-undangan⁸³ dan informasi publik mengandung materi berikut:⁸⁴

- informasi yang dapat membahayakan negara;
- informasi yang berkaitan dengan kepentingan perlindungan usaha dari persaingan usaha tidak sehat;
- informasi yang berkaitan dengan hak-hak pribadi;
- informasi yang berkaitan dengan rahasia jabatan; dan/atau
- informasi publik yang diminta belum dikuasai atau didokumentasikan.

UU Keterbukaan Informasi Publik juga menerapkan sanksi pidana terkait dengan aksesibilitas informasi publik. Sanksi pidana diterapkan bagi badan publik yang dengan sengaja tidak menyediakan, tidak memberikan, dan/atau tidak menerbitkan informasi publik secara berkala, informasi publik yang wajib diumumkan secara serta-merta, dan/atau informasi publik yang harus diberikan atas dasar permintaan sesuai dengan UU Keterbukaan Informasi Publik.⁸⁵ Sanksi pidana juga ditujukan pada setiap orang yang dengan sengaja dan tanpa hak mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan.⁸⁶

Akses terhadap informasi publik di ruang digital tak selalu disediakan secara wajar oleh badan publik. Misalnya, sengketa informasi pemilihan yang diajukan oleh *Indonesia Corruption Watch* (ICW) terhadap KPU di Komisi Informasi Pusat (KIP). Pada Pemilu Tahun 2024 lalu, ICW memintakan informasi tentang dana kampanye, riwayat hidup calon anggota legislatif, dan data tim kampanye kepada KPU, tetapi KPU menolak memberikan informasi karena dianggap sebagai informasi yang dikecualikan.⁸⁷ Terhadap laporan ICW, Komisi Informasi menyatakan bahwa akses ke sistem informasi dana kampanye dan laporan sumbangan dana kampanye adalah informasi yang dikecualikan untuk melindungi privasi, tetapi perihal daftar tim kampanye dan riwayat hidup yang tidak mengandung data

pribadi, harus disediakan oleh KPU.⁸⁸

Permohonan ICW yang dikabulkan sebagian tersebut menjadi titik balik untuk memahami kembali aspek transparansi dan keterbukaan informasi dalam UU Pemilu dan UU Keterbukaan Informasi Publik ketika dibenturkan kepada proteksi data pribadi dalam UU Pelindungan Data Pribadi. Pemahaman demikian malah menghambat akses informasi publik melalui media elektronik untuk mengetahui informasi yang seharusnya disediakan kepada publik secara serta-merta. Perlu terdapat ukuran sejauh mana informasi tergolong sebagai data pribadi. Dalam hal dana kampanye, penting bagi publik untuk mengetahui siapa pihak yang terlibat sebagai donatur sebagai bentuk transparansi dan akuntabilitas pendanaan politik, sebagaimana diamanatkan dalam UU Pemilu. Tanpa adanya ukuran tersebut, badan publik berpotensi untuk mengelak permohonan keterbukaan informasi publik berlandaskan pemahaman data privasi yang parsial dan tak bertujuan untuk kepentingan publik.

I. UU Pers

Pada UU Pers, aspek akses internet ditujukan untuk memberikan jaminan dan perlindungan bagi jurnalis untuk mengakses, mengolah, dan mendistribusikan informasi kepada publik, yang dapat melalui media elektronik. Aspek tersebut merupakan perlindungan

dan jaminan yang diakomodasikan utamanya dalam Pasal 28F UUD 1945. Setidaknya terdapat empat hal yang relevan dalam hal ini:⁸⁹

- kemerdekaan pers dijamin sebagai hak asasi warga negara;
- terhadap pers nasional tidak dikenakan penyensoran, pembredelan, atau pelarangan penyiaran;
- untuk menjamin kemerdekaan pers, pers nasional mempunyai hak mencari, memperoleh, dan menyebarkan gagasan dan informasi;
- dalam mempertanggungjawabkan pemberitaan di depan hukum, wartawan mempunyai hak tolak.

m. UU Perlindungan Konsumen

UU Perlindungan Konsumen menggariskan aspek internet yang berkelindan dengan hak konsumen dan pelaku usaha atas akses informasi mengenai transaksi yang akan dilakukan untuk memberikan kepastian hukum dan keamanan bagi kedua belah pihak. Sejatinya, hal tersebut tercermin sejak tujuan pembentukan Undang-Undang *a quo*, yaitu di antaranya, menciptakan sistem perlindungan konsumen yang mengandung unsur kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi.⁹⁰ Undang-Undang ini juga memberikan hak bagi konsumen dan kewajiban bagi pelaku usaha

untuk memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang/jasa serta memberi penjelasan penggunaan, perbaikan, dan pemeliharaan.⁹¹

2. Proteksi dan Keamanan Digital

Bagian ini mengulas jaminan terhadap keamanan dan perlindungan digital pengguna internet tanpa pembatasan yang mengancam HAM, kecuali dalam kondisi luar biasa (*exceptional conditions*). Hal ini meliputi: (1) perlindungan atas segala bentuk kekerasan yaitu kekerasan yang terjadi di internet atau menggunakan internet; dan (2) keamanan atas akses internet dan saat berada di internet, termasuk aman dari serangan teknis di internet (*virus, malware, phishing*).

Ketentuan mengenai digital yang memberikan proteksi tersebar dalam bidang penyiaran, usaha, otoritas jasa keuangan, hukum pidana khususnya mengenai alat bukti dan penghapusan konten terkait kekerasan seksual, pemilu, keterbukaan informasi, hingga perlindungan data pribadi. Hal ini menunjukkan semakin berkembangnya kesadaran juga kebutuhan akan perlindungan hukum terkait digital. Tidak seluruh pengaturan ini melalui undang-undang, melainkan juga oleh putusan Mahkamah Konstitusi (MK). Artinya, di satu sisi MK juga menyadari keperluan pengaturan terkait digital dan di sisi lain peran masyarakat untuk memunculkan hukum-hukum baru melalui aktivisme juga penting.

Pelindungan ini juga termasuk pemidanaan untuk berbagai sektor. Mulai dari menghambat atau menghalangi kebebasan pers, ancaman atau kekerasan digital, kekerasan seksual, pejabat yang melampaui kewenangannya terkait sistem informasi hingga terkait sistem informasi penghitungan suara hasil pemilu.

Di sisi lain, ketentuan proteksi digital menimbulkan sejumlah masalah yang terdiri dari beberapa pola. Gejala yang paling mengemuka adalah dasar proteksi yang dapat ditafsirkan secara luas. Dalam kategori ini kata yang muncul adalah (1) membahayakan keutuhan Negara Kesatuan; (2) menghina seseorang, agama, suku, ras, golongan, calon; (3) mengganggu ketertiban umum; (4) mempersoalkan dasar negara Pancasila, Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, dan bentuk Negara Kesatuan Republik Indonesia; (5) tanpa hak; (6) cara apapun; (7) memengaruhi; (8) tertib; (9) sopan; (10) kepentingan hukum negara; dan (11) kepentingan nasional tertentu.

Gejala berikutnya adalah pengaturan proteksi ini beririsan dengan kebebasan berpendapat termasuk mendapatkan informasi. Unsur yang sering muncul adalah “melawan hukum” sebagai batasan misal tidak boleh melawan hukum dalam larangan mengumpulkan atau memperoleh data pribadi yang bukan miliknya. Larangan dapat menysar orang yang melakukan advokasi terhadap berbagai isu sosial termasuk advokasi isu anti korupsi. Tanpa hak adalah pengaturan berikutnya yang muncul lebih dari satu kali. Selain itu juga, ada “yang tidak bersifat publik” karena dalam konteks pemerintahan yang tidak demokratis bisa ditentukan sewenang-wenang oleh pemerintah. Berikutnya adalah “orang lain” yang bisa saja diartikan mencakup pejabat publik dan terakhir adanya ketentuan tentang komputer atau sistem elektronik yang dilindungi oleh negara yang bisa mencakup banyak sistem sehingga membatasi kebebasan berpendapat.

Gejala ketiga adalah pengaturan tindak pidana berbasis elektronik untuk melindungi kepentingan hukum negara atau kepentingan nasional tertentu, khususnya keselamatan dan keamanan sistem elektronik.

Pelindungan hak atas kebebasan berpendapat tidak menjadi dasar pengaturan digital dalam KUHP padahal seluruh peraturan perundang-undangan terikat kepada HAM sesuai dengan mandat Konstitusi.

Terakhir, munculnya norma non-hukum yang menjadi dasar pengaturan. Kesopanan adalah norma sosial dan karenanya dapat berda-beda antara satu orang dengan orang lainnya. Oleh karena itu, kesopanan seharusnya tidak menjadi dasar pengaturan hukum.

a. UU Pers

Undang-undang Pers memberikan beberapa perlindungan kepada jurnalis. Pertama adalah Pasal 4 ayat (2), yaitu “terhadap pers nasional tidak dikenakan penyensoran, pembredelan, atau pelarangan penyiaran. Selanjutnya, Pasal 4 ayat (3) menjamin kemerdekaan pers, sehingga pers nasional mempunyai hak mencari, memperoleh, dan menyebarluaskan gagasan dan informasi. Lebih dari itu, Pasal 18 ayat (1) memberikan hukuman terhadap orang yang melakukan tindakan yang berakibat menghambat atau menghalangi pelaksanaan ketentuan Pasal 4 ayat (2) dan ayat (3) tersebut yaitu pidana penjara paling lama dua tahun atau denda paling banyak Rp.500.000.000,00.

b. UU ITE

Pasal 29 Perubahan Kedua UU ITE, yaitu Undang-Undang Nomor 1 Tahun 2024, memberikan perlindungan berupa ancaman pemidanaan terhadap setiap

orang yang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik secara langsung kepada korban yang berisiko ancaman kekerasan dan/atau menakutkan. Penjelasan ketentuan ini menyatakan bahwa “termasuk dalam perbuatan yang dimaksud dalam ketentuan ini adalah perundungan di ruang digital (*cyber bullying*)”. Pasal baru ini memberikan batasan tentang siapa yang dimaksud “korban” yaitu orang yang mengalami penderitaan fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh tindak pidana.

c. UU Pengembangan dan Penguatan Sektor Keuangan *jo.* Undang-Undang Nomor 7 Tahun 2011 tentang Mata Uang

Pelindungan dalam sektor keuangan setidaknya mengenai wewenang penyidik Otoritas Jasa Keuangan dan kewajiban penyelenggara sistem elektronik. UU Pengembangan dan Penguatan Sektor Keuangan Bagian Keempat mengenai Otoritas Jasa Keuangan, khususnya Pasal 49 (7) huruf j, memberikan wewenang kepada Penyidik Otoritas Jasa Keuangan untuk meminta data, dokumen, atau alat bukti lain baik cetak maupun elektronik kepada penyelenggara jasa telekomunikasi atau penyelenggara jasa penyimpanan data dan/atau dokumen. Bab IX Undang-Undang ini tentang Penawaran Efek dan Perusahaan Publik dalam Pasal 69A ayat (3) juga mewajibkan penyelenggara

sistem elektronik untuk memperoleh izin usaha dari Otoritas Jasa Keuangan.

d. UU TPKS

UU TPKS memberikan perubahan mendasar mengenai pelindungan terhadap kekerasan seksual termasuk yang berbasis elektronik.⁹² Tindakan yang dilarang secara spesifik salah satunya terdapat dalam Pasal 14 ayat (1) huruf b, yaitu transmisi informasi elektronik yang bermuatan seksual di luar kehendak penerima. Ketentuan lain ada dalam Pasal 14 ayat (1) huruf c, yaitu melakukan penguntitan atau pelacakan menggunakan sistem elektronik. Kedua larangan ini merupakan delik aduan berdasarkan Pasal 14 ayat (3), yaitu proses hukum terjadi atas pengaduan korban. Pelindungan ini bertambah untuk anak dan penyandang disabilitas, yaitu persetujuan mereka tidak menghapuskan tuntutan pidana.⁹³

Pelindungan berikutnya adalah tindak pidana kekerasan seksual yang ada dalam undang-undang ini, kecuali pelecehan seksual fisik, mendapat penambahan $\frac{1}{3}$ (satu per tiga) untuk pembedanya apabila dilakukan menggunakan sarana elektronik. Hal penting lainnya, Pasal 24 UU TPKS menjadi dasar hukum bahwa alat bukti termasuk informasi elektronik.⁹⁴ Terakhir, UU TPKS memberikan wewenang kepada jaksa, demi kepentingan umum, untuk dapat mengajukan permintaan kepada ketua pengadilan negeri untuk memerintahkan kementerian yang

menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika menghapus informasi elektronik dan/atau dokumen elektronik yang bermuatan Tindak Pidana Kekerasan Seksual.⁹⁵

e. UU Pilkada

Pasal 195 UU Pilkada memuat larangan mendistorsi sistem informasi penghitungan suara. Hal ini merupakan bentuk perlindungan terhadap hak politik dan hak atas informasi. Pasal 64 UU Pilkada sekilas terlihat sebagai ketentuan yang baik karena mengatur penyampaian materi kampanye dengan cara yang sopan, tertib, dan edukatif. Masalah dalam ketentuan ini adalah definisi sopan dan tertib yang tidak jelas, sehingga dapat diartikan secara luas dan multitafsir. Selain itu, kesopanan adalah norma sosial dan dapat berbeda-beda antara satu orang dengan orang lainnya. Kesopanan karena itu seharusnya tidak menjadi norma hukum.

f. UU Hak Cipta

Putusan MK terkait pengujian UU Hak Cipta memberikan perluasan makna tentang tempat perdagangan. Norma mengenai “tempat perdagangan dilarang membiarkan penjualan dan/atau penggandaan barang hasil pelanggaran Hak Cipta dan/atau Hak Terkait di tempat perdagangan yang dikelolanya” bertentangan dengan UUD 1945 dan tidak mempunyai kekuatan hukum mengikat sepanjang tidak dimaknai, “Pengelola tempat

perdagangan dan/atau Platform Layanan Digital berbasis *User Generated Content* (UGC) dilarang membiarkan penjualan, penayangan, dan/atau penggandaan barang hasil pelanggaran Hak Cipta dan/atau Hak Terkait di tempat perdagangan dan/atau Layanan Digital yang dikelolanya”.

g. KUHP

Pasal 536b KUHP Baru mengatur bahwa pejabat yang melampaui kewenangannya meminta sistem elektronik memberikan dokumen dan informasi elektronik mengenai komunikasi yang terjadi melalui jejaring sistem elektronik tersebut dipidana dengan pidana penjara paling lama 3 (tiga) tahun atau pidana denda paling banyak kategori IV. Ketentuan ini memberikan perlindungan atas hak privasi dan informasi, yaitu membatasi pejabat melakukan tindakan sewenang-wenang. Hal yang perlu diwaspadai adalah penggunaan pasal ini untuk pejabat yang berusaha memberikan informasi kepada publik, misalnya tentang korupsi yang dilakukan aparat. Oleh karena itu, penggunaan ketentuan ini perlu mengacu kepada instrumen HAM dan kepentingan publik.

KUHP tidak hanya dapat digunakan untuk orang di Indonesia, tetapi juga menasar setiap orang yang berada di luar wilayah Indonesia yang melakukan tindak pidana terhadap kepentingan Negara Kesatuan Republik Indonesia (NKRI) yang berhubungan dengan

“keselamatan atau keamanan sistem komunikasi elektronik”.⁹⁶ KUHP memberikan penjelasan bahwa ketentuan ini dimaksudkan untuk “melindungi kepentingan hukum negara atau kepentingan nasional tertentu di luar negeri”. Apa yang dimaksud dengan kepentingan nasional tertentu yang ingin dilindungi dalam ketentuan ini, “menggunakan perumusan yang limitatif dan terbuka”. Selanjutnya penjelasan ini menyatakan:

“Artinya, ruang lingkup kepentingan nasional yang akan dilindungi ditentukan secara limitatif, tetapi jenis Tindak Pidananya tidak ditentukan secara pasti. Penentuan jenis Tindak Pidana yang dipandang menyerang atau membahayakan kepentingan nasional diserahkan dalam praktik secara terbuka dalam batas yang telah ditentukan sebagai tindak pidana menurut hukum pidana Indonesia”.

Penjelasan ini menunjukkan bahwa pasal KUHP memang dimaksudkan untuk menjadi ketentuan yang longgar. Alasan pembuat undang-undang adalah:

“Perumusan limitatif yang terbuka ini dimaksudkan untuk memberikan fleksibilitas praktik dan dalam perkembangan formulasi Tindak Pidana oleh pembentuk Undang-Undang pada masa yang akan datang”.

Hukum pidana memiliki prinsip legalitas. Naskah akademik RUU KUHP menyebutkan asas ini berasal dari doktrin *nullum delictum nulla poena sine praevia*

lege poenali, yaitu tiada tindak pidana dan hukuman pidana tanpa sebelumnya ditetapkan dalam suatu undang-undang.⁹⁷ Asas ini terdiri dari *stricta (strict)*, *scripta (written)*, dan *certa (settled)*, yaitu:

“Undang-undang yang memenuhi syarat legalitas karena sudah ada sebelumnya, dipublikasikan, jelas, dan berwenang untuk menentukan legalitas atau ilegalitas suatu tindakan. Kriteria ini sering dianggap sebagai prasyarat untuk menetapkan terdakwa bertanggung jawab atas suatu tindakan pidana berdasarkan asas-asas hak asasi manusia tentang proses hukum yang wajar”.⁹⁸

Ketidakpastian jenis tindak pidana ini berpotensi menimbulkan kriminalisasi, meskipun pembuat KUHP beralih demikian:

“Fleksibilitas itu tetap dalam batas kepastian menurut ketentuan peraturan perundang-undangan. Penentuan Tindak Pidana yang menyerang kepentingan nasional hanya terbatas pada perbuatan tertentu yang sungguh-sungguh melanggar kepentingan hukum nasional yang dilindungi”.

Masalah pertama adalah pada penentuan kepentingan hukum nasional, bagaimana akuntabilitas bahwa suatu hal memang masuk pada kepentingan hukum nasional. Masalah kedua ada pada kepentingan hukum nasional yang dilindungi. Setelah memenuhi kriteria hukum nasional, bagaimana menentukan

bahwa hukum nasional tersebut masuk dalam yang dilindungi. Ketiga adalah mengenai kata “sungguh-sungguh”, bagaimana ukuran “sungguh-sungguh” itu?

Hak menyampaikan pendapat dalam Kovenan Hak Sipil dan Politik dibatasi dalam Pasal 19 ayat (3) yang lengkapnya sebagai berikut:

Pelaksanaan hak yang dicantumkan dalam ayat 2 pasal ini menimbulkan kewajiban dan tanggung jawab khusus. Oleh karenanya dapat dikenai pembatasan tertentu, tetapi hal ini hanya dapat dilakukan sesuai dengan hukum dan sepanjang diperlukan untuk: (a) menghormati hak atau nama baik orang lain; (b) melindungi keamanan nasional atau ketertiban umum atau kesehatan atau moral umum.

Unsur keperluan pembatasan paling dekat tampaknya pada keamanan nasional. Penjelasan mengenai keamanan nasional dapat dilihat dalam Siracusa Principles, yang salah satunya membatasi bahwa keamanan nasional hanya dapat digunakan untuk membenarkan tindakan pembatasan hak-hak tertentu jika tindakan tersebut dilakukan untuk melindungi keberadaan bangsa atau integritas teritorial atau kemerdekaan politiknya dari kekerasan atau ancaman kekerasan.⁹⁹ Keamanan nasional ini tidak dapat dijadikan alasan untuk memberlakukan pembatasan demi mencegah ancaman lokal atau ancaman yang relatif terisolasi terhadap hukum dan ketertiban.¹⁰⁰ Selain itu

keamanan nasional tidak dapat digunakan sebagai dalih untuk memaksakan pembatasan yang tidak jelas atau sewenang-wenang.¹⁰¹

Hak atas kebebasan berpendapat termasuk informasi seharusnya merupakan hal penting yang juga menjadi nilai pengaturan sistem komunikasi elektronik. KUHP saat ini lebih menitikberatkan kepentingan negara, dalam hal ini keamanan elektronik, daripada hak atas kebebasan.

Ketentuan kedua dalam KUHP yang berpotensi negatif adalah Pasal 157 yang secara lengkap mengatur tentang ancaman kekerasan, yaitu:

“Setiap perbuatan berupa ucapan, tulisan, gambar, simbol, atau gerakan tubuh, baik dengan maupun tanpa menggunakan sarana dalam bentuk elektronik atau nonelektronik yang dapat menimbulkan rasa takut, cemas, atau khawatir akan dilakukannya Kekerasan”.

Maksud untuk melindungi orang dari ancaman kekerasan dapat berujung pada kriminalisasi karena pengaturan yang terlalu luas. Ketentuan ini memerlukan panduan atau penjelasan untuk membuktikan rasa takut, cemas atau khawatir ini.

Ketentuan selanjutnya adalah Pasal 258 ayat (1) yang mengatur larangan setiap orang secara melawan hukum mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak

bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel. Masalah dalam ketentuan ini adalah adanya kemungkinan pemerintah menentukan suatu informasi tertutup padahal menyangkut kepentingan publik, sehingga seharusnya dapat diketahui umum. Akibatnya, ketika ada orang yang mengakses informasi atau dokumen tersebut, maka ia masuk kategori orang yang melakukan larangan dalam Pasal 258 ayat (1) ini.

Pasal berikutnya yang berpotensi menjerat kriminalisasi adalah Pasal 332 ayat (1). Larangan dalam pasal ini adalah orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun. Ada kemungkinan "orang lain" dalam pasal ini diberlakukan untuk pejabat publik. Perlu diperjelas bahwa orang lain tidak bisa mencakup pejabat publik dengan informasi mengenai kepentingan publik.

Masalah kelima terletak dalam Pasal 332 ayat (2) yang mengatur setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik. "Cara apapun" berpotensi diartikan meluas dan mungkin menimbulkan kriminalisasi.

Masalah berikutnya ada pada Pasal 333 yang secara keseluruhan berpotensi ditafsirkan secara luas. Sayangnya, tidak ada

penjelasan untuk Pasal 333. Ketentuan yang paling jelas bermasalah adalah ayat c, yaitu *"tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer atau sistem elektronik yang dilindungi oleh negara"*. Ketiadaan kriteria tentang komputer atau sistem elektronik yang dilindungi oleh negara membuat pidana dalam pasal ini langsung berlaku meskipun negara melindungi sistem elektronik yang seharusnya tidak perlu dilindungi. Pengaturan yang meluas juga ada dalam Pasal 333 huruf d, yaitu tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik milik pemerintah. "Tanpa hak" bahkan bisa bermakna tanpa izin. Hal serupa juga ada dalam Pasal 333 huruf e yang mempidanakan orang *"tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan komputer atau sistem elektronik tersebut menjadi rusak"*. Ketentuan huruf f dalam pasal juga serupa, yaitu memengaruhi atau mengakibatkan terganggunya komputer atau sistem elektronik yang digunakan oleh pemerintah. Cakupan "memengaruhi" dalam ayat ini tidak jelas, sehingga berpotensi diimplementasikan secara luas.

Pasal 333 ayat (3) juga berpotensi meluas, tetapi dalam konteks sistem elektronik masyarakat. Tepatnya, ayat ini mempidanakan

orang yang “*tanpa hak atau melampaui wewengangnya menggunakan atau mengakses komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan komputer atau sistem elektronik tersebut menjadi rusak*”. Sama seperti ketentuan di atas, apa yang dimaksud sebagai “tanpa hak” maupun “menggunakan” bisa diartikan secara luas.

h. UU Keterbukaan Informasi Publik

Keterbukaan informasi publik tentu suatu hal yang positif karena bermanfaat, salah satunya untuk membatasi penyalahgunaan kekuasaan. Pasal 1 angka 1 UU Keterbukaan Informasi Publik memberikan definisi bahwa dalam Undang-Undang ini, yang dimaksud dengan: Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun nonelektronik.

Ketentuan ini menjamin hak setiap orang untuk informasi menjadi lebih luas karena memberikan akses informasi melalui ragam bentuk. Informasi elektronik membuat informasi dapat diakses dari jarak jauh. Sayangnya, pengaturan ini masih bersifat umum, sehingga tergantung dari penyedia informasi. Informasi elektronik yang bersifat umum

dapat mengesampingkan penyandang disabilitas, misalnya teman netra yang tidak bisa melihat. Ke depan, undang-undang ini perlu menambahkan kewajiban penyedia informasi menyediakan dalam bentuk yang dapat diakses oleh ragam penyandang disabilitas, sehingga tidak hanya dalam bentuk tulisan atau visualisasi, tetapi juga suara.

i. UU Pemilu

Pasal 536 UU Pemilu memberikan perlindungan melalui pidana terhadap orang yang dengan sengaja merusak, mengganggu, atau mendistorsi sistem informasi penghitungan suara hasil Pemilu. Ancamannya pidana penjara paling lama 3 (tiga) tahun dan denda paling banyak Rp36.000.000,00 (tiga puluh enam juta rupiah). Pasal 280 (4) UU Pemilu mengharuskan media, termasuk media daring, untuk mematuhi larangan dalam kampanye pemilu. Di antara larangan tersebut terdapat beberapa ketentuan yang dapat ditafsir secara luas, salah satunya mempersoalkan dasar negara Pancasila, Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, dan bentuk NKRI.¹⁰² Penjelasan ayat ini menyatakan sudah jelas, tetapi kata “mempersoalkan” memiliki arti yang luas. Kritik, misalnya, termasuk dalam “mempersoalkan”. Saat seseorang mengkritik penafsiran resmi Pancasila oleh pemerintah, maka kemungkinan ia dapat terjerat ketentuan ini dalam kampanye pemilu.

Ketentuan berikutnya yang berpotensi menimbulkan masalah adalah Pasal 280 ayat (1) huruf b yang mengatur larangan “melakukan kegiatan yang membahayakan keutuhan Negara Kesatuan Republik Indonesia”, huruf c mengatur tentang “menghina seseorang, agama, suku, ras, golongan, calon, dan/atau peserta pemilu yang lain”, dan huruf e mengatur, “menggangu ketertiban umum”. Tiga ketentuan ini dapat ditafsirkan secara luas.

Dalam Pasal 280 ayat (1) huruf b, kata “membahayakan” bisa diartikan secara luas karena disambungkan dengan kata abstrak, yaitu “keutuhan Negara”. Mari bandingkan dengan “membahayakan keselamatan orang di jalan”. Kalimat terakhir memiliki makna yang lebih jelas. Hal serupa terjadi pada Pasal 280 ayat (1) huruf c. Menghina bisa ditafsirkan secara subjektif dari sisi orang yang merasa terhina. Kritik seperti menyatakan calon lain berasal dari partai politik yang korup, sangat mungkin dikategorikan sebagai penghinaan. Terlebih Putusan MK Nomor 76/PUU/XV/2017 telah memaknai antargolongan sebagai: “tidak hanya meliputi suku, agama, ras, melainkan meliputi lebih dari itu yaitu semua entitas yang tidak terwakili atau terwadahi oleh istilah suku, agama dan ras”. Putusan MK ini, oleh karena itu, dapat menjadi dasar perluasan makna antargolongan, sehingga partai politik dapat masuk ke dalamnya.

Pasal 280 ayat (1) huruf e memiliki penjelasan bahwa “yang dimaksud dengan “ketertiban umum” adalah suatu keadaan yang memungkinkan penyelenggaraan pemerintahan, pelayanan umum, dan kegiatan masyarakat dapat berlangsung sebagaimana biasanya”. Secara umum, penjelasan ini tampak tidak memiliki masalah, tetapi jika diperhatikan, frasa “kegiatan masyarakat dapat berlangsung sebagaimana biasanya” bermakna terlalu luas. Misalnya, jalan yang beberapa ruas jalannya tidak dapat dipakai karena demonstrasi, juga dapat diartikan tidak dapatnya kegiatan masyarakat berlangsung sebagaimana biasanya.

j. UU Perlindungan Data Pribadi

Undang-undang ini memberikan beberapa perlindungan terhadap data digital. Pasal 6 - Pasal 11 memberikan hak kepada subjek data pribadi untuk: (1) melengkapi, memperbarui, memperbaiki kesalahan/ketidakkuratan; (2) mendapat akses dan memperoleh salinan data pribadi tentang dirinya; (3) mengakhiri pemrosesan, menghapus dan memusnahkan data; serta (4) menarik persetujuan pemrosesan data pribadi. Selain itu, Pasal 13 mengatur hak subyek data pribadi untuk mendapat dan menggunakan data pribadi tentang dirinya dari pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.

Pelindungan berikutnya terkait dengan pemrosesan data pribadi. Pasal 34 ayat (1) mewajibkan Pengendali Data Pribadi melakukan penilaian dampak Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi. Ayat berikutnya memberikan cakupan tentang pemrosesan Data Pribadi yang memiliki potensi risiko tinggi mulai dari pengambilan keputusan, pemrosesan dan penggunaan. Pengambilan keputusan yang dimaksud adalah pengambilan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi. Pemrosesan terdiri atas pemrosesan Data Pribadi yang bersifat spesifik, Data Pribadi dalam skala besar, Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi, pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data, dan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi. Adapun penggunaan terkait teknologi baru dalam pemrosesan Data Pribadi. Sayangnya, ketentuan lebih lanjut mengenai penilaian dampak pelindungan data pribadi tersebut diatur dalam Peraturan Pemerintah.

UU Pelindungan Data Pribadi bermaksud “menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan

*penghormatan atas pentingnya pelindungan data pribadi”.*¹⁰³

Walaupun demikian, undang-undang ini memiliki beberapa ketentuan yang sekilas terlihat berisi proteksi, tetapi sesungguhnya berpotensi mengancam keamanan digital. Pasal 65 berisi tiga larangan, yaitu: (1) melarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi;¹⁰⁴ (2) mengungkapkan Data Pribadi yang bukan miliknya;¹⁰⁵ dan menggunakan Data Pribadi yang bukan miliknya.¹⁰⁶ Masalah pada ketentuan ini adalah pada pemaknaan “melawan hukum”. Ketentuan ini dapat dikenakan kepada orang yang melakukan advokasi terhadap isu sosial, termasuk advokasi isu anti korupsi.

3. Kebebasan Berekspresi (*Liberty*)

Dalam pemetaan yang dilakukan terhadap regulasi *existing* yang terkait dengan tata kelola internet di Indonesia, khususnya aspek kebebasan berekspresi atau “*liberty*”, ditemukan terdapat tujuh undang-undang terkait, yaitu UU Pemilu, UU Pilkada, UU Pers, UU Keterbukaan Informasi Publik, UU ITE, UU Pornografi, dan KUHP Baru. Terhadap sejumlah regulasi tersebut, tolok ukur analisa dilakukan dengan mendasarkan pada prinsip liberty pada ICRP, sebagai cerminan dari hak atas kebebasan berpendapat dan berekspresi, sebagaimana telah dimuat dalam UDHR¹⁰⁷ dan ICCPR.¹⁰⁸ Lebih jauh, prinsip ini juga menegaskan bahwa kebebasan merupakan hal yang esensial

hadir dalam masyarakat untuk mengejawantahkan hak asasi manusia dan demokrasi. Hal tersebut meliputi (1) hak atas online protest; (2) kebebasan dari sensor, termasuk pemblokiran, serangan siber, online harassment; (3) hak terhadap informasi, (4) kebebasan media; dan (5) kebebasan dari hate speech.

Jaminan kebebasan yang ditemukan dalam undang-undang terkait bernilai minim. Hal ini menguatkan tesis bahwa tendensi pengaturan ruang digital bersifat proteksionis, sebab orientasi pengaturan ditujukan untuk memperketat pengawasan kepada pengguna, bukan mengakomodasikan dan menjamin hak kebebasan berekspresi di ruang digital.

a. UU Pemilu

Titik tekan pengaturan aspek kebebasan dalam undang-undang ini terdapat pada pelaksanaan kampanye pemilu yang secara langsung dan tidak langsung bersinggungan dengan tata kelola internet. Hal ini diatur dalam Pasal 287 ayat (1), (2), (3), (4), dan (5) UU Pemilu yang berbunyi sebagai berikut:

“(1) Pemberitaan, penyiaran, dan iklan Kampanye Pemilu dapat dilakukan melalui media massa cetak, media daring (online), media sosial, dan lembaga penyiaran sesuai dengan ketentuan

Undang-Undang ini.

(2) Pemberitaan, penyiaran, dan iklan Kampanye Pemilu sebagaimana dimaksud pada ayat (1) dilaksanakan dalam rangka penyampaian pesan Kampanye Pemilu oleh Peserta Pemilu kepada masyarakat.

(3) Pesan Kampanye Pemilu sebagaimana dimaksud pada

ayat (2) dapat berupa tulisan, suara, gambar, tulisan dan gambar, atau suara dan gambar, yang bersifat naratif, grafis, karakter, interaktif atau tidak interaktif, serta yang dapat diterima melalui perangkat penerima pesan.

(4) Media massa cetak, media daring, media sosial, dan lembaga penyiaran dalam memberitakan, menyiarkan, dan mengiklankan Kampanye Pemilu sebagaimana dimaksud pada ayat (1) harus mematuhi larangan dalam Kampanye Pemilu sebagaimana dimaksud dalam Pasal 280.

(5) Media massa cetak, media daring, media sosial, dan lembaga penyiaran sebagaimana dimaksud pada ayat (1) selama Masa Tenang dilarang menyiarkan berita, iklan, rekam jejak Peserta Pemilu, atau bentuk lainnya yang mengarah pada kepentingan Kampanye Pemilu yang menguntungkan atau merugikan Peserta Pemilu”

Ketentuan di atas sangat terkait dengan prinsip kebebasan berekspresi dalam proses kampanye pemilu karena pasal ini menyebutkan secara jelas bahwa pesan kampanye dapat dilakukan secara online melalui internet. Melandaskan pada keterkaitan itu, Pasal 19 UDHR menekankan bahwa setiap orang bebas untuk berekspresi dan berpendapat, termasuk menyatakan pendapat tanpa gangguan, termasuk mencari, menerima, dan menyebarkan informasi dan ide melalui berbagai media dan tanpa mempedulikan batas-batasnya.¹⁰⁹ Meskipun di

samping itu, ICCPR memungkinkan pembatasan terhadap kebebasan berekspresi, tetapi pembatasan hanya dapat dilakukan berdasarkan undang-undang dengan memperhatikan pada batasan hak untuk menghormati hak terhadap reputasi orang lain, atau perlindungan terhadap keamanan nasional, atau kesehatan publik atau moral.

Penyebaran konten kampanye oleh peserta pemilu di internet akan bersinggungan dengan kebebasan berekspresi. UU Pemilu telah memberikan “rambu” implementasi pelaksanaannya, yaitu dalam Pasal 280 ayat (1) UU Pemilu, yang mencakup larangan:

“(a) mempersoalkan dasar negara Pancasila, Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, dan bentuk Negara Kesatuan Republik Indonesia; (b) melakukan kegiatan yang membahayakan keutuhan Negara Kesatuan Republik Indonesia; (c) menghina seseorang, agama, suku, ras, golongan, calon, dan/atau Peserta Pemilu yang lain; (d) menghasut dan mengadu domba perseorangan ataupun masyarakat; (e) mengganggu ketertiban umum; (f) mengancam untuk melakukan kekerasan atau menganjurkan penggunaan kekerasan kepada seseorang, sekelompok anggota masyarakat, dan/atau Peserta Pemilu yang lain; (g) merusak dan/atau menghilangkan alat peraga kampanye Peserta Pemilu; (h) menggunakan fasilitas pemerintah, tempat ibadah, dan tempat pendidikan;

(i) membawa atau menggunakan tanda gambar dan/atau atribut selain dari tanda gambar dan/atau atribut Peserta Pemilu yang bersangkutan; dan (j) menjanjikan atau memberikan uang atau materi lainnya kepada peserta Kampanye Pemilu.”

Substansi pelarangan di atas yang bernilai multitafsir telah dikritisi pada aspek proteksi dan keamanan digital sebelumnya. Pada konteks ini, prinsip kebebasan berekspresi dan berpendapat harus dirasakan setiap individu, mencakup peserta pemilu, maupun masyarakat yang menerima informasi terkait dengan kampanye pemilu. Dengan demikian, sebenarnya ada kaitannya juga dengan hak atas informasi bagi setiap individu, khususnya aksesibilitas informasi kampanye, serta pencegahan dan penegakkan hukum atas materi konten yang mengandung SARA. Saat ini, ketentuan demikian belum cukup dimuat dalam UU Pemilu. Pada sisi yang lain, perlu dilakukan penelaahan lebih dalam terkait implementasinya.

b. UU Pilkada

Serupa dengan UU Pemilu, Pasal 65 ayat (1) huruf f UU Pilkada memuat pengaturan terkait dengan pelaksanaan kampanye yang dilakukan melalui media elektronik dalam pemilihan kepala daerah (Gubernur, Bupati, dan Walikota). Pasal ini menyebutkan, “Kampanye dapat dilaksanakan melalui: f. iklan media massa cetak dan media massa elektronik”. Ketentuan ini menarik

UU Pilkada sebagai salah satu aturan yang tak terhindarkan dari tata kelola internet.

Prinsip kebebasan berekspresi menjadi prinsip utama yang bersinggungan langsung dalam pengaturan ini. Peserta pemilu memiliki hak berekspresi dalam setiap aktivitas kampanye yang dilakukan melalui media elektronik. Hal yang sama berlaku juga bagi masyarakat secara umum di luar peserta pemilu. Ekspresi dan opini sebagai reaksi atas implementasi kebebasan berekspresi dari para peserta pemilu melekat pada masyarakat, bahkan media, sebagai pihak yang melakukan penyebarluasan gagasan dan informasi peserta pemilu kepada masyarakat secara luas. Dalam prinsip ini, kebebasan berekspresi tidak serta merta berdiri sendirian. Sebagai hak dasar, ia bersinggungan langsung maupun tidak langsung dengan kebebasan lain seperti kebebasan atas protes secara online, kebebasan dari tindakan penyensoran, kebebasan atas pers dan media, hak atas informasi, dan kebebasan dari ujaran kebencian.

Kendati demikian, UU Pilkada tidak spesifik menerangkan rambu terhadap pelaksanaan kampanye melalui media elektronik. Pasal 65 ayat (2) hanya menyebutkan bahwa pelaksanaan kampanye yang dilaksanakan melalui iklan media massa cetak dan media massa elektronik difasilitasi oleh KPU Provinsi dan KPU Kabupaten/Kota yang didanai oleh Anggaran Pendapatan dan Belanja Daerah. Implementasi

batasan SARA tidak dimuat dalam undang-undang, tetapi prinsip yang dimuat dalam UU Pemilu dan undang-undang lain¹⁰ dapat dikaitkan ke dalam konteks penyelenggaraan pilkada.

C. UU Pers

UU Pers merupakan salah satu peraturan yang melandasi pemenuhan hak bagi jurnalis maupun media. Pasal 4 UU Pers secara jelas menyebutkan bahwa:

“1. Kemerdekaan pers dijamin sebagai hak asasi warga negara. 2. Terhadap pers nasional tidak dikenakan penyensoran, pembredelan atau pelarangan penyiaran. 3. Untuk menjamin kemerdekaan pers, pers nasional mempunyai hak mencari, memperoleh, dan menyebarluaskan gagasan dan informasi. 4. Dalam mempertanggungjawabkan pemberitaan di depan hukum, wartawan mempunyai Hak Tolak.”

Melalui pasal ini, negara menjamin perlindungan dan pemenuhan hak atas kebebasan pers dengan melakukan pelarangan terhadap penyensoran, pembredelan, dan pelarangan penyiaran. Bahkan, secara jelas disebutkan bahwa jurnalis memiliki hak untuk mencari, memperoleh, dan menyebarluaskan gagasan dan informasi, serta hak tolak.

Hal demikian sangat terkait dengan prinsip kebebasan berekspresi, yang menjadi salah satu prinsip penting dalam tata kelola internet, termasuk di

dalamnya adalah kebebasan dari penyensoran, kebebasan media, dan hak terhadap informasi. Secara umum, Pasal 4 UU Pers telah sejalan dengan ICRP dengan memuat ketentuan yang menjamin perlindungan terhadap kebebasan pers. Akan tetapi, kewajiban negara sebagai pemangku utama dalam perlindungan hak asasi manusia belum sepenuhnya terejawantahkan, baik dari aspek normatif apalagi implementatif.

Negara memiliki kewajiban untuk menghormati (*to respect*) dalam hukum HAM internasional belum sepenuhnya dimuat. Prinsip ICRP mendudukan kebebasan media dengan menjelaskan bahwa keberagaman media harus dihargai dengan mengacu pada perlindungan dan penghormatan hak-hak yang dimuat dalam ICCPR. Lebih lanjut, ICRP juga mendudukan kebebasan dari penyensoran kepada setiap orang (tak terbatas pada media), untuk menggunakan internet tanpa sensor dalam bentuk apapun. Jadi, ketika terjadi tindakan penyensoran terhadap suatu informasi atau gagasan tertentu, hal ini bukan hanya melanggar kebebasan pers, tetapi juga hak bagi setiap individu untuk mengakses informasi dan bebas dari penyensoran dalam bentuk apapun. Tindakan ini termasuk juga pada jenis tindakan yang memungkinkan dilakukan untuk mengintimidasi pengguna internet atau membatasi ekspresi secara online yang mencakup kebebasan dari serangan siber dan kebebasan dari pelecehan secara *online*. Penghormatan dan perlindungan semacam tidak

cukup tersentuh dalam UU Pers melalui Pasal 4, pasal lain, maupun penjelasan pasalnya.

d. UU Keterbukaan Informasi Publik

Peraturan lain yang masuk ke dalam cakupan tata kelola internet adalah UU Keterbukaan Informasi Publik, yaitu dalam Pasal 7 ayat (6) dan Pasal 54 ayat (1). Kedua pasal ini secara langsung berkaitan dengan prinsip kebebasan, khususnya dalam hak atas informasi. Melalui pasal ini, Badan Publik (pemerintah) mendapat kewenangan untuk menyediakan informasi melalui media elektronik. Pasal 7 ayat (6) UU Keterbukaan Informasi Publik menyebutkan sebagai berikut:

“Dalam rangka memenuhi kewajiban menyediakan informasi yang akurat, benar dan tidak menyesatkan, membangun dan mengembangkan sistem informasi dan dokumentasi untuk mengelola Informasi Publik secara baik dan efisien sehingga dapat diakses dengan mudah, serta membuat pertimbangan secara tertulis setiap kebijakan yang diambil untuk memenuhi hak setiap Orang atas Informasi Publik, Badan Publik dapat memanfaatkan sarana dan/atau media elektronik dan nonelektronik.”

Sementara itu, Pasal 54 ayat (1) UU KIP menyebutkan sebagai berikut:

“Setiap Orang yang dengan sengaja dan tanpa hak

mengakses dan/atau memperoleh dan/atau memberikan informasi yang dikecualikan sebagaimana diatur dalam Pasal 17 huruf a, huruf b, huruf d, huruf f, huruf g, huruf h, huruf i, dan huruf j dipidana dengan pidana penjara paling lama 2 (dua) tahun dan pidana denda paling banyak Rp 10.000.000,00 (sepuluh juta rupiah).”

Pasal ini memberikan batasan terhadap penyebarluasan informasi tertentu atau terhadap pemenuhan hak atas informasi. Ini diatur dalam Pasal 17 UU Keterbukaan Informasi Publik yang terkait dengan: (1) informasi publik yang dapat menghambat proses penegakan hukum;¹¹¹ (2) informasi publik yang dapat mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dan persaingan usaha tidak sehat;¹¹² (3) informasi publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat membahayakan pertahanan dan keamanan negara;¹¹³ (4) Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkapkan kekayaan alam Indonesia; (5) Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan ketahanan ekonomi nasional; (6) Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik, dapat merugikan kepentingan hubungan luar negeri; (7) Informasi Publik yang apabila dibuka dapat mengungkapkan isi akta otentik yang bersifat pribadi dan

kemauan terakhir ataupun wasiat seseorang; (8) Informasi Publik yang apabila dibuka dan diberikan kepada Pemohon Informasi Publik dapat mengungkap rahasia pribadi; (9) memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan; dan (10) informasi yang tidak boleh diungkapkan berdasarkan Undang-Undang.

Pada dasarnya, pemenuhan hak atas informasi mendasari hak bahwa semua orang memiliki hak untuk mencari, menerima, dan menyebarkan informasi dan gagasan melalui internet.¹¹⁴ Sejalan dengan hal tersebut, maka semua orang memiliki hak untuk mengakses, mendapat informasi, terkait dengan pemerintahan atau informasi publik yang disebarkan oleh pemerintah secara tepat waktu, dengan cara yang dapat diakses berdasarkan hukum nasional dan internasional.¹¹⁵

Menelaah kedua pasal tersebut di atas, pasal tersebut banyak bersinggungan dengan pengaturan hak atas informasi dalam prinsip kebebasan berekspresi sebagaimana dikandung dalam ICRP. Pertama, penggunaan kata “dapat” dalam Pasal 7 ayat (6) UU Keterbukaan Informasi Publik memiliki celah kepada badan publik untuk menyediakan informasi secara elektronik. Padahal, dalam prinsip tata kelola internet, pemenuhan hak atas informasi, termasuk penyediaan informasi elektronik,

seharusnya menjadi kewajiban yang harus dipenuhi oleh Badan Publik, mengingat perkembangan penggunaan teknologi informasi pasca pandemi COVID-19 menjadi sangat pesat dan menjadi kebutuhan di Indonesia.

Kedua, hukuman pengecualian dalam Pasal 54 ayat (1) yang berkaitan dengan Pasal 17 UU Keterbukaan Informasi Publik. Pasal ini kental bersinggungan dengan pemenuhan hak bagi setiap orang atas informasi, termasuk untuk menyebarkan informasi. Pasal ini berpeluang membatasi hak atas informasi, baik mendapat maupun menyebarkan, dengan dalih bahwa informasi-informasi tersebut dikategorikan sebagai informasi yang dikecualikan. Merujuk pada Pasal 17, pengecualian terhadap informasi publik masih dilihat samar. Misalnya, Pasal 17 huruf c angka 7 yang masih cenderung umum karena berisi pembatasan informasi yang menyangkut sistem intelijen negara. Belum lagi, Pasal 17 huruf b yang dalam praktiknya sering dijadikan landasan dalam membatasi informasi perizinan perusahaan yang berkaitan dengan izin dan potensi kerusakan alam yang ditimbulkan atas aktivitas bisnis tertentu.

Meskipun pada sisi yang lain, pengecualian dalam Pasal 17 telah melandasi perlindungan terhadap hak atas privasi masyarakat, khususnya Pasal 17 huruf g dan huruf h UU Keterbukaan Informasi Publik. Hal ini patut mendapat apresiasi dan pengawalan terhadap

implementasinya dalam melindungi hak atas privasi masyarakat.

e. UU Pornografi

Keterkaitan UU Pornografi dengan tata kelola internet secara khusus ada pada ketentuan penyebarluasan informasi bermuatan pornografi yang dimuat di media elektronik, khususnya dalam Pasal 28 ayat (2), Pasal 31, dan Pasal 32 UU Pornografi. Pasal tersebut bersinggungan dengan pemenuhan hak atas informasi dan kebebasan dari tindakan sensor. Pasal 28 ayat (2) UU Pornografi memberi kewenangan kepada penuntut umum untuk melakukan pemusnahan pornografi, dengan membuat berita acara yang sekurang-kurangnya memuat nama media elektronik yang penyebarluaskan pornografi. Sejalan dengan ketentuan tersebut, Pasal 31 dan 32 UU Pornografi memuat sanksi pidana kepada setiap orang yang meminjamkan atau mengunduh pornografi, bahkan orang yang memperdengarkan, mempertontonkan, memanfaatkan, memiliki, atau menyimpan produk pornografi.

Ketiga pasal ini bersinggungan dengan hak bagi setiap orang untuk mengakses informasi, yang dalam hal ini terkait dengan akses informasi terkait seksualitas. UU Pornografi memberi definisi pornografi yang sangat luas, bahkan menyangkut pada pengendalian moralitas individu. Merujuk pada Pasal 1 angka 1 UU

Pornografi, cakupan pornografi termasuk pada gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat. Definisi ini terlalu luas karena melandasi definisinya pada “norma kesusilaan” yang longgar, sehingga pada saat yang sama akan bertentangan dengan hak atas informasi—termasuk mengenai seksualitas, dan kebebasan media (yang menyebarkan informasi terkait seksualitas) terhadap penyensoran.

Padahal, jika kembali merujuk pada pedoman pengaturan prinsip tata kelola digital dalam ICRP, setiap orang memiliki hak untuk menggunakan internet tanpa sensor dalam bentuk apapun, termasuk terbebas dari sensor online dan pemblokiran. Pedoman ini menyebutkan bahwa setiap pemblokiran maupun penyaringan yang bertujuan mencegah akses terhadap konten (termasuk konten informasi edukasi seksualitas) adalah tindakan yang tidak dapat dibenarkan. Di samping itu, setiap orang memiliki hak untuk mencari, menerima, dan menyebarkan informasi (termasuk tentang seksualitas) ke internet. Pengaturan dalam Pasal 28 ayat (2), Pasal 31, dan Pasal 32 UU Pornografi, dengan definisi pornografi yang sangat meluas,

sama sekali belum mengakomodasikan hak atas informasi dan kebebasan dari penyensoran.

e. KUHP

KUHP menjadi salah satu undang-undang dengan pasal yang banyak bersinggungan dengan tata kelola internet dan prinsip kebebasan berekspresi dalam ICRP. Ketentuan ini ada dalam Pasal 158, Pasal 258 ayat (1), Pasal 332 ayat (1), (2), dan (3), dan Pasal 335 KUHP.

Umumnya, pasal-pasal ini terkait definisi muka umum yang menarik media elektronik sebagai “ruang” umum berisi informasi maupun dokumen elektronik, penyadapan,¹¹⁷ mengakses komputer dan/atau sistem elektronik milik orang lain dengan tanpa hak atau secara melawan hukum,¹¹⁸ dan menggunakan atau mengakses komputer atau sistem elektronik untuk memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah dengan tanpa hak atau secara melawan hukum.¹¹⁹

Terkait dengan Pasal 158 KUHP, dapat dilihat bahwa definisi “di muka umum” dalam pasal ini tidak membedakan antara orang yang memang melakukan tindakan agar informasi atau dokumen elektronik dapat diketahui orang lain atau yang tidak dimaksudkan untuk diketahui orang lain, tetapi dapat diketahui. Hal demikian bersinggungan kuat dengan kebebasan dan hak atas privasi bagi setiap orang. Perlu penjelasan lebih lanjut agar dapat membedakan antara korban yang

informasi atau dokumen elektroniknya dibuat diketahui orang lain, dengan pelaku yang membuat orang lain mengetahui atau melihat informasi atau dokumen elektronik itu.

Sementara itu, Pasal 258 ayat (1) KUHP berkaitan dengan penghormatan dan pemenuhan hak atas informasi. Dalam peraturan ini, perlu untuk melihat kemungkinan seseorang mendengarkan secara melawan hukum tanpa sengaja. Kemudian, ada kemungkinan bahwa pemerintah menentukan suatu informasi tertutup padahal menyangkut kepentingan publik, sehingga seharusnya dapat diketahui umum. Dengan demikian, perlu adanya perbedaan antara orang yang melakukan secara sengaja dengan tidak. Lebih lanjut, masih terkait dengan singgungannya terhadap hak atas informasi, Pasal 332 ayat (1) KUHP juga memiliki keterkaitan yang sama. Ketentuan ini perlu melihat kemungkinan bahwa "orang lain" yang dicantumkan dalam pasal ini, diberlakukan pula untuk pejabat publik, sehingga terhadap informasi yang mengenai kepentingan publik, harusnya dapat dikecualikan.

Lebih lanjut, Pasal 332 ayat (2) KUHP yang bersinggungan langsung dengan hak atas perlindungan hukum dan bebas dari diskriminasi. Penggunaan frasa "cara apapun" dalam pasal ini berpotensi diartikan meluas dan menimbulkan kriminalisasi. Sementara pada Pasal 333 ayat (3) KUHP, "cara apapun"

berpotensi diartikan meluas dan mungkin menimbulkan kriminalisasi, apalagi jika disambungkan dengan kata "melanggar" dan "melampaui". Hal demikian berpotensi melanggar hak atas informasi dan kepastian hukum. Masalah lain juga terlihat dalam Pasal 335 KUHP yang berpotensi menjadi masalah apabila pemerintah menentukan informasi yang seharusnya hak publik menjadi suatu informasi yang dirahasiakan. Ini akan berkaitan erat dengan prinsip kebebasan dalam tata kelola internet dalam ICRP, khususnya dalam hal hak atas informasi. Untuk mengimplementasikan pasal ini, perlu menyesuaikan dan mengacu pada instrumen hak asasi manusia.

UU ITE

Dua pasal populer dalam UU ITE memiliki keterkaitan yang sangat kuat dengan prinsip tata kelola internet dan singgungannya dengan prinsip kebebasan itu sendiri, yaitu Pasal 27A dan Pasal 28 ayat (3) UU ITE. Kedua pasal ini terkait dengan penyerangan kehormatan atau nama baik seseorang, dan pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat. Pertama, terkait dengan Pasal 27A UU ITE yang merupakan versi baru dari pengaturan Pasal 27 UU ITE yang lama (telah dicabut dalam perubahan kedua). Kendati muatan pasal dalam 27A UU ITE lebih jelas daripada Pasal 27 UU ITE yang lama, tetapi frasa "menyerang kehormatan" tetap bersifat luas dan multitafsir. Di samping itu, perlu dikritisi pula

bahwa penyerangan kehormatan atau nama baik orang seharusnya tidak dihukum penjara untuk mencegah kriminalisasi terhadap ekspresi tertentu. Kalaupun ketentuan ini diatur sebagai hukum pidana, hukuman seharusnya berupa denda.

Kedua, terkait dengan Pasal 28 ayat (3) UU ITE yang terkait dengan larangan terhadap kebebasan berpendapat, yang mencakup pada lingkup digital. Ketentuan larangan terhadap kebebasan berpendapat dalam pasal ini harusnya hanya berlaku untuk *hate speech*, yang di dalamnya juga mengandung pernyataan rasis atau menyinggung SARA. Kata “menimbulkan” dalam pasal ini bersifat multitafsir karena dapat diartikan bahwa apabila ada orang yang tersinggung dengan informasi yang disebarkan, kemudian membuat keonaran. Dengan demikian, dalam hal ini, perlu ditekankan bahwa informasi yang disebarkan merupakan *hate speech* yang mengandung SARA dengan tujuan untuk menimbulkan kerusuhan.

h. UU Pembentukan Peraturan Perundang-undangan

Keterkaitannya pasal ini dengan prinsip tata kelola internet adalah terkait dengan hak atas informasi yang menjadi bagian dalam prinsip kebebasan berekspresi dalam ICRP, yaitu berada dalam Pasal 88 ayat (1), khususnya bagian penjelasan. Peraturan ini memberikan kewajiban bagi DPR dan Pemerintah untuk melakukan penyebarluasan mengenai proses

pembentukan perundang-undangan melalui media elektronik dan/atau media cetak. Ketentuan ini sangat terkait dengan pemenuhan hak atas informasi yang melandasi bahwa setiap orang memiliki hak untuk mengakses secara efektif informasi dari pemerintah, yang harus diberitahukan secara tepat waktu dan dapat diakses oleh masyarakat.¹²⁰ Penggunaan “dan/atau” memberi peluang pada DPR dan Pemerintah untuk hanya menggunakan salah satu media saja (elektronik atau cetak). Padahal dalam praktiknya, penggunaan media cetak dan elektronik harus dimaksimalkan untuk digunakan. Hal demikian dilakukan untuk mengecilkan jarak keterbatasan akses yang dimiliki oleh masyarakat secara umum. Hal tersebut juga ditujukan untuk mewujudkan partisipasi bermakna masyarakat (*meaningful participation*) dalam pembentukan kebijakan.

“
Pada dasarnya, sejumlah peraturan perundang-undangan di Indonesia mengatur tentang pengelolaan internet dan interaksi masyarakat di ruang digital, kendati tak seluruh pengaturan secara eksplisit ditujukan untuk meregulasi interaksi di ruang digital.

Hak Digital untuk
Demokrasi dan
Civic Space:

Studi Pemetaan Regulasi
Internet di Indonesia

06

Implementasi Penegakan Hukum dalam Ruang Digital

6. Implementasi Penegakan Hukum dalam Ruang Digital

“*Dengan sejumlah aturan yang telah dibentuk untuk mengatur ruang digital, penegakkannya juga menjadi satu hal yang perlu diidentifikasi apakah sudah terlaksana sesuai dengan prinsip-prinsip hak asasi manusia.*”

Terlebih, ruang digital memiliki kompleksitas dan perkembangan yang dinamis, sehingga dalam penegakkannya harus dengan mekanisme yang tepat dan juga pembagian kewenangan yang proporsional. Kecenderungan adanya jarak antara norma dengan implementasi juga perlu dilihat dan dievaluasi bagaimana aturan yang telah dibentuk sudah cukup atau belum untuk menjadi dasar penegakkan hukum.

1. Akses Internet

a. Pembatasan Akses Informasi dengan Sensor dan Pemblokiran Konten Media Sosial serta Perlambatan dan Akses Internet

Dalam hal hak atas akses internet, UU ITE merupakan aturan penting yang kemudian memiliki beberapa peraturan turunan. Pada UU ITE, walaupun sifat “autoblokir” ada pada konten perjudian dan pornografi, tetapi kluster jenis konten yang sesuai dengan frasa “*meresahkan masyarakat dan mengganggu ketertiban umum*” masih bermakna luas, sehingga menjadi multitafsir. Peraturan perundang-undangan lainnya atau di bawahnya pun belum dapat menjelaskan frasa tersebut yang berakibat pada adanya potensi gangguan informasi yang rentan mis-*flag*, sehingga terjadi blokir, sensor, dan penurunan konten.

Dampak dari kebijakan autoblokir tersebut misalnya yang terjadi pada September 2023, yang mana terjadi pemblokiran pada situs Google Docs, Sheets, dan Slide. Transparansi dan penjelasan lebih lanjut mengenai pemblokiran situs-situs seperti itu juga sulit untuk didapatkan. Padahal, tata kelola tidak hanya sebatas patroli siber dan pengawasan yang rentan terjerat otoritarianisme digital dengan penurunan atau pemblokiran konten. Pembatasan akses informasi dengan mengandalkan Mesin Pengais Konten Negatif (AIS) milik Kominfo rentan mengalami kesalahan.¹²¹

Pada periode Januari-Maret 2024, hasil pemantauan SAFEnet menemukan adanya gangguan akses terhadap konten individu dan media di laman Facebook dan X (Twitter). Pada 24 Januari 2024, Soe Tjen Marching mendapatkan peringatan dari Twitter perihal permintaan Kominfo untuk menghapus *tweet*-nya. Selain itu, pada Februari 2024 terdapat surat peringatan dari X untuk penghapusan konten (*take down*) kepada dua unggahan Ambrosius Mulait. Dua media berbasis di Papua, yaitu Laolao Papua dan The Papua Journal mengalami gangguan internet terkait sensor dan blokir.¹²²

Berdasarkan data Kominfo, total pemblokiran konten negatif sebanyak 7.378.517 konten. Konten tersebut didominasi sebagai konten yang diklaim bermuatan perjudian sebanyak 3.811.146 konten, pornografi

sebanyak 1.221.241 konten, dan hak kekayaan intelektual sebanyak 20.268 konten. Selanjutnya, konten lainnya adalah yang bermuatan penipuan, konten negatif yang direkomendasikan instansi sektor, terorisme/radikalisme, pelanggaran keamanan informasi, SARA, perdagangan produk dengan aturan khusus, berita bohong atau hoaks, konten yang melanggar nilai sosial dan budaya, konten yang meresahkan masyarakat, separatisme atau organisasi terlarang, pencemaran nama baik, dan kekerasan pada anak.

Pemblokiran konten negatif itu dilakukan di berbagai platform media sosial. X menjadi *platform* dengan penanganan tertinggi, yakni 1.414.789 konten. Selanjutnya, Meta dengan 681.370 konten, file sharing sebanyak 141.457 konten, Google 35.863 konten. Kemudian, diikuti oleh TikTok, Telegram, MiChat, Bigo Live, Mango Live, Snack Video, Hello-App, Thread, AppStore, Line, dan Yahoo.

Tentu saja klaim tersebut menimbulkan berbagai pertanyaan karena kewenangan pemerintah dalam melakukan pemblokiran tersebut didasarkan pada pasal karet atau multitafsir dari Pasal 40 UU ITE. Misalnya, berkaitan dengan konten yang melanggar nilai sosial dan budaya, serta konten yang meresahkan masyarakat yang tidak memiliki tolok ukur tertentu yang jelas.¹²³

Tak hanya sensor dan pemblokiran akses terhadap

konten media sosial, pembatasan terhadap kebebasan sipil juga pernah dilakukan Kominfo dengan melakukan pemblokiran akses internet di Papua.¹²⁴ Pada 21 Agustus - 6 September 2019, Pemerintah melakukan pemblokiran atau pelambatan (*throttling*) koneksi internet di Papua sebagai respon terhadap aksi demonstrasi di Papua Barat. Demonstrasi besar-besaran tersebut dilatarbelakangi oleh adanya tindakan rasisme terhadap sejumlah mahasiswa Papua di Surabaya. Tindakan Pemerintah didasari oleh Pasal 40 ayat (2a) dan (2b) UU ITE. Pengadilan Tata Usaha Negara Jakarta kemudian memutuskan bahwa Presiden Joko Widodo dan Kominfo melakukan perbuatan melanggar hukum, sebab keputusan akses hanya terhadap informasi elektronik dan/atau dokumen elektronik yang “bermuatan melanggar hukum”, tidak mencakup keputusan akses jaringan internet.¹²⁵

b. Disinformasi Pemilu dan Moderasi Konten yang belum Memadai

Terdapat kekosongan hukum terkait disinformasi pemilu, terutama di ruang digital. Pengaturan yang ada saat ini hanya dilekatkan pada manajemen bagi pelaksana kampanye, peserta pemilu, dan tim kampanye.¹²⁶ Kendati UU Pemilu telah mengatur norma larangan menyinggung isu SARA, aturan tersebut belum dapat melindungi kelompok rentan, yaitu

perempuan, kelompok penyandang disabilitas, minoritas beragama dan ras, serta minoritas gender, yang menjadi objek target disinformasi pemilu, ujaran kebencian, *trolling*, dan *doxing*.¹²⁷

Selain itu, tidak terdapat dorongan regulasi dan *political will* KPU dan Bawaslu untuk meminta akuntabilitas dan transparansi *platform* media sosial dalam melakukan penayangan konten kampanye pemilu yang mengandung unsur disinformasi dan misinformasi,¹²⁸ serta mendorong kebijakan efektivitas algoritma dan responsivitas terhadap pengaduan.¹²⁹ Aturan turunan tentang kampanye dalam Peraturan KPU Nomor 15 Tahun 2023 tentang Kampanye Pemilu juga tidak cukup untuk merespon hal tersebut, isu khusus yang diatur di dalamnya terkait dengan pembatasan akun peserta pemilu di setiap *platform* media sosial maksimal 20 (dua puluh) akun dan keterlibatan Komdigi untuk menerima formulir pendaftaran akun media sosial peserta pemilu.

c. Tantangan Akses Informasi Publik

Akses terhadap informasi publik di ruang digital tak selalu disediakan secara wajar oleh badan publik. Misalnya, informasi tentang peserta pemilu dan dana kampanye pemilu. Kasus ini sempat disengketakan oleh Indonesia Corruption Watch (ICW) ke Komisi Informasi Pusat. Pada Pemilu Tahun 2024 lalu, ICW memintakan informasi tentang

dana kampanye, riwayat hidup calon anggota legislatif, dan data tim kampanye kepada KPU, tetapi KPU menolak memberikan informasi karena dianggap sebagai informasi yang dikecualikan.¹³⁰ Terhadap laporan ICW, Komisi Informasi menyatakan bahwa akses ke sistem informasi dana kampanye dan laporan sumbangan dana kampanye adalah informasi yang dikecualikan untuk melindungi privasi, tetapi perihal daftar tim kampanye dan riwayat hidup yang tidak mengandung data pribadi, harus disediakan oleh KPU.¹³¹

Permohonan ICW yang dikabulkan sebagian menjadi titik balik untuk memahami kembali aspek transparansi dan keterbukaan informasi dalam UU Pemilu dan UU Keterbukaan Informasi Publik ketika dibenturkan kepada proteksi data pribadi dalam UU Pelindungan Data Pribadi. Pemahaman demikian malah menghambat akses informasi publik melalui media elektronik untuk mengetahui informasi yang seharusnya disediakan kepada publik secara serta-merta. Perlu terdapat ukuran sejauh mana informasi tergolong sebagai data pribadi. Dalam hal dana kampanye, penting bagi publik untuk mengetahui siapa pihak yang terlibat sebagai donatur sebagai bentuk transparansi dan akuntabilitas pendanaan politik, sebagaimana diamanatkan dalam UU Pemilu. Tanpa adanya ukuran tersebut, badan publik berpotensi untuk mengelak permohonan keterbukaan informasi publik

berlandaskan pemahaman data privasi yang parsial dan tak bertujuan untuk kepentingan publik.

2. Proteksi dan Keamanan Digital

a. Maraknya Kebocoran Data dan Minimnya Akuntabilitas Negara

Berkaitan dengan perlindungan data pribadi, instansi pemerintahan justru yang paling sering mengalami kebocoran data. Pada Maret 2023, *cracker* bernama “Bjorka” diduga membocorkan 19,5 juta data pengguna BPJS Ketenagakerjaan dan dijual di forum gelap. Pada Mei 2023, Lock Bit mencuri 15 juta data nasabah dan 1,5 *terabyte* data internal milik Bank Syariah Indonesia (BSI) dan menyebarkan data yang sudah dienkripsi di *dark web*. Pada bulan November 2023, seorang peretas mengklaim telah membobol situs web resmi milik Kementerian Pertahanan dan mendapatkan sebanyak 1,64 *terabyte* dokumen. Kemudian, pada November 2023, terjadi dugaan kebocoran data pemilih yang dapat mengancam integritas Pemilu 2024, yang ditunjukkan dengan unggahan akun anonim “Jimbo” di BreachForum terkait 252,327,304 data yang diklaim berasal dari situs KPU. Data tersebut dijual seharga US\$74,000 dan terdiri atas Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga, nomor paspor, nama pemilih, tempat pemungutan suara, status difabel, jenis kelamin, tempat dan tanggal lahir, status perkawinan, dan

alamat.¹³²

Pada tahun 2024, serangan siber *ransomware* Lock Bit 3.0 melumpuhkan server Pusat Data Nasional Sementara (PDNS). Dampaknya, sejumlah layanan publik terganggu. Selain itu, pada bulan Agustus diduga terjadi kebocoran 4,7 juta data Nomor Identitas Pegawai Negeri Sipil (NIP) dan NIK milik Aparatur Sipil Negara (ASN) dari Satu Data ASN yang dikelola oleh Badan Kepegawaian Negara (BKN). Pada bulan September, sebanyak enam juta data NPWP diduga bocor.¹³³

b. Proteksi Korban Kekerasan Seksual di Ranah Digital

Berdasarkan laporan pemantauan situasi yang dilakukan oleh SAFEnet pada tahun 2023, angka Kekerasan Berbasis Gender Online (KBGO) yang masuk ke kanal aduan SAFEnet mengalami peningkatan secara signifikan. Laporan di tahun 2023 mencapai angka 1.052 kasus sementara di tahun sebelumnya mencapai 698 kasus dan di tahun 2021 mencapai 667 kasus.¹³⁴ Sementara itu, Komnas Perempuan menerima 1.721 kasus pada tahun 2021, 1697 kasus pada 2022, dan kembali menurun di tahun 2023 sebanyak 1272 kasus. Penurunan kasus yang tercatat di Komnas Perempuan salah satunya adalah faktor disahkannya UU TPKS yang mengakomodasikan penanganan KBGO, sehingga meningkatkan kesadaran publik untuk melaporkan kasusnya menggunakan UU TPKS.¹³⁵

Berdasarkan sebaran usia, korban terbanyak ialah berusia 18-25 tahun dengan total 562 aduan atau 53,42% (lima puluh tiga koma empat puluh dua persen) dari total aduan yang masuk. Sementara usia anak, 12-17 tahun menempati urutan kedua dengan aduan kasus KBGO terbanyak, yaitu mencapai 230 kasus dari total aduan yang masuk ke SAFEnet.

Berdasarkan laporan aduan tersebut dan mengingat tingginya angka korban dengan usia anak, lembaga perlindungan anak ECPAT Indonesia juga menyampaikan tingginya angka eksploitasi seksual anak di *platform* besar seperti META. Peningkatan perlindungan kepada anak di dunia digital harus terus ditingkatkan secara holistik, mulai dari pembuatan kebijakan yang ideal untuk usia anak hingga pengawasan dari orang tua kepada anak dan literasi digital kepada anak sebagai subjek pemakai internet itu sendiri.

Namun demikian, pada kasus KBGO, korban kerap kali mengalami reviktimisasi, salah satunya adalah dilaporkan balik oleh pelaku menggunakan beberapa pasal bermasalah, misalnya menggunakan UU ITE. Reviktimisasi adalah tindakan atau kondisi menempatkan korban kekerasan seksual menjadi korban untuk kedua kalinya atau lebih. Selain menggunakan UU ITE, pada beberapa kasus, korban dijerat menggunakan UU Pornografi karena dianggap bersedia menjadi objek dalam konten intim. Padahal korban

kerap kali dijebak, misalnya tidak menyadari aktivitas seksualnya direkam dan diperjualbelikan. Lapisan konsen pada kasus penyebaran konten intim nonkonsensual sering diabaikan karena berbagai faktor, salah satunya inkompetensi Aparat Penegak Hukum dalam menangani masalah KBGO. Korban dianggap dengan sengaja atau atas persetujuan dirinya menjadi objek atau model yang mengandung muatan pornografi.

Salah satu contoh kasusnya adalah ketika video NI, LM, dan CT tersebar ke publik. NI dikenakan Pasal 29¹³⁶ jo. Pasal 4 UU Pornografi. NI akhirnya dijatuhkan vonis hukuman tiga tahun lima bulan penjara dan denda Rp250 juta rupiah. Ketiga orang tersebut bukanlah penyebar video intim, penyebar video intim tersebut adalah Reza, rekan dari NI. Vonis tersebut dijatuhkan kepada NI karena NI dianggap ceroboh dalam menyimpan rekaman tersebut, NI juga dianggap sebagai publik figur yang tidak bisa memberikan contoh yang baik kepada publik.¹³⁷

UU Pornografi masih memuat sejumlah masalah. Pertama, Pasal 4 ayat (1) dan Pasal 8 UU Pornografi secara berturut-turut menyebutkan:

“Setiap orang dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit

memuat: a. persenggamaan, termasuk persenggamaan yang menyimpang; b. kekerasan seksual; c. masturbasi atau onani; d. ketelanjangan atau tampilan yang mengesankan ketelanjangan; e. alat kelamin; atau f. pornografi anak.”

“Setiap orang dilarang dengan sengaja atau atas persetujuan dirinya menjadi objek atau model yang mengandung muatan pornografi.”

Korban kekerasan seksual seperti NI, LM, dan CT seharusnya mendapat perlindungan hukum dari kasus penyebaran konten intim nonkonsensual. Terminologi pornografi lekat kaitannya dengan industri pembuatan konten yang memang ditujukan untuk kepentingan komersial dan hiburan untuk publik. Sementara itu, di banyak kasus, konten yang dibuat seringkali justru tanpa adanya persetujuan untuk direkam dan/atau disebar, sehingga apabila mengacu pada terminologi pornografi, konten tersebut tidak termasuk dalam kategori.

UU Pornografi menimbulkan disparitas dalam pengaturan hukum di Indonesia dan kerap kali digunakan tanpa memandang KBGO secara holistik, termasuk pada kasus-kasus penyebaran konten intim nonkonsensual. Terlebih, UU Pornografi mengabaikan konsen yang seharusnya dipahami secara substantif dari setiap kasus dan korban.

Alih-alih menggunakan UU Pornografi, sebaiknya Aparat

Penegak Hukum mengarahkan korban ketika melaporkan kasusnya untuk menggunakan UU UU TPKS. Tentu ini berkenaan dengan pencegahan, penanganan, pemulihan, dan penegakan hukum yang bisa dilaksanakan dengan komprehensif dan terintegrasi, dibandingkan dengan menggunakan peraturan perundang-undangan yang lain seperti UU Pornografi atau UU ITE. Alasan lain UU TPKS belum banyak digunakan juga disebabkan oleh belum dilakukannya sosialisasi di seluruh daerah di Indonesia, sehingga Aparat Penegak Hukum belum memiliki pengetahuan dan mekanisme penanganan yang baik, meskipun seharusnya penyidik harus memahami pembaruan hukum. Padahal, implementasi UU TPKS tidak harus menunggu peraturan turunan, melainkan bisa langsung diterapkan secara umum.

Di sisi lain, pembuktian pada kasus kekerasan seksual dinilai lebih sulit dilakukan apabila dibandingkan dengan jenis tindak pidana lainnya. Kerap kali korban melaporkan kasusnya setelah sekian lama terjadi dan tidak menyimpan bukti kejadian, sehingga Aparat Penegak Hukum seringkali menolak laporan korban. Padahal, kekerasan seksual tidak hanya bisa terjadi secara fisik, sehingga pembuktiannya tidak hanya dapat melalui *visum et repertum*, melainkan juga bisa mengandalkan metode pembuktian lainnya, misalnya keterangan ahli kejiwaan

(psikiater) atau menggunakan metode pembuktian dengan cara digital forensik. UU TPKS dinilai lebih ideal dan adil dalam memandang KBGO. Misalnya, Pasal 14 UU TPKS sudah mengakomodasikan beberapa tindak pidana kekerasan seksual yang terjadi di ranah daring atau yang difasilitasi oleh teknologi. Demikian dengan pemenuhan hak korban untuk mendapatkan *Rights to be Forgotten* atau mekanisme penghapusan informasi korban di internet terkait dengan kasus yang pernah terjadi.

Kasus lain yang membuktikan UU ITE tidak bisa melindungi masyarakat sipil dalam memperjuangkan hak dan keadilan dapat dilihat pada kasus Meila Fajriah. Meila adalah Perempuan Pembela HAM, seorang advokat yang menangani dan mendampingi 30 korban kekerasan seksual di Yogyakarta pada tahun 2020. Namun, pada 28 Desember 2021, Meila dilaporkan oleh pelaku kekerasan seksual, Ibrahim Malik, dengan Pasal 27 ayat (3) UU ITE karena menyebut nama Ibrahim Malik dengan jelas dan lengkap dalam konferensi pers yang dilakukan dan diunggah ke kanal Youtube LBH Yogyakarta.¹³⁸ Fenomena ini cukup untuk menjelaskan betapa UU ITE tidak memiliki peran proteksi kepada masyarakat sipil, terlebih pembela HAM. Selain itu, praktik kriminalisasi terhadap Perempuan Pembela HAM dan pendamping korban kekerasan seksual merupakan permasalahan struktural yang kerap divalidasi oleh negara. Praktik ini juga merupakan bentuk invalidasi

perasaan dan pengalaman korban kekerasan seksual, sehingga penyelesaian kasusnya cenderung sulit

Pada Agustus 2024, Indonesia mengalami gelombang protes atau demonstrasi yang berujung pada 13 (tiga belas) insiden serangan digital yang dialami oleh masyarakat sipil, mayoritas korban adalah mahasiswa yang melakukan aksi demonstrasi. Aksi #PeringatanDarurat dan #KawalPutusanMK dipicu oleh dugaan Mahkamah Konstitusi mempermudah jalan Gibran Rakabuming Raka, putra Presiden Joko Widodo dalam proses pencalonan Wakil Presiden bersama dengan Prabowo Subianto. Selain itu, aksi ini juga berkaitan dengan Putusan Mahkamah Konstitusi yang melonggarkan ambang batas pencalonan kepala daerah untuk semua partai politik peserta Pemilu Tahun 2024.¹³⁹ Pada momentum tersebut, serangan digital yang terjadi antara lain adalah *doxing*, pengambilalihan akun, hingga tindakan aparat menyusupi grup-grup percakapan internal milik beberapa kelompok mahasiswa di WhatsApp. Tindakan pelanggaran hak digital tersebut tidak ditindaklanjuti oleh aparat kepolisian, justru mereka terlibat sebagai pelaku. Hal ini menunjukkan bahwa negara belum memproteksi masyarakat sipil sepenuhnya.

3. Kebebasan Berekspresi (*Liberty*)

a. Kriminalisasi Pendapat dan Ekspresi di Ruang Digital

Kriminalisasi terhadap Daniel Tangkilisan menjadi kasus yang menarik banyak perhatian publik pada rentang waktu 2023-2024 lalu. Mulanya, Daniel menuliskan keresahannya di laman Facebook pribadinya mengenai aktivitas tambak udang ilegal yang ada di tempat tinggalnya, yakni Karimunjawa, sebuah kawasan Taman Nasional yang seharusnya dilindungi. Ia divonis melanggar Pasal 28 UU ITE mengenai ujaran kebencian selama 7 (tujuh) bulan penjara. Pengadilan Tinggi Jepara, Provinsi Jawa Tengah juga mengenakan denda kepada Daniel senilai Rp5 juta (\$315) dalam putusannya pada tanggal 4 April.¹⁴⁰

Selain itu, terdapat kasus Haris-Fatia yang dikriminalisasi dengan pasal pencemaran nama baik, yakni Pasal 27 ayat (3) UU ITE dan KUHP yang dilaporkan oleh Mantan Menteri Koordinator Bidang Kemaritiman dan Investasi Luhut Binsar Pandjaitan. Pelapor merasa namanya dicemarkan dengan panggilan "Lord" dalam siaran *podcast* Haris dan Fatia yang membahas mengenai tambang di Papua dan perusahaan yang bertanggung jawab di baliknya. Pada kasus ini, Haris dan Fatia divonis tidak bersalah. Kendati demikian, hal ini menjadi bukti bahwa upaya pembungkaman ekspresi dan pendapat di ruang digital masih dilakukan menggunakan hukum sebagai alatnya

Pasca UU ITE direvisi di awal tahun 2024, justru tidak terdapat penurunan angka kriminalisasi. Pada Januari-Maret 2024, tercatat sebanyak 30 (tiga puluh) kasus

pelanggaran kebebasan berekspresi di ranah digital dengan terlapor sebanyak 52 (lima puluh dua) orang. Pada periode ini, pasal yang paling banyak digunakan untuk melakukan pelaporan adalah Pasal 28 ayat (2) UU ITE, yaitu sebanyak enam kasus. Kemudian, UU ITE tanpa disebutkan pasal spesifik sebanyak lima kasus dan Pasal 27A UU ITE sejumlah tiga kasus.¹⁴²

Selanjutnya, pada April-Juni 2024, pemantauan SAFEnet menemukan sejumlah 48 (empat puluh delapan) laporan ke kepolisian terkait dengan ekspresi di ranah digital. Jumlah korban pada periode ini adalah 45 (empat puluh lima) orang. Pelaporan tersebut didasarkan pada UU ITE tanpa disebutkan pasal yang spesifik sebanyak 16 (enam belas) kasus, Pasal 28 ayat (2) UU ITE tercatat sebanyak 6 (enam) kasus, dan Pasal 27 ayat (3) UU ITE sebanyak 4 (empat) kasus, disusul dengan pasal-pasal lainnya dalam UU ITE. Selain itu, Pasal 156a KUHP dan Pasal 310 KUHP tercatat masing-masing satu kasus dalam periode ini.¹⁴³

Menurut pantauan SAFEnet, aparat penegak hukum tidak sepenuhnya menerapkan perubahan UU ITE tahun 2024. Beberapa kasus yang tercatat masih menggunakan UU ITE yang lama (UU ITE 2016 jo. UU ITE 2008). Padahal, UU ITE 2024 sudah berlaku sejak 2 Januari 2024. Salah satu kasusnya adalah kasus Septia yang masih dalam proses persidangan. Jaksa Penuntut Umum dalam kasus ini mendakwa Septia dengan Pasal

27 ayat (3) UU ITE 2016 tentang pencemaran nama baik dan melapisinya dengan Pasal 36 UU ITE 2016 tentang pelanggaran yang menyebabkan kerugian bagi orang lain.¹⁴⁴

b. Kriminalisasi Jurnalis

Aliansi Jurnalis Independen (AJI) mencatat setidaknya 14 (empat belas) wartawan dan satu media massa dilaporkan menggunakan UU ITE dalam kurun waktu 2019-2021. Sejak disahkan pada 2008-2023, UU ITE telah menjerat sebanyak 43 (empat puluh tiga) jurnalis. Dari jumlah tersebut, lima orang di antaranya diputus bersalah oleh pengadilan. Di antaranya, kasus Jurnalis Muhammad Asrul dijatuhi vonis penjara tiga bulan oleh Pengadilan Negeri Palopo, Sulawesi Selatan pada 23 November 2021. Asrul divonis bersalah setelah membongkar dugaan kasus korupsi di Palopo lewat tiga tulisannya yang dimuat di Berita.news. Di tahun yang sama, jurnalis Mohamad Sadli Saleh divonis dua tahun penjara oleh Majelis Hakim Pengadilan Negeri Pasarwajo, Kabupaten Buton, Sulawesi Tenggara.

Padahal, UU Pers menjamin kemerdekaan pers dan terdapat mekanisme khusus untuk melakukan banding terhadap produk jurnalistik. Alih-alih mengkriminalisasi, produk jurnalistik yang dianggap tidak sesuai dengan data dan fakta dapat dipersoalkan melalui mekanisme hak jawab dan hak tolak yang dapat dimintakan melalui Dewan Pers.

Hak Digital untuk
Demokrasi dan
Civic Space

Studi Pemetaan Regulasi
Internet di Indonesia

Kesimpulan dan Rekomendasi

Kesimpulan dan Rekomendasi

A ● Kesimpulan

Studi ini berupaya memetakan regulasi internet dan ruang digital di Indonesia serta mengidentifikasi celah pada tiap pengaturan untuk mewujudkan regulasi tata kelola internet yang berbasis hak asasi manusia. Tolok ukur analisis regulasi tata kelola internet tersebut merujuk pada *The Charter of Human Rights and Principles for the Internet* (ICRP), terutama untuk menghasilkan pengaturan tata kelola internet yang memperhatikan aspek akses internet, aspek proteksi dan keamanan digital, serta aspek kebebasan. Berdasarkan studi yang dilakukan oleh SAFEnet dan PSHK, di bawah ini merupakan kesimpulan-kesimpulan yang telah dikristalkan dari kajian.

Pertama, melalui penelitian ini ditemukan bahwa saat ini terdapat 13 (tiga belas) undang-undang dan 153 (seratus lima puluh tiga) pasal yang mengatur tata kelola internet di Indonesia. Dari jumlah tersebut, ditemukan terdapat 51 (lima puluh satu) norma yang mengatur aspek akses internet atau setara dengan 33.3% (tiga puluh tiga koma tiga persen), 80 (delapan puluh) ketentuan yang mengatur aspek proteksi dan keamanan digital atau setara dengan 52.3% (lima puluh dua koma tiga persen), dan 22 (dua puluh dua) ketentuan yang mengatur aspek kebebasan (*liberty*) atau setara dengan 14.4% (empat belas koma empat persen). Dari data tersebut, terlihat bahwa orientasi pengaturan tata kelola internet yang tersebar pada 13 (tiga belas) undang-undang tersebut memiliki kecenderungan proteksionis (*protection heavy*). Artinya, negara memiliki kecenderungan untuk mengontrol warga negara dalam beraktivitas di ruang digital. Paradigma ini diperkuat dengan minimnya jaminan kebebasan dalam undang-undang-undang yang menjadi objek riset, dalam hal ini, jaminan kebebasan hanya ditemukan dalam sembilan undang-undang saja.

Pengaturan dalam setiap undang-undang tersebut pun ditemukan dalam jumlah yang minim, misalnya paling banyak terdapat enam jaminan perlindungan dalam KUHP, lima jaminan dalam UU ITE, tiga jaminan dalam UU Pornografi dan UU Keterbukaan

Informasi Publik, dan satu jaminan dalam UU Pemilu, UU Pers, UU Pilkada, UU Perlindungan Konsumen, dan UU Pembentukan Peraturan Perundang-Undangan. Bandingkan dengan pengaturan terkait proteksi dalam UU ITE saja yang berjumlah 25 (dua puluh lima) ketentuan, atau dalam UU Perlindungan Konsumen terdapat 20 (dua puluh) ketentuan.

Terdapat dua jenis undang-undang yang mengandung aspek proteksi dan keamanan digital, yaitu undang-undang yang mengatur perikatan antarindividu dan pengaturan yang bersifat publik. Konteks yang mengatur perikatan antarindividu ditemukan dalam UU Perlindungan Konsumen dan yang bersifat publik dapat ditemukan di KUHP dan UU Pornografi. Undang-undang yang mengatur perikatan antarindividu, ketentuannya lebih bersifat melindungi salah satu pihak karena hubungan perikatan di antara mereka berpotensi tidak setara, seperti hubungan antara korporasi *marketplace* dengan pembeli individu. Sebaliknya, undang-undang dengan aspek proteksi dalam bidang yang bersifat publik, bersifat kontrol dan memberikan sanksi pidana untuk mereka yang melanggar. Pendekatan proteksi ternyata memiliki wajah lain ketimbang memberikan perlindungan. Pendekatan proteksi berujung kontrol dan pengawasan ketat, sehingga membahayakan kebebasan. Di sisi lain, implementasi peraturan tidak konsisten dan cenderung bias. Ketentuan undang-undang yang memuat proteksi dalam relasi bisnis maupun perikatan antarindividu cenderung minim diimplementasikan. Sebaliknya, undang-undang yang memuat proteksi terhadap individu di ranah publik, diimplementasikan dengan pendekatan pembedaan, sehingga memakan banyak korban, misalnya pencemaran nama baik di ruang digital, singgungan SARA, dan lain sebagainya.

Sementara pada aspek akses, pengaturan

lebih banyak kaitannya dengan keterbukaan informasi. Regulasi yang ada tidak berkaitan dengan jaminan akses dalam konteks jangkauan dan perangkat untuk menunjang pemerataan terhadap akses internet, melainkan konteks akster terhadap informasi, baik untuk menjangkau informasi publik, mengolah informasi, hingga menyebarkan informasi melalui *platform* digital. Hal demikian juga erat berkaitan dengan aspek kebebasan yang pada dasarnya menjamin kebebasan dalam ruang digital. Namun demikian, perkembangan akses terhadap informasi publik saat ini membenturkan konteks keterbukaan informasi yang seharusnya dapat diakses masyarakat luas pada rezim UU Keterbukaan Informasi Publik dengan perlindungan data pribadi yang bersifat privat. Seperti pada kasus informasi kepemiluan, informasi penyumbang dana kampanye dianggap sebagai informasi yang privat oleh KIP, sehingga tidak dapat serta-merta diakses oleh masyarakat, kendati informasi tersebut krusial untuk pengawasan dan penelusuran sumber dana kampanye yang legal.

Apabila tiga aspek ini di teropong secara keseluruhan, maka terdapat kecenderungan bahwa negara lebih mengedepankan proteksi, sedangkan kebebasan merupakan jaminan yang paling sedikit diakomodasikan. Selain itu, proteksi paling banyak ditemukan dalam UU ITE, akses pada keterbukaan informasi paling banyak diatur dalam UU Keterbukaan Informasi Publik, dan kebebasan paling banyak diatur dalam KUHP. Peta ini menarik karena kebebasan paling banyak diatur dalam hukum pidana, yang artinya dapat menjadi pisau bermata dua, yaitu tidak hanya melindungi kebebasan, tetapi juga dapat merampasnya atau dengan kata lain, kembali menjadi alat kontrol.

Kedua, implementasi peraturan perundang-undangan yang sudah dibahas sebelumnya tidak cukup melindungi

masyarakat sipil dalam beraktivitas di ruang digital. Misalnya, UU Pornografi yang masih digunakan untuk mengkriminalisasi korban kekerasan seksual, misalnya pada kasus penyebaran konten intim nonkonsensual. Contoh lainnya adalah KUHP yang seringkali digunakan untuk mengkriminalisasi masyarakat sipil yang menyampaikan pendapat atau kritik kepada pemerintah. Perlawanan terhadap *status quo* atau pemangku kekuasaan yang disampaikan di ruang digital menghadapi risiko kriminalisasi menggunakan pasal-pasal karet terkait distribusi informasi mengandung SARA, pencemaran nama baik, ujaran kebencian dan permusuhan, dan muatan kesusilaan.

Dalam temuan ini, upaya *controlling* dari negara tidak hanya terlihat dari banyaknya aspek proteksi yang diatur, kecenderungan ini terlihat hingga pada tahap implementasi. Pada aspek akses internet, masih seringkali terdapat pembatasan dengan tidak proporsional, transparan, dan sesuai dengan kebutuhan. Di sisi lain, pasal-pasal yang mengatur mengenai proteksi justru masih banyak yang dijadikan sebagai justifikasi untuk melindungi pandangan mayoritas saja atau hanya menguntungkan kepentingan individu yang timpang kuasanya dengan mengkriminalisasi masyarakat, terutama kelompok rentan. Pada aspek kebebasan, selain jaminan perlindungan yang minim, dalam implementasinya, pasal-pasal yang mengatur mengenai jaminan kebebasan berpendapat dan berekspresi jarang digunakan.

Ketiga, kendati pengaturan tata kelola internet cenderung bersifat proteksionis, tidak terdapat penekanan pada akuntabilitas negara untuk bertanggung jawab dan memberikan pemulihan atas kesalahan atau kelalaian instansi negara yang berujung pada kerugian bagi masyarakat. Misalnya, pada kasus kebocoran data pribadi, negara sebagai subjek yang seharusnya menjamin hak-hak masyarakat sipil sebagai warga

negara tidak memenuhi tanggung jawabnya, dibuktikan dengan tidak adanya langkah mitigasi yang tepat guna dan tidak ada pertanggungjawaban atas kelalaian tersebut.

Kasus-kasus yang diteliti juga menunjukkan tidak berjalannya akuntabilitas, baik dalam kasus-kasus individual maupun pelanggaran HAM oleh negara. Individu maupun pembela HAM yang mengalami ancaman digital tidak mendapatkan hak pemulihan, baik berupa pengungkapan dan proses hukum terhadap pelaku, maupun pengembalian pada keadaan semula. Hal serupa terjadi pada kasus pelanggaran HAM yang dilakukan pemerintah, yaitu *throttling* ataupun *internet shutdown*.

Keempat, pengaturan tata kelola internet bukan merupakan isu sektoral, sehingga terdapat pertautan antara aspek pengaturan pada norma di satu undang-undang dengan undang-undang lainnya. Misalnya, pertautan antara UU Pemilu dengan UU Pelindungan Data Pribadi. Pada kasus kebocoran data pemilih, misalnya, pendekatan pertanggungjawaban KPU tak dapat mengandalkan UU Pemilu semata, tetapi juga harus merujuk pada UU Pelindungan Data Pribadi untuk memberikan perlindungan dan pemulihan hak pada pemilih, serta menuntut akuntabilitas atas kelalaian KPU sebagai pengendali data.

Kelima, undang-undang yang berusia lebih dari lima tahun harus diperbarui agar lebih relevan dan sesuai dengan konteks perkembangan pemanfaatan ruang digital dan perlindungan pengguna ruang digital dewasa ini. Misalnya, UU Pers agar dapat melindungi kebebasan jurnalis yang membagikan informasi melalui *platform* media sosial, serta UU Pemilu dan UU Pilkada, misalnya agar terdapat aturan kampanye yang lebih relevan dengan pemanfaatan sosial media saat ini.

Keenam, pengaturan tentang tata kelola internet yang ada saat ini belum cukup efektif

memberikan perlindungan kepada kelompok rentan, yaitu kelompok perempuan, kelompok minoritas kepercayaan, kelompok keberagaman gender, jurnalis, dan masyarakat sipil yang kritis terhadap kekuasaan. Alih-alih memberikan perlindungan, ketentuan yang ada malah mengekang kebebasan dan mengancam keselamatan kelompok rentan tersebut, seperti kriminalisasi menggunakan UU ITE dan UU Pornografi.

Ketujuh, jangkauan ketentuan hukum yang ada saat ini belum cukup untuk mendorong akuntabilitas *platform* media sosial. Belum terdapat pengaturan di level undang-undang yang menjadi dasar pertanggungjawaban dan transparansi bagi *platform* media sosial dalam mengeset algoritma dan memoderasi konten untuk dicermati pengguna media sosial.

Dari kesimpulan di atas, dapat dilihat bahwa terdapat kecenderungan pengaturan dan arah penegakkan hukum dalam tata kelola internet justru adalah mengekang dan mengontrol kebebasan masyarakat di ruang digital. Hukum tentang tata kelola internet yang ada saat ini belum menggunakan pendekatan untuk mengakomodasikan hak asasi manusia, terutama hak digital masyarakat. Hal ini menggambarkan jelas bahwa terdapat potensi ancaman terhadap demokrasi dan penyempitan ruang gerak masyarakat sipil di ruang digital, termasuk pemenuhan hak-hak digital. Celaknya, kebebasan di ruang digital terkait dan tidak dapat dipisahkan dari kebebasan di ruang fisik. Artinya, hilangnya kebebasan di ruang digital dapat berarti kehilangan berganda.

B. Rekomendasi Penyempurnaan Kebijakan

Untuk menciptakan regulasi internet yang memenuhi hak digital di Indonesia, kami merekomendasikan hal berikut:

1. Pemerintah dan DPR melakukan revisi komprehensif terhadap pengaturan terkait tata kelola internet yang lebih menjamin aspek akses, aspek proteksi dan keamanan digital, serta aspek kebebasan dengan seimbang. Komitmen ini dimulai dengan membentuk tim lintas sektor yang melibatkan masyarakat sipil untuk melakukan pemetaan regulasi dan membentuk naskah akademik tata kelola internet yang berbasis hak asasi manusia dan memperluas ruang gerak masyarakat sipil;
2. Sebagai upaya pendahuluan dalam melakukan revisi komprehensif tersebut di atas, kami mendorong para pihak untuk melakukan langkah-langkah sebagai berikut:
 - Mahkamah Agung untuk membentuk Peraturan/Surat Edaran Mahkamah Agung untuk menangani kasus terkait dengan tata kelola internet dan kaitannya dengan aspek akses, aspek proteksi dan keamanan digital, serta aspek kebebasan;
 - Peningkatan kompetensi dari pelaksana teknis dan membentuk mekanisme pengawasan untuk mengurangi *human error* dan memastikan implementasi prosedur yang mempengaruhi hak digital masyarakat;
 - Meningkatkan transparansi dan akuntabilitas pemerintah dan sektor bisnis digital tentang keputusan dan pelambatan akses, kebocoran data, dan penyensoran konten;

- Aparat penegak hukum menjalankan akuntabilitas penegakan hukum di ruang digital kepada masyarakat melalui keterbukaan laporan penanganan kasus;
- Presiden melakukan pengawasan ketat kepada Kepolisian dan Kejaksaan agar memiliki perspektif hak asasi manusia dan perlindungan korban dalam penegakkan hukum di ruang digital; dan
- DPR menjalankan fungsi pengawasan terhadap penegakan hukum di ruang digital termasuk meminta laporan secara berkala terhadap Presiden, Jaksa Agung dan Kapolri setidaknya mengenai penegakan hukum dan penggunaan anggaran di ruang digital.



Rekomendasi Riset Lanjutan

Penelitian yang kami lakukan tak terhindarkan dari kekurangan. Oleh karena itu, penelitian ini masih membuka sejumlah celah untuk dilakukan peninjauan lebih lanjut. Sejumlah hal yang dapat menjadi objek penelitian lanjutan, yaitu:

1. Meneliti lebih lanjut tentang singgungan antara hak digital dengan hak-hak asasi manusia di ruang fisik, terutama hak ekonomi, sosial, dan budaya (ekosob). Dalam hal ini, penelitian lebih lanjut dapat menyibak bagaimana hak sipil dan politik di ruang digital memengaruhi pengejawantahan hak sipil dan politik di ruang fisik, bagaimana hak sipil dan politik di ruang digital memengaruhi hak ekosob di ruang fisik, bagaimana hak ekosob di ruang digital memengaruhi hak sipil dan politik di ruang fisik, dan bagaimana hak ekosob di ruang fisik memengaruhi hak ekosob di ruang digital;
2. Meneliti lebih lanjut tentang identifikasi peran aktor terkait dalam tata kelola internet, sehingga dapat membentuk pengaturan tata kelola internet yang berbasis hak asasi manusia dan memperluas ruang gerak masyarakat sipil.

Daftar Pustaka

Buku dan Laporan Penelitian

Auditya Firza Saputra, Agil Oktaryal, dan Antoni Putra. 2021. *Makalah Advokasi – 2 Tahun #ReformasiDikorupsi dan Keruhnya Ekosisten Hukum Indonesia*. Jakarta: Pusat Studi Hukum dan Kebijakan Indonesia.

Center for Law and Democracy. 2011. “Commentary on Internet Rights and Principles Charter”, diakses melalui <<https://www.law-democracy.org/live/commentary-on-internet-rights-and-principles-charter/>> pada [20/08/2024].

Internet Rights & Principles Dynamic Coalition. 2011. *The Charter of Human Rights and Principles for the Internet*.

Kementerian Pendidikan dan Kebudayaan Republik Indonesia. 2024. *Laporan Akhir Penulisan Kerangka Ilmiah tentang Implementasi Undang-Undang Nomor 44 Tahun 2006 tentang Pornografi (dalam Bidang Pendidikan dan Kesehatan)*.

Komnas Perempuan. 2024. “CATAHU 2023: Catatan Tahunan Kekerasan Terhadap Perempuan Tahun 2023”, <https://komnasperempuan.go.id/download-file/1115>.

Komnas Perempuan. 2024. “CATAHU 2023: Catatan Tahunan Kekerasan Terhadap Perempuan Tahun 2023”, <https://komnasperempuan.go.id/download-file/1115>.

Laura J. Gurak. 1997. *Persuasion and Privacy in Cyberspace: The Online Protests Over Lotus Market Place and the Clipper Chip*, Yale University Press, New Haven.

Muhamad Heychael, Nenden Sekar Arum, dan Hafizh Nabiyin. 2024. *Kebebasan atau Kebencian? Mengkaji Akuntabilitas Platform Media Sosial dalam Penyebaran Ujaran Kebencian terhadap Kelompok Rentan di Pemilu 2024*. Bali: SAFEnet.

SAFEnet. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: Januari-Maret 2024*. SAFEnet.

_____. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: Juli-September 2024*. SAFEnet.

_____. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: April-Juni 2024*. SAFEnet.

_____. 2024. *Laporan Situasi Hak-hak Digital Indonesia 2023: Sudah Roboh Tertimpa Pemilu Pula*. SAFEnet.

Artikel

Admire Mare. 2023. *Digital Spaces, Rights and Responsibilities – Towards a duty of care model in Southern Africa*, Friedrich Ebert Stiftung, <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>, diakses pada 26 September 2024.

Amalia Salabi. 2023. *Kode Etik Kampanye di Media Sosial untuk Pemilu 2024*. Diakses melalui <<https://rumahpemilu.org/kode-etik-kampanye-di-media-sosial-untuk-pemilu-2024/>>, pada [15/10/2024].

John Palfrey. 2010. “Four Phases of Internet Regulation”. *Public Law & Legal Theory Working Paper Series Paper No. 10-42*.

Laura De Nardis. 2010. “The Emerging Field of Internet Governance”. *Yale Information Society Project Working Paper Series*.

Michael W. Müller. 2018. “Mapping Paradigms of European Internet Regulation: The Example of Internet Content Control”. *Frontiers of Law in China Vol. 13 No. 3*.

Mitu, B & Vega, D. O. C. 2014. “Digital Activism: A Contemporary Overview”. *Revista de Stiinte Politice*, 44.

Admire Mare. 2023. *Digital Spaces, Rights and Responsibilities – Towards a duty of care model in Southern Africa*, Friedrich Ebert Stiftung, <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>, diakses pada 26 September 2024.

Amalia Salabi. 2023. *Kode Etik Kampanye di Media Sosial untuk Pemilu 2024*. Diakses melalui <<https://rumahpemilu.org/kode-etik-kampanye-di-media-sosial-untuk-pemilu-2024/>>, pada [15/10/2024].

John Palfrey. 2010. “Four Phases of Internet Regulation”. *Public Law & Legal Theory Working Paper Series Paper No. 10-42*.

Laura De Nardis. 2010. “The Emerging Field of Internet Governance”. *Yale Information Society Project Working Paper Series*.

Michael W. Müller. 2018. “Mapping Paradigms of European Internet Regulation: The Example of Internet Content Control”. *Frontiers of Law in China Vol. 13 No. 3*.

Mitu, B & Vega, D. O. C. 2014. “Digital Activism: A Contemporary Overview”. *Revista de Stiinte Politice*, 44.

Paul M. Schwartz. 1999. “Privacy and Democracy in Cyberspace”, *Vanderbilt Law Review*, Vol. 52 No. 6.

Paul M. Schwartz. 1999. “Privacy and Democracy in Cyberspace”, *Vanderbilt Law Review*, Vol. 52 No. 6.

Stuart Biegler. 2018. Beyond Our Control? Dalam Michael W. Müller, *Mapping Paradigms of European Internet Regulation: The Example of Internet Content Control*, *Frontiers of Law in China Vol. 13 No. 3*.

Triyo Handoko. 2022. Otoritarianisme Digital dan Bahayanya bagi Demokrasi. Diakses melalui <<https://www.remotivi.or.id/headline/konsep-dan-isu/756>> pada [22/08/2024].

William H. Dutton dan Malcolm Peltu. 2005. “The emerging Internet governance mosaic: connecting the pieces”. *Forum Discussion Paper No. 5*. Oxford Internet Institute University, Oxford.

Sumber Internet

BBC News Indonesia. 2020. *PTUN Jakarta putusan pemblokiran internet di Papua dan Papua Barat ‘melanggar hukum’*. Diakses melalui <<https://www.bbc.com/indonesia/majalah-52901391>>, pada [15/10/2024].

_____. 2024. *Advokat LBH Yogyakarta yang tangani kasus dugaan kekerasan seksual di Ull ditetapkan sebagai tersangka ‘pencemaran nama baik’*. Diakses melalui <https://www.bbc.com/indonesia/articles/c80xwnl79e7o> pada [10/10/2024].

CNN Indonesia. 2020. “Facebook Akan Tuntut Pemerintah Thailand”. Diakses melalui <https://www.cnnindonesia.com/teknologi/20200825192002-185-539254/facebook-akan-tuntut-pemerintah-thailand> pada [25/11/2020].

Diskusi SAFEnet dengan Kominfo, “Mengupas Kebijakan dan Teknis Pengendalian Konten dan Pembatasan Akses Internet”, https://youtu.be/p_YErZOCKiA?si=zWTaHqjvuiiRHeup, 14 Oktober 2024.

Indonesia Corruption Watch. 2024. *Siaran Pers – KPU Enggan Buka Informasi Penyumbang Dana Kampanye, Berpotensi Lindungi Cukong Politik*. Diakses melalui <<https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>>, pada [16/10/2024].

International Covenant on Civil and Political Rights, United Nations Human Rights Office of The High Commissioner, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> diakses pada 3 Oktober 2024.

Komisi Informasi Pusat. 2024. *MK KI Pusat Putuskan Sengketa Informasi Antara ICW dan KPU*. Diakses melalui <<https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>>, pada [16/10/2024].

LBH Pers. 2024. “Permohonan Eksepsi Ditolak, Majelis Hakim Melanjutkan Kriminalisasi Septia”. *Siaran Pers*, <https://lbhpers.org/2024/10/04/siaran-pers-permohonan-eksepsi-ditolak-majelis-hakim-melanjutkan-kriminalisasi-septia/> pada [15/10/2024].

Lembaga Studi & Advokasi Masyarakat (ELSAM). 2023. *Data Pemilih Diduga Bocor, Integritas Pemilu 2024 Terancam*. Diakses melalui <<https://www.elsam.or.id/siaran-pers/data-pemilih-diduga-bocor-integritas-pemilu-2024-terancam>>, pada [15/10/2024].

Liputan 6. 2019. *Vonis Penjara untuk Ariel 8 Tahun Silam yang Membuat Luna Maya Pingsan*. Diakses melalui <https://www.liputan6.com/news/read/3881634/vonis-penjara-untuk-ariel-8-tahun-silam-yang-membuat-luna-maya-pingsan?page=2> pada [15/10/2024].

Mongabay. 2024. *Daniel Tangkilisan Karimunjawa Marin National Park Indonesia Enviromental Activist Jailed*. Diakses melalui <https://news.mongabay.com/2024/04/daniel-tangkilisan-karimunjawa-marin-national-park-indonesia-enviromental-activist-jailed/> pada [10/10/2024].

Oxford Reference. (tanpa tahun). *Lex praevia*. Diakses melalui <<https://www.oxfordreference.com/display/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-1284>>, pada [10/07/2024].

Reska K. Nistanto. 2023. "Kominfo Sudah Pulihkan Google Docs, Bukan Diblokir Tapi Kesalahan Teknis," KOMPAS.com, September 22, 2023, <https://tekno.kompas.com/read/2023/09/22/09202577/kominfo-sudah-pulihkan-google-docs-bukan-diblokir-tapi-kesalahan-teknis>, diakses pada [18/10/2014].

SAFEnet. 2024. SAFEnet: *Jangan Korban Data Warga, Perkuat Keamanan PDN*. Diakses melalui <<https://safenet.or.id/id/2024/06/safenet-jangan-korbankan-data-warga-perkuat-keamanan-pdn/>> pada [22/08/2024].

Tempo. 2024. *4,7 Juta Data NIP dan NIK ASN Diduga Bocor, Pemerintah Sarankan Ganti Kata*. Diakses melalui <<https://www.tempo.co/digital/4-7-juta-data-nip-dan-nik-asn-diduga-bocor-pemerintah-sarankan-ganti-kata-sandi-25998>>, pada [20/10/2024].

Universal Declaration of Human Rights, United Nations, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>, diakses pada 3 Oktober 2024.

Catatan Akhir

- ¹ Paul M. Schwartz, "Privacy and Democracy in Cyberspace", *Vanderbilt Law Review*, Vol. 52 No. 6, 1999, hal. 1648-1649.
- ² Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests Over Lotus Market Place and the Clipper Chip*, Yale University Press, New Haven, 1997, hal. 56
- ³ Admire Mare, *Digital Spaces, Rights and Responsibilities - Towards a duty of care model in Southern Africa*, Friedrich Ebert Stiftung, <https://library.fes.de/pdf-files/bueros/africa-media/20188.pdf>, diakses pada 26 September 2024, 2023.
- ⁴ Mitu, B & Vega, D. O. C. (2014) *Digital Activism: A Contemporary Overview*. *Revista de Stiinte Politice*, 44, hal.103-112.
- ⁵ CNN Indonesia. 2020. "Facebook Akan Tuntut Pemerintah Thailand". Diakses melalui <https://www.cnnindonesia.com/teknologi/20200825192002-185-539254/facebook-akan-tuntut-pemerintah-thailand> pada [25/11/2020].
- ⁶ Auditya Firza Saputra, Agil Oktaryal, dan Antoni Putra. 2021. *Makalah Advokasi - 2 Tahun #ReformasiDikorupsi dan Keruhnya Ekosistem Hukum Indonesia*. Jakarta: Pusat Studi Hukum dan Kebijakan Indonesia.
- ⁷ Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik: (Kementerian Komunikasi dan Informatika, 2024), hal. 2.
- ⁸ *Id.*, hal. 4.
- ⁹ *Id.*, hal. 6.
- ¹⁰ Kementerian Pendidikan dan Kebudayaan Republik Indonesia. 2024. *Laporan Akhir Penulisan Kerangka Ilmiah tentang Implementasi Undang-Undang Nomor 44 Tahun 2006 tentang Pornografi (dalam Bidang Pendidikan dan Kesehatan)*, hal. 2.
- ¹¹ Pada pemerintahan Prabowo Subianto dan Gibran Rakabuming Raka, Kementerian Komunikasi dan Informasi diubah menjadi Kementerian Komunikasi dan Digital.
- ¹² SAFEnet. 2024. *SAFEnet: Jangan Korban Data Warga, Perkuat Keamanan PDN*. Diakses melalui <<https://safenet.or.id/id/2024/06/safenet-jangan-korbankan-data-warga-perkuat-keamanan-pdn/>> pada [22/08/2024].
- ¹³ Triyo Handoko. 2022. *Otoritarianisme Digital dan Bahayanya bagi Demokrasi*. Diakses melalui <<https://www.remotivi.or.id/headline/konsep-dan-isu/756>> pada [22/08/2024].
- ¹⁴ Michael W. Müller. 2018. "Mapping Paradigms of European Internet Regulation: The Example of Internet Content Control". *Frontiers of Law in China Vol. 13 No. 3*, hal. 332.
- ¹⁵ *Id.*
- ¹⁶ *Id.*
- ¹⁷ Stuart Biegler. 2018. *Beyond Our Control?* Dalam Michael W. Müller, *Mapping Paradigms of European Internet Regulation: The Example of Internet Content Control*, *Frontiers of Law in China Vol. 13 No. 3*, 2018, hal. 332.
- ¹⁸ Michael W. Müller, *supra note 14*, hal. 335.
- ¹⁹ *Id.*
- ²⁰ *Id.*, hal. 335-336.
- ²¹ *Id.*, hal. 336.
- ²² Laura De Nardis. 2010. "The Emerging Field of Internet Governance". *Yale Information Society Project Working Paper Series*, hal. 2.
- ²³ *Id.*, hal. 2-3.
- ²⁴ *Id.*
- ²⁵ William H. Dutton dan Malcolm Peltu. 2005. "The emerging Internet governance mosaic: connecting the pieces". *Forum Discussion Paper No. 5*, *Oxford Internet Institute University, Oxford*, hal. 6.
- ²⁶ *Ibid.*, hal. 16.
- ²⁷ *Id.*, hal. 19.
- ²⁸ *Id.*, hal. 20.
- ²⁹ John Palfrey. 2010. "Four Phases of Internet Regulation". *Public Law & Legal Theory Working Paper Series Paper No. 10-42*, hal. 2.
- ³⁰ *Id.*
- ³¹ *Id.*, hal. 2-3.
- ³² *Id.*, hal. 3
- ³³ *Id.*, hal. 7.
- ³⁴ *Id.*, hal. 8 - 9.
- ³⁵ *Id.*, hal. 9.
- ³⁶ *Id.*, hal. 10.
- ³⁷ *Id.*
- ³⁸ *Id.*, hal. 12.
- ³⁹ *Id.*, hal. 14.
- ⁴⁰ *Id.*, hal. 15.
- ⁴¹ *Id.*, hal. 16
- ⁴² *Id.*, hal. 19
- ⁴³ *Id.*, hal. 17
- ⁴⁴ *Id.*, hal. 19.
- ⁴⁵ Internet Rights & Principles Dynamic Coalition. 2011. *The Charter of Human Rights and Principles for the Internet*, hal. 1.
- ⁴⁶ *Id.*, hal. 5.
- ⁴⁷ Center for Law and Democracy. 2011. "Commentary on Internet Rights and Principles Charter", diakses melalui <<https://www.law-democracy.org/live/commentary-on-internet-rights-and-principles-charter/>> pada [20/08/2024], hal. 2.
- ⁴⁸ *Id.*, hal. 6.
- ⁴⁹ Internet Rights & Principles Dynamic Coalition, *supra note 45*, hal. 13.

- ⁵⁰ *Id.*
- ⁵¹ *Id.*, hal. 15.
- ⁵² Pasal 3 UU ITE.
- ⁵³ Penjelasan Pasal 3 UU ITE.
- ⁵⁴ Pasal 4 UU ITE.
- ⁵⁵ Pasal 33 UU ITE.
- ⁵⁶ Pasal 37 UU ITE.
- ⁵⁷ Pasal 20 ayat (2a), (2b), (2c), dan (2d) UU ITE.
- ⁵⁸ BBC News Indonesia. 2020. *PTUN Jakarta putusan pemblokiran internet di Papua dan Papua Barat 'melanggar hukum'*. Diakses melalui <<https://www.bbc.com/indonesia/majalah-52901391>>, pada [15/10/2024].
- ⁵⁹ *Id.*
- ⁶⁰ Pasal 22 angka 2 UU Pengembangan dan Penguatan Sektor Keuangan (Perubahan Pasal 5 huruf a angka 7 UU Pasar Modal).
- ⁶¹ Pasal 22 angka 22 UU Pengembangan dan Penguatan Sektor Keuangan (Perubahan Pasal 69A ayat (1) UU Pasar Modal).
- ⁶² Pasal 7 dan Pasal 32 ayat (1) dan ayat (2) UU Perlindungan Data Pribadi.
- ⁶³ Pasal 16 ayat (2) huruf e UU Pelindungan Data Pribadi, 332.
- ⁶⁴ Pasal 33 UU Pelindungan Data Pribadi.
- ⁶⁵ Pasal 39 ayat (1) dan (2) UU Pelindungan Data Pribadi.
- ⁶⁶ Pasal 88 ayat (1) dan Pasal 92 ayat (1) UU Pembentukan Peraturan Perundang-Undangan.
- ⁶⁷ Pasal 97B UU Pembentukan Peraturan Perundang-Undangan.
- ⁶⁸ Pasal 46 UU TPKS.
- ⁶⁹ Pasal 47 UU TPKS.
- ⁷⁰ Pasal 287 ayat (1), (2), (3), dan (4) UU Pemilu.
- ⁷¹ Pasal 218 ayat (1) UU Pemilu.
- ⁷² Pasal 536 UU Pemilu.
- ⁷³ Amalia Salabi. 2023. *Kode Etik Kampanye di Media Sosial untuk Pemilu 2024*. Diakses melalui <<https://rumahpemilu.org/kode-etik-kampanye-di-media-sosial-untuk-pemilu-2024/>>, pada [15/10/2024].
- ⁷⁴ *Id.*
- ⁷⁵ *Id.*
- ⁷⁶ Muhamad Heychael, Nenden Sekar Arum, dan Hafizh Nabiyin. 2024. *Kebebasan atau Kebencian? Mengkaji Akuntabilitas Platform Media Sosial dalam Penyebaran Ujaran Kebencian terhadap Kelompok Rentan di Pemilu 2024*. Bali: SAFEnet, hal. 4.
- ⁷⁷ Pasal 64 dan Pasal 65 UU Pilkada.
- ⁷⁸ Pasal 195 UU Pilkada.
- ⁷⁹ Pasal 18 dan Pasal 19 UU Pornografi.
- ⁸⁰ Pasal 4 ayat (1) dan ayat (2) UU Keterbukaan Informasi Publik.
- ⁸¹ Pasal 7 ayat (1), (2), (3), (4), (5), dan (6) UU Keterbukaan Informasi Publik.
- ⁸² Pasal 2 ayat (1) dan ayat (3) UU Keterbukaan Informasi Publik.
- ⁸³ Pasal 6 ayat (2) UU Keterbukaan Informasi Publik.
- ⁸⁴ Pasal 6 ayat (3) UU Keterbukaan Informasi Publik.
- ⁸⁵ Pasal 52 UU Keterbukaan Informasi Publik.
- ⁸⁶ Pasal 54 ayat (1) dan ayat (2) UU Keterbukaan Informasi Publik.
- ⁸⁷ Indonesia Corruption Watch. 2024. *Siaran Pers - KPU Enggan Buka Informasi Penyumbang Dana Kampanye, Berpotensi Lindungi Cukong Politik*. Diakses melalui <<https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>>, pada [16/10/2024].
- ⁸⁸ Komisi Informasi Pusat. 2024. *MK KI Pusat Putusan Sengketa Informasi Antara ICW dan KPU*. Diakses melalui <<https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>>, pada [16/10/2024].
- ⁸⁹ Pasal 4 UU Pers.
- ⁹⁰ Pasal 3 UU Perlindungan Konsumen.
- ⁹¹ Pasal 4 dan Pasal 7 UU Perlindungan Konsumen.
- ⁹² Pasal 4 UU TPKS mengatur tindak pidana kekerasan seksual termasuk kekerasan seksual berbasis elektronik.
- ⁹³ Pasal 14 ayat (5) UU TPKS.
- ⁹⁴ Pasal 15 ayat (1) huruf i UU TPKS.
- ⁹⁵ Pasal 47 UU TPKS.
- ⁹⁶ Pasal 5 ayat (g) KUHP.
- ⁹⁷ Naskah Akademik RUU KUHP, hal. 10-11.
- ⁹⁸ Oxford Reference. (tanpa tahun). *Lex praevia*. Diakses melalui <<https://www.oxfordreference.com/display/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-1284>>, pada [10/07/2024].
- ⁹⁹ Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights angka 29.
- ¹⁰⁰ Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights angka 30.
- ¹⁰¹ Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights angka 31.
- ¹⁰² Pasal 280 (1) huruf a UU Pemilu.
- ¹⁰³ Bagian Menimbang UU Pelindungan Data Pribadi.

- ¹⁰⁴ Pasal 65 ayat (1) UU Pelindungan Data Pribadi.
- ¹⁰⁵ Pasal 65 ayat (2) UU Pelindungan Data Pribadi.
- ¹⁰⁶ Pasal 65 ayat (3) UU Pelindungan Data Pribadi.
- ¹⁰⁷ Universal Declaration of Human Rights, United Nations, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>, diakses pada 3 Oktober 2024.
- ¹⁰⁸ International Covenant on Civil and Political Rights, United Nations Human Rights Office of The High Commissioner, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> diakses pada 3 Oktober 2024.
- ¹⁰⁹ Lihat Pasal 19 UDHR, dan The Charter of Human Rights and Principles for The Internet, Internet Rights and Principles Coalition, hal.16
- ¹¹⁰ Lihat Undang-Undang Nomor 9 Tahun 1998 tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum dan Undang-Undang Nomor 40 Tahun 1999 tentang Pers.
- ¹¹¹ Pasal 17 huruf a UU Keterbukaan Informasi Publik.
- ¹¹² Pasal 17 huruf b UU Keterbukaan Informasi Publik.
- ¹¹³ Pasal 17 huruf c UU Keterbukaan Informasi Publik.
- ¹¹⁴ Lihat ICRP hal. 16
- ¹¹⁵ *Id.*
- ¹¹⁶ Lihat Pasal 158 KUHP.
- ¹¹⁷ Lihat Pasal 258 KUHP.
- ¹¹⁸ Lihat Pasal 332 KUHP.
- ¹¹⁹ Lihat Pasal 335 KUHP.
- ¹²⁰ Lihat ICRP, hlm. 16
- ¹²¹ Reska K. Nistanto. 2023. "Kominfo Sudah Pulihkan Google Docs, Bukan Diblokir Tapi Kesalahan Teknis," KOMPAS.com, September 22, 2023, <https://tekno.kompas.com/read/2023/09/22/09202577/kominfo-sudah-pulihkan-google-docs-bukan-diblokir-tapi-kesalahan-teknis>, diakses pada [18/10/2014].
- ¹²² SAFEnet. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: Januari-Maret 2024*. SAFEnet, hal. 15-17.
- ¹²³ Diskusi SAFEnet dengan Kominfo, "Mengupas Kebijakan dan Teknis Pengendalian Konten dan Pembatasan Akses Internet", https://youtu.be/p_YErZOCKiA?si=zWtAHqjvuiuRHeup, 14 Oktober 2024.
- ¹²⁴ BBC News Indonesia. 2020. *PTUN Jakarta putusan pemblokiran internet di Papua dan Papua Barat 'melanggar hukum'*. Diakses melalui <https://www.bbc.com/indonesia/majalah-5290139>, pada [15/10/2024].
- ¹²⁵ *Id.*
- ¹²⁶ Amalia Salabi. 2023. *Kode Etik Kampanye di Media Sosial untuk Pemilu 2024*. Diakses melalui <https://rumahpemilu.org/kode-etik-kampanye-di-media-sosial-untuk-pemilu-2024/>, pada [15/10/2024].
- ¹²⁷ *Id.*
- ¹²⁸ *Id.*
- ¹²⁹ Muhamad Heychael, Nenden Sekar Arum, dan Hafizh Nabiyin. 2024. *Kebebasan atau Kebencian? Mengkaji Akuntabilitas Platform Media Sosial dalam Penyebaran Ujaran Kebencian terhadap Kelompok Rentan di Pemilu 2024*. Bali: SAFEnet, hal. 4.
- ¹³⁰ Indonesia Corruption Watch. 2024. *Siaran Pers - KPU Enggan Buka Informasi Penyumbang Dana Kampanye, Berpotensi Lindungi Cukong Politik*. Diakses melalui <https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>, pada [16/10/2024].
- ¹³¹ Komisi Informasi Pusat. 2024. *MK KI Pusat Putuskan Sengketa Informasi Antara ICW dan KPU*. Diakses melalui <https://antikorupsi.org/id/kpu-enggan-buka-informasi-penyumbang-dana-kampanye-berpotensi-lindungi-cukong-politik>, pada [16/10/2024].
- ¹³² Lembaga Studi & Advokasi Masyarakat (ELSAM). 2023. *Data Pemilih Diduga Bocor, Integritas Pemilu 2024 Terancam*. Diakses melalui <https://www.elsam.or.id/si-aran-pers/data-pemilih-diduga-bocor-integritas-pemilu-2024-terancam>, pada [15/10/2024].
- ¹³³ Tempo. 2024. *4,7 Juta Data NIP dan NIK ASN Diduga Bocor, Pemerintah Sarankan Ganti Kata*. Diakses melalui <https://www.tempo.co/digital/4-7-juta-data-nip-dan-nik-asn-diduga-bocor-pemerintah-sarankan-ganti-kata-sandi-25998>, pada [20/10/2024].
- ¹³⁴ SAFEnet. 2024. *Laporan Situasi Hak-hak Digital Indonesia 2023: Sudah Roboh Tertimpa Pemilu Pula*. SAFEnet, hal. 30
- ¹³⁵ Komnas Perempuan. 2024. "CATAHU 2023: Catatan Tahunan Kekerasan Terhadap Perempuan Tahun 2023", <https://komnas-perempuan.go.id/download-file/1115>.
- ¹³⁶ Pasal 29 UU Pornografi mengatur: "Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengeksport, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksud dalam Pasal 4 ayat (1) dipidana dengan pidana penjara paling singkat 6 (enam) bulan dan paling lama 12 (dua belas) tahun dan/atau pidana denda paling sedikit Rp250.000.000,00 (dua ratus lima puluh juta rupiah) dan paling banyak Rp6.000.000.000,00 (enam miliar rupiah).
- ¹³⁷ Liputan 6. 2019. *Vonis Penjara untuk Ariel 8 Tahun Silam yang Membuat Luna Maya Pingsan*. Diakses melalui <https://www.liputan6.com/news/read/3881634/vonis-penjara-untuk-ariel-8-tahun-silam-yang-membuat-luna-maya-pingsan?page=2> pada [15/10/2024].

- ¹³⁸ BBC Indonesia. 2024. *Advokat LBH Yogyakarta yang tangani kasus dugaan kekerasan seksual di UII ditetapkan sebagai tersangka 'pencemaran nama baik*. Diakses melalui <https://www.bbc.com/indonesia/articles/c80xwnl79e7a> pada [10/10/2024].
- ¹³⁹ SAFEnet. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: Juli-September 2024*. SAFEnet, hal. 22.
- ¹⁴⁰ Mongabay. 2024. *Daniel Tangkilisan Karimunjawa Marin National Park Indonesia Environmental Activist Jailed*. Diakses melalui <https://news.mongabay.com/2024/04/daniel-tangkilisan-karimunjawa-marin-national-park-indonesia-environmental-activist-jailed/> pada [10/10/2024].
- ¹⁴¹ SAFEnet, *supra note* 133, hal. 9.
- ¹⁴² SAFEnet. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: Januari-Maret 2024*, 2024. SAFEnet, hal. 15.
- ¹⁴³ SAFEnet. 2024. *Laporan Pemantauan Hak-hak Digital di Indonesia Periode: April-Juni 2024*. SAFEnet, hal. 9.
- ¹⁴⁴ LBH Pers. 2024. "Permohonan Eksepsi Ditolak, Majelis Hakim Melanjutkan Kriminalisasi Septia". *Siaran Pers*, <https://lbhpers.org/2024/10/04/siaran-pers-permohonan-eksepsi-ditolak-majelis-hakim-melanjutkan-kriminalisasi-septia/> pada [15/10/2024].



SAFEnet

Southeast Asia
Freedom of
Expression Network
(SAFEnet)



PSHK
Pusat Studi Hukum &
Kebijakan Indonesia

Pusat Studi Hukum
dan Kebijakan
Indonesia
(PSHK)

Hak Digital untuk Demokrasi dan *Civic Space*:

Studi Pemetaan Regulasi
Internet di Indonesia

**April
2025**