

Laporan Situasi Hak-hak Digital Indonesia 2019

Bangkitnya Otoritarian Digital



SAFE net
SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

Juli 2020

**Bangkitnya Otoritarian Digital
Laporan Situasi Hak-hak Digital Indonesia 2019**

Tim Penyusun

Penanggungjawab : Damar Juniarto

Koordinator : Anton Muhajir

Tim Akses Informasi : Unggul Sagena, A. Ryan Sanjaya, Abul Hasan Banimal, Aseanty Fahlevi, Supriyono

Tim Kebebasan Berekspresi : Ika Ningtyas, Nenden Sekar Arum, Bimo Fundrika

Tim Keamanan Digital : Ellen Kusuma, Nike F. Andaru

Desain dan Ilustrasi : Daeng Ipul

Southeast Asia Freedom of Expression Network (SAFEnet)
Jl Gita Sura III no 55 Peguyangan Kaja
Denpasar, Bali 80115

Telepon: +628119223375

Surel: info@safenet.or.id

Situsweb: safenet.or.id

Daftar Isi

Pengantar	1
Profil SAFEnet	3
Ringkasan	5
Data Kasus	
• Hak untuk mengakses internet	9
• Hak untuk bebas bereskpresi	19
• Hak atas rasa aman	27
Epilog	43

Pengantar

Tahun politik 2019 memang sudah berlalu, tetapi sisanya masih terasa hingga tahun ini. Pemilihan presiden (pilpres) yang seharusnya menjadi perayaan dan kontestasi wajar dalam demokrasi, terasa penuh dengan silang sengketa termasuk di dunia maya. Hal itu turut mewarnai situasi kebebasan berinternet di negeri ini selama 2019. Sisa-sisa sengketa pilpres itu terasa antara lain pada terjadinya pemadaman internet pada 2019 serta maraknya kriminalisasi menggunakan pasal-pasal karet dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Saling sengketa dari pilpres 2019 menjadi salah satu catatan penting situasi hak-hak digital di Indonesia sepanjang tahun lalu. Meskipun demikian, pelanggaran hak-hak digital di Indonesia juga terjadi karena alasan lain, seperti konflik sosial dan lingkungan, terutama di daerah-daerah. Warga dikriminalkan atau dilanggar hak atas rasa amannya karena aktivitasnya dalam mengawasi layanan publik.

Situasi politik yang dinamis mengakibatkan terjadinya pelanggaran hak-hak digital selama 2019 meningkat tajam dibandingkan tahun-tahun sebelumnya. Data di Polri menunjukkan bahwa selama tiga tahun terakhir, jumlah kasus terkait Internet yang ditangani kepolisian memang terus bertambah yaitu 1.338 kasus pada 2017 lalu 2.552 (2018), dan 3.005 (sampai Oktober 2019).

Peningkatan kriminalisasi warga terkait aktivitasnya di Internet selama 2019 itu menjadi salah satu catatan yang terus berulang dari tahun ke tahun. Pengulangan lain adalah pembungkaman suara-suara kritis warga yang berekspresi dan berpendapat melalui Internet, terutama media sosial. Aktivistis dan jurnalis menjadi kelompok paling banyak menjadi korban, selain munculnya korban-korban baru terutama di kalangan akademisi.

Seperti sebelumnya, SAFEnet mencatat berbagai pelanggaran hak-hak digital warga tersebut melalui laporan tahunan, tradisi yang kami mulai sejak tahun lalu. Karena itu pula maka kami mengubah judul laporan, tidak lagi *Laporan Tahunan*, tetapi *Laporan Situasi Hak-hak Digital Indonesia*. Perubahan ini kami anggap perlu agar lebih bisa mencerminkan isi dari laporan itu sendiri selain juga mengenalkan isu tentang hak-hak digital.

Southeast Asia Freedom of Expression Network (SAFEnet) memberikan perhatian pada isu hak-hak digital sejak 2018, lima tahun setelah jaringan ini berdiri dan pada awalnya semata mengadvokasi kebebasan berekspresi daring (*online*). Secara umum, hak-hak digital ini meliputi hak untuk mengakses Internet, hak untuk berekspresi menggunakan media digital, dan hak atas rasa aman di media digital.

Laporan ini adalah upaya untuk tidak sekadar mencatat berbagai pelanggaran hak-hak digital yang terjadi selama 2019, tetapi juga menempatkannya dalam konteks lebih luas, bagaimana dampaknya terhadap demokrasi. Sebagai sebuah terminologi baru, hak-hak digital memang belum mendapatkan perhatian serius, termasuk

bagaimana hak-hak ini terkait erat dengan hak lebih mendasar, hak asasi manusia (HAM).

Laporan ini kami susun menggunakan tiga metode. Pertama, pengumpulan data dari laporan yang masuk langsung kepada kami selama 2019, terutama untuk kasus kriminalisasi dan kekerasan berbasis gender daring. Kedua, pengumpulan dari sumber-sumber skunder seperti kepolisian dan pengadilan yang datanya terbuka kepada publik, seperti di situs web mereka. Ketiga, melalui pemantauan media (*media monitoring*).

Kami membagi struktur laporan itu dalam tiga bidang utama terkait hak-hak digital yaitu hak untuk mengakses Internet, hak untuk berekspresi menggunakan media digital, dan hak atas rasa aman di dunia digital. Pembagian ini tidak kaku, karena pada satu dua kasus, dia bisa saja saling terkait sehingga tak bisa dihindarinya irisan bagian (kluster). Hal ini sekaligus untuk menunjukkan bagaimana tiap bagian dalam hak-hak digital memang terkait erat satu sama lain sebagai satu kesatuan.

Selain sebagai alat untuk mengenalkan isu hak-hak digital, kami berharap laporan situasi hak-hak digital ini juga bisa menjadi alat advokasi, mendorong agar negara mewujudkan pemenuhan dan perlindungan hak-hak digital ini. Selamat membaca.

Denpasar, Juli 2020



Tentang SAFEnet

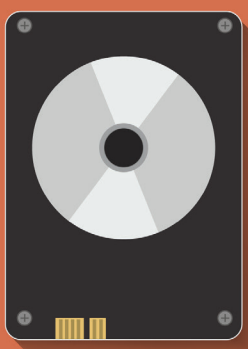
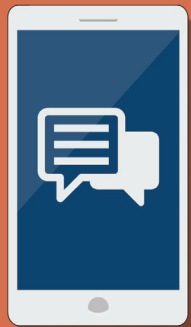
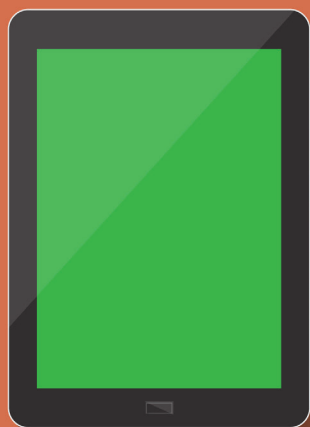
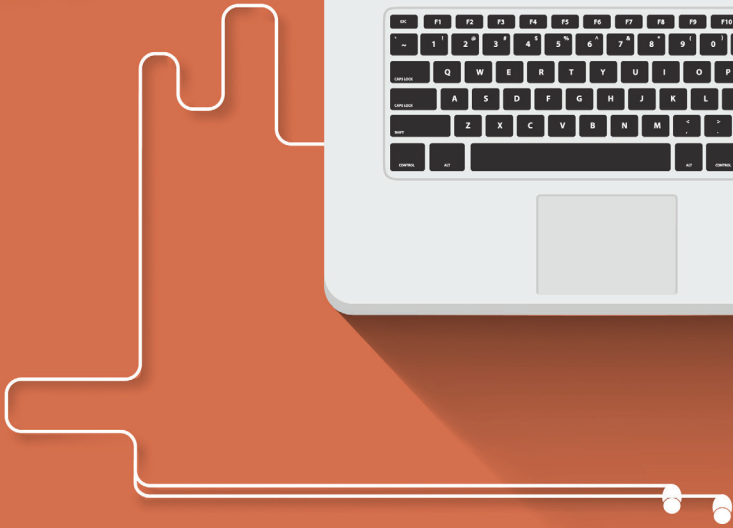
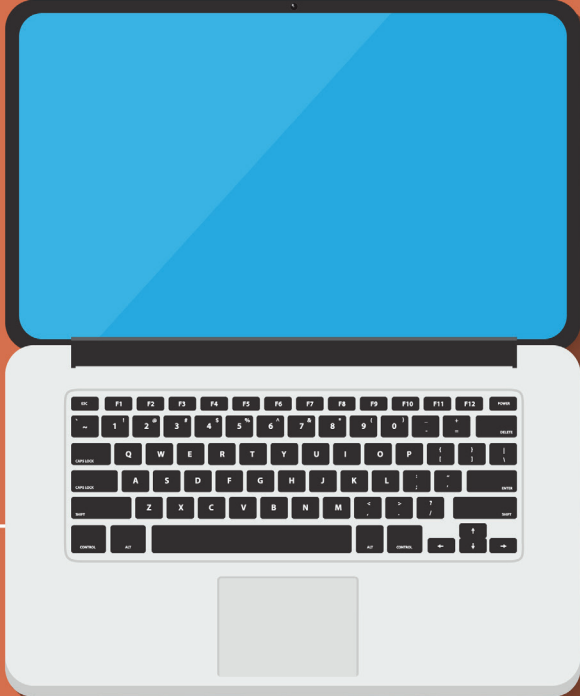
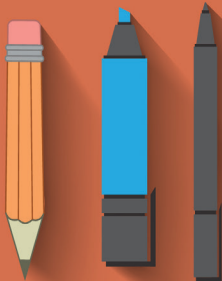
Southeast Asia Freedom of Expression Network (SAFEnet) merupakan jaringan pembela hak-hak digital di Asia Tenggara yang berdiri pada 27 Juni 2013 di Bali. Pada Januari 2019, SAFEnet resmi berbadan hukum dengan nama Perkumpulan Pembela Kebebasan Berekspresasi Asia Tenggara yang berkedudukan dan berkantor di Denpasar hingga saat ini.

Pendiri SAFEnet adalah blogger, jurnalis, ahli tatakelola Internet, dan aktivis. Latar belakang saat itu adalah maraknya kriminalisasi terhadap netizen (warganet) karena ekspresinya di Internet setelah berlakunya Undang-undang (UU) Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Meskipun UU ini kemudian direvisi menjadi UU No 19 tahun 2016, kriminalisasi terhadap warganet tetap marak.

Pada 2018 SAFEnet mulai memperlebar isu advokasi ke arah hak-hak digital setelah sebelumnya hanya fokus pada advokasi kebebasan berekspresasi daring. Hal tersebut karena makin meluasnya isu terkait Internet dari sudut pandang hak asasi manusia (HAM). Tidak semata hak untuk berekspresasi, tapi juga hak untuk mengakses Internet dan hak atas rasa aman.

Saat ini SAFEnet memiliki sekitar 40 sukarelawan yang tersebar di 23 kota, termasuk Pekanbaru, Pontianak, hingga Papua. Para sukarelawan memantau kasus-kasus terkait hak-hak digital, mengampanyekan pentingnya perlindungan hak-hak digital, dan membangun kapasitas masyarakat sipil dalam memperjuangkan hak-hak digital.

Kegiatan itu sejalan dengan program utama SAFENet yaitu (1) memantau pelanggaran hak-hak digital di Asia Tenggara, (2) memberikan advokasi pada tingkat kebijakan dan membantu korban untuk mengakses keadilan, serta (3) membangun dukungan, solidaritas, dan jaringan di antara pembela hak-hak digital lain di Asia Tenggara dan Indonesia khususnya.





Ringkasan

Kita pernah mengalami euforia, Internet dan media sosial bisa menjadi ruang untuk tumbuh suburnya kebebasan masyarakat sipil dan mendorong lahirnya masyarakat madani (*civil society*) yang berlandaskan pada demokrasi. Ada kebebasan, kesetaraan, dan kedaulatan warga. Euforia itu terwujud antara lain dengan menjamurnya gerakan-gerakan masyarakat berbasis Internet sebagai penyeimbang dan pengawas kekuasaan yang cenderung otoritarian.

Lebih dari satu dekade berlalu setelah lahirnya media-media sosial, seperti Facebook dan Twitter, yang turut menjadi katalis gerakan-gerakan masyarakat sipil termasuk di Indonesia, euforia itu meredup. Kebebasan di Internet yang pernah kita nikmati, makin hari makin dibatasi dengan aneka rupa pembenaran dan pola. Kesetaraan yang sempat kita rayakan, kini di bawah bayang-bayang distopia. Kedaulatan hak-hak digital yang belum sepenuhnya kita capai, kini nyaris sepenuhnya terampas.

Muram sekali, tetapi begitulah adanya.

Kecenderungan setahun terakhir menunjukkan bahwa hak-hak digital di Indonesia yang baru saja bisa kita nikmati sekitar satu dekade terakhir, kini justru di bawah ancaman kekuasaan yang otoriter. Pendokumentasian tentang situasi hak-hak digital Indonesia yang kami lakukan sepanjang tahun lalu mendukung tesis itu.

Seperti infrastruktur Internet yang menyangganya, hak-hak digital adalah satu mata rantai yang saling terkait mulai dari hak untuk mengakses, hak untuk berekspresi, dan hak atas rasa aman. Pertama-tama, warga seharusnya tidak hanya bebas mengakses Internet, tetapi bahkan dijamin haknya untuk memperoleh akses yang setara tanpa harus tersekat lokasi dan demografi. Kedua, dengan akses yang dimiliki, tiap warga seharusnya bebas mengekspresikan pendapat dan opininya tanpa harus takut akan ancaman. Ketiga, tanpa ancaman, setiap warga akan menemukan ruang bersama yang aman dan nyaman di dunia maya.

Sayangnya, situasi setahun terakhir kian jauh dari ideal.

Pemutusan Akses Internet

Selama 2019, terjadi tiga kali pemadaman Internet (*Internet shutdown*) sepihak yaitu di Jakarta dan sebagian Indonesia lain (tidak ada data jelas dari pemerintah) pada 22-24 Mei 2019, kemudian di Papua dan Papua Barat pada 21 Agustus 2019, serta pada 23-29 September 2019 di Wamena dan Jayapura.

Pelambatan dan atau pemblokiran akses Internet di Jakarta dan sebagian wilayah lain Indonesia pada Mei 2019 terkait dengan unjuk rasa menyikapi hasil pemilihan presiden 2019. Selama tiga hari ini, pemerintah resmi melakukan pemadaman Internet dengan istilah pelambatan Internet (*Internet throttling*) untuk “mencegah hoaks” dan “langkah antisipatif konflik agar tidak meluas” dan “menjaga ketertiban dan keamanan”.

Adapun pemutusan akses Internet di Papua dan Papua Barat terkait erat dengan demo menentang tindakan rasisme pada mahasiswa Papua di Surabaya dan Malang, Jawa Timur. Pemerintah melakukan pelambatan akses di beberapa wilayah Provinsi Papua Barat dan Provinsi Papua, termasuk Kota Jayapura, Kabupaten Jayapura, Kabupaten Mimika, dan Kabupaten Jayawijaya serta Kota Manokwari dan Kota Sorong.

Pemadaman Internet menjadi pola baru pemerintah Indonesia dari sebelumnya lebih banyak memblokir akses pada situs atau aplikasi tertentu. Kebijakan ini memang pola baru untuk melanggar hak atas Internet atas nama keamanan nasional sebagaimana juga terjadi di wilayah Rakhine (Myanmar), Kashmir (India), dan Catalan (Spanyol).

Pemutusan akses Internet sebagai pola baru pembatasan akses terhadap Internet itu melengkapi tantangan lama keterjangkauan akses Internet di Indonesia, kesenjangan lokasi, demografi, dan gender. Dari sisi lokasi, Internet di Indonesia pada 2019 masih terkonsentrasi di Jawa (55%), diikuti Sumatera

21%, Papua 10%, Kalimantan 9%, sedangkan Bali dan Nusa Tenggara memiliki pengguna Internet terkecil, hanya 5%.

Dari sisi gender, akses Internet di Indonesia juga masih mengalami kesenjangan digital di mana sebanyak 72% dari laki-laki dewasa memiliki ponsel sedangkan perempuan dewasa 64%. Adapun pengguna ponsel yang mengakses Internet sebesar 43% pada laki-laki dan 36% pada perempuan.

Kriminalisasi terhadap Ekspresi

Ketika akses Internet makin dibatasi melalui beragam cara, termasuk pemutusan akses, dan menghadapi masalah lama yang belum terselesaikan, seperti kesenjangan digital, pada saat yang sama, penggunaannya menghadapi ancaman berulang difasilitasi oleh pasal-pasal karet dalam UU ITE. Pendokumentasian sepanjang 2019 menunjukkan bahwa kriminalisasi terhadap ekspresi tetap marak terjadi.

Dari laporan masuk ke SAFEnet, terdapat 24 kasus pemidanaan dengan UU ITE. Jumlah itu menurun dibandingkan kasus setahun sebelumnya yang mencapai 25 kasus. Dari sisi latar belakang, jurnalis dan media masih menjadi korban terbanyak dari kriminalisasi ini sebanyak 8 kasus, terdiri atas 1 media dan 7 jurnalis menjadi korban. Dalam dua tahun terakhir, jumlah media dan jurnalis yang dipidanakan cenderung lebih tinggi dibandingkan tahun-tahun sebelumnya.

Korban terbanyak kedua adalah aktivis dan warga dengan 5 kasus. Jumlah ini naik 1 kasus dibandingkan tahun sebelumnya. Posisi berikutnya adalah tenaga pendidik dan artis masing-masing 3 kasus.

Dari aspek pasal pemidanaan, Pasal 27 ayat 3 UU ITE (defamasi) paling banyak

digunakan untuk melaporkan yaitu sebanyak 10 kasus. Disusul Pasal 28 ayat 2 (kebencian) sebanyak 8 kasus. Penggunaan dua pasal sekaligus juga muncul yaitu, Pasal 27 ayat 1 (pornografi) dengan Pasal 27 ayat 3 sebanyak 3 kasus. Terakhir, penggunaan Pasal 27 ayat 1 dengan Pasal 28 ayat 2 terdapat 1 kasus.

Dua fakta tersebut menunjukkan keterkaitan bahwa jurnalis, aktivis, dan warga kritis paling banyak dikriminalisasi dengan menggunakan pasal-pasal karet yang cenderung multitafsir dengan tujuan membungkam suara-suara kritis. Tesis itu kemudian didukung oleh fakta lain bahwa ternyata latar belakang pelapor yang paling banyak menggunakan pasal-pasal karet itu adalah pejabat publik dan politisi dengan 10 laporan.

Hal lain yang perlu diwaspadai adalah meluasnya korban kriminalisasi menggunakan UU ITE. Sepanjang tahun lalu, mulai marak terjadi kriminalisasi terhadap akademisi yang bersuara kritis terhadap isu politik nasional maupun di kampusnya.

Meskipun demikian, data yang kami himpun hanya puncak gunung es dari jumlah kasus sebenarnya. Sebagai perbandingan, menurut Direktorat Tindak Pidana Siber Markas Besar Kepolisian Republik Indonesia (Mabes Polri), jumlah penyelidikan terhadap akun media sosial selalu naik setiap tahun, yakni 1.338 kasus pada 2017, 2.552 kasus pada 2018, dan melonjak pada 2019 menjadi 3.005 kasus hingga Oktober 2019. Dari 3.005 kasus hingga Oktober itu, aduan terbanyak adalah penghinaan tokoh, penguasa, atau badan umum dengan 676 kasus.

Dari jumlah itu, kasus terbanyak adalah penyelidikan menyangkut penghinaan tokoh, penguasa dan badan umum. Pada 2017 ada 679 kasus yang diselidiki terkait penghinaan, kemudian meningkat 1.177 pada 2018 dan turun pada 2019 menjadi 676 kasus. Kasus tinggi lainnya yakni mengenai dugaan provokasi dan ujaran kebencian.

Tiga kasus ini kerap merujuk pada penggunaan pasal-pasal karet di UU ITE. Jeratan pasal karet dalam UU ITE terus berlanjut sepanjang tahun lalu.

Ancaman yang Kian Mencekam

Setelah pembatasan akses dan ancaman kriminalisasi, pengguna Internet di Indonesia juga harus menghadapi semakin kuatnya

kekerasan digital, terutama kepada suara-suara kritis terhadap kekuasaan maupun perempuan.

Sejak Juli 2019, SAFEnet bekerjasama dengan Komisi Nasional (Komnas) Perempuan mencatat kasus-kasus kekerasan berbasis gender siber (KBGS). Sepanjang 2019, SAFEnet menerima 60 aduan kasus KBGS di mana 44 kasus di antaranya adalah dari rujukan Komnas Perempuan pada SAFEnet. Adapun 16 aduan lain masuk melalui kanal-kanal komunikasi SAFEnet, termasuk yang diarahkan oleh mitra atau komunitas lain untuk membuat pengaduan di SAFEnet.

Dari jumlah tersebut, 53 korban yang mengadu adalah perempuan dan 7 lainnya tidak menyebut gendernya. Bentuk KBGS paling banyak dilaporkan adalah penyebaran konten intim tanpa persetujuan (*nonconsensual dissemination of intimate images*) sebanyak 45 kasus, pelanggaran privasi (seperti doksing, pengawasan nonkonsensual, penyadapan, akses tanpa otorisasi) sebanyak 7 kasus, pembuatan akun peniru atau impersonasi sebanyak 2 kasus, pamer alat kelamin di ruang digital tanpa persetujuan (*digital exhibitionism*) sebanyak 3 kasus, dan bentuk lain seperti memermalukan korban di ruang digital publik (*online shaming*) atau pelanggaran privasi korban di luar dari penjelasan di atas.

KBGS di atas tidak selamanya terjadi secara tunggal dalam satu bentuk. Terdapat pula beberapa kekerasan yang terjadi sekaligus. Misalnya penyebaran informasi data pribadi korban tanpa persetujuan ke dunia maya. Begitupun dengan platform yang digunakan, tidak hanya satu platform media sosial, tetapi juga beberapa sekaligus. Misalnya, tak hanya di percakapan ringkas (instant messenger), tetapi juga Twitter, Instagram, dan Facebook.

Seperti halnya pada pembatasan akses Internet dan kriminalisasi terhadap pengguna, pelanggaran terhadap rasa aman ini pun ada yang terjadi karena motivasi politik. Pada awalnya, kasus-kasus KBGS lebih banyak terjadi karena motivasi balas dendam oleh pasangan atau mantan

pasangan serta relasi timpang antara laki-laki dan perempuan. Namun, pada tahun lalu juga mulai terjadi KBGS dengan motivasi politik. Seorang aktivis perempuan menjadi korban melalui penyebaran foto telanjangnya dengan fitnah perselingkuhan bersama mitra kerjanya yang juga aktivis. Penyebaran materi itu adalah upaya mendelegitimasi kerja-kerja mereka dalam menolak revisi Undang-Undang Komisi Pemberantasan Korupsi (KPK).

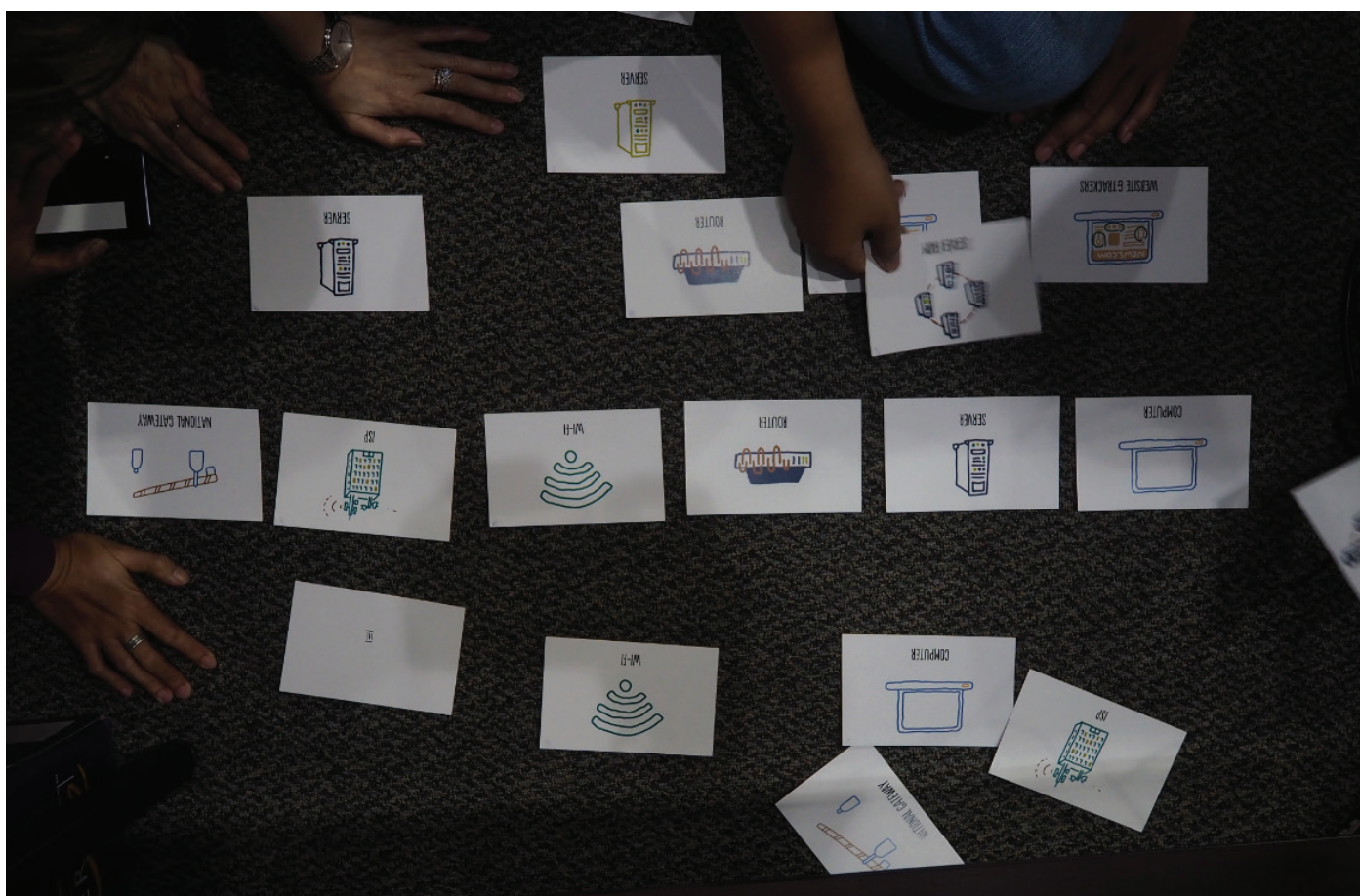
Politisasi tubuh perempuan sebagaimana terjadi pada aktivis penolak revisi UU KPK itu menjadi penanda bagaimana kian hari Internet telah menjadi alat bagi kekuasaan untuk membungkam suara-suara kritis warga melalui berbagai cara. Tidak hanya membatasi dan bahkan memutus akses Internet atau mengancam dengan kriminalisasi terhadap ekspresi politik mereka, tetapi juga bahkan melakukan kekerasan berbasis gender siber untuk tujuan politik.

Jika semua pelanggaran hak-hak digital oleh negara itu dibiarkan, maka kebebasan Internet yang pernah kita gadang-gadang sebagai sebuah kemajuan di Indonesia hanya menunggu waktu untuk kembali masuk kuburan.

“

Setelah pembatasan akses dan ancaman kriminalisasi, pengguna Internet di Indonesia juga harus menghadapi semakin kuatnya kekerasan digital, terutama pada suara-suara kritis terhadap kekuasaan dan perempuan.

”



Hak untuk Mengakses Internet

Internet di Indonesia

Tidak ada data pasti berapa jumlah pengguna Internet di Indonesia hingga 2019. Namun, beberapa sumber menyebut jumlahnya berkisar 120 juta jiwa hingga 175,4 juta jiwa. Menurut Data Reportal, hingga Januari 2020, jumlah pengguna Internet mencapai 175,4 juta, dengan penambahan 25 juta atau 17% dibandingkan tahun sebelumnya. Penetrasi Internet mencapai sekitar 64% dari jumlah penduduk. Sumber yang sama menyebut, jumlah pengguna media sosial di Indonesia mencapai 160 juta hingga Januari 2020, meningkat 12 juta atau 8,1% antara April 2019 hingga Januari 2020¹.

Data lain dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyebutkan, jumlah pengguna Internet Indonesia hingga Mei 2019 sebanyak 171,1 juta, meningkat 10% dari tahun sebelumnya yaitu 143,26 juta.

Adapun tingkat penetrasi mencapai 64,8%². Sebagian besar pengguna mengakses Internet dari perangkat bergerak (*mobile devices*), seperti telepon seluler, tablet, dan laptop. Saking banyaknya pengguna perangkat bergerak, jumlahnya bahkan melebihi jumlah pengguna yaitu mencapai 338,2 juta atau 124% dari jumlah penduduk.

Menurut Statista Dossier hanya 14% pengguna berlangganan Internet rumah (*fixed Internet subscription*), tetapi 97% pengguna Internet rumahan tersebut mengakses pula dari perangkat ponsel³. Adapun penggunaannya masih didominasi kebutuhan pesan singkat melalui platform berbasis Internet dan media sosial⁴.

² <https://dailysocial.id/post/pengguna-internet-indonesia-2018>

³ <https://www.statista.com/statistics/1036571/indonesia-fixed-internet-subscription-at-home/>

⁴ <https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/>

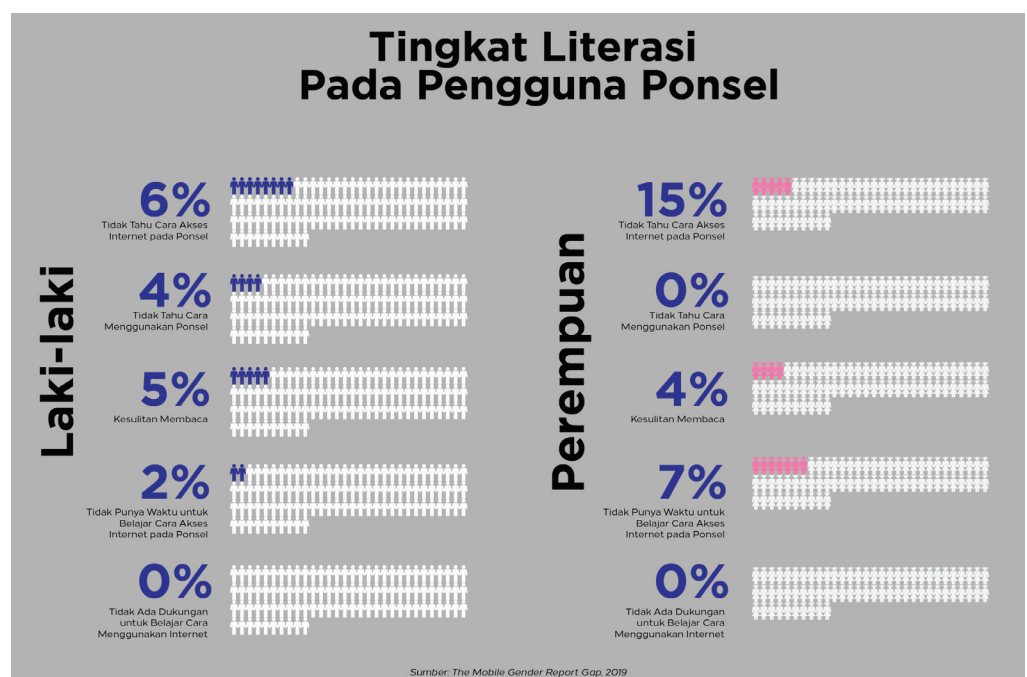
¹ <https://datareportal.com/reports/digital-2020-indonesia>

Akses Internet : Geografi, Demografi dan Gender

Masih menurut hasil survei APJII, hingga akhir 2018, akses Internet masih terfokus di Pulau Jawa (55,7%) baru kemudian Sumatera (21,6%), Sulawesi, Papua, dan Maluku (10,9%), Kalimantan (6,6%), dan Bali Nusa Tenggara (5,2%). Selain demografi, masih terdapat pula kesenjangan akses Internet di mana hanya 20,3% petani penggarap yang menggunakan Internet di Indonesia. Bandingkan dengan, misalnya, buruh pabrik yang 71,6% di antaranya menggunakan Internet atau Aparat Sipil Negara yang mencapai 89,9%. Adapun alasan mereka tidak memakai Internet adalah karena tidak tahu cara menggunakan.

Dari sisi umur, APJII mencatat bahwa penetrasi tertinggi pengakses Internet datang dari umur 15-19 tahun sebesar 91%. Disusul kelompok usia 20-24 tahun (88,5%) dan 25-29 tahun (82,7%). Penetrasi terendah adalah kelompok usia 65 tahun keatas (8,5%). Dari kalangan umur tersebut, tidak tercatat perbandingan antara pengguna lelaki dan perempuan, tetapi menurut laporan tahunan GSMA 2019, Indonesia masih mengalami kesenjangan digital berdasarkan gender. Sebesar 72% dari laki-laki dewasa memiliki ponsel, sementara pada perempuan dewasa mencapai 64%. Menariknya, tidak setiap orang yang menggunakan ponsel itu mengakses Internet. Pengguna ponsel yang mengakses Internet sebesar 43% pada laki-laki dan 36% pada perempuan.

Persoalan akses Internet itu tidak terbatas pada persoalan infrastruktur yang disediakan, tetapi juga karena tingkat literasi. Kesenjangan tingkat literasi Internet pada gender perempuan dan laki-laki ditunjukkan pada tabel berikut ini:



Sayangnya, di tengah lebarnya kesenjangan digital antara Jawa dan luar Jawa, terjadi pula pelanggaran hak atas akses Internet yang bahkan sebenarnya sudah sangat terbatas tersebut, misalnya pemadaman Internet di Papua dan Papua Barat.

Polemik Pemadaman Internet

Dalam konteks hak atas akses kepada informasi, kasus yang menjadi perhatian utama di Indonesia adalah terjadinya pemadaman akses Internet. Pemerintah Indonesia menggunakan beberapa istilah dalam pemadaman akses Internet seperti pelambatan Internet (*Internet throttling*), “antisipasi hoaks”, “percepatan proses pemulihan keamanan”, “pencegahan kerusakan” dan beragam frasa lain, yang pada intinya adalah tetap *Internet shutdown* yang melanggar HAM.

Secara sederhana, pemutusan Internet adalah gangguan terhadap komunikasi berbasis Internet secara sengaja yang mengakibatkan tidak bisa diaksesnya layanan Internet. Pemutusan akses Internet ini bisa dilakukan pada populasi, lokasi, atau layanan tertentu dengan tujuan mengontrol arus informasi. Dia bisa terjadi di tingkat nasional atau pada daerah dan pengguna tertentu.

Selama 2019, terjadi tiga kali pemadaman Internet sepihak yaitu di Jakarta dan sebagian Indonesia lain (tidak terdapat data jelas dari pemerintah) serta dua kali di Papua dan Papua Barat. Tiga kali pemadaman tersebut dilakukan pada 22-24 Mei 2019, pada 21 Agustus 2019 di Papua dan Papua Barat, serta pada 23-29 September 2019 di Wamena dan Jayapura. Ketiganya memiliki motivasi yang sama yaitu politik.



Pemblokiran akses dan pelambatan Internet pada Mei 2019 terjadi setelah adanya unjuk rasa pasca-pengumuman hasil pemilihan presiden (Pilpres), tepatnya pada 22-24 Mei 2019. Selama tiga hari ini, pemerintah resmi melakukan pemadaman Internet dengan memunculkan dan memperkenalkan istilah pelambatan Internet (*Internet throttling*) secara resmi ke masyarakat dengan tujuan “mencegah hoaks” dan “langkah antisipatif konflik agar tidak meluas” dan “menjaga ketertiban dan keamanan”.

Dalih menjaga ketertiban dan keamanan itu menimbulkan banyak masalah terhadap warga. Pembatasan Internet justru menyulitkan jurnalis melakukan verifikasi di lapangan atau warga yang memverifikasi informasi kepada kerabatnya di lapangan, termasuk yang ikut berunjuk rasa. Pembatasan Internet itu juga mengakibatkan terjadinya informasi satu arah dan monopolistik dari Pemerintah.

Pemadaman akses Internet kedua pada September 2019 menjadi bukti bahwa pola itupun kemudian semakin lumrah bagi pemerintah. Pemerintah memadamkan Internet di Papua setelah kerusuhan sipil pecah di sejumlah kota di Papua Barat dan Papua. Kerusuhan bermula dari diskriminasi rasial pada mahasiswa Papua di Surabaya. Lambannya penanganan kasus kekerasan rasial oleh penegak hukum berbuntut unjuk rasa di berbagai daerah.

Alih-alih pemerintah mengusut tuntas pelaku rasialisme dan kekerasan terhadap mahasiswa Papua, antara lain di Malang, 15 Agustus 2019 dan di Surabaya pada 16 Agustus 2019, Kementerian Komunikasi dan Informasi (Kemkominfo) justru memperlambat dan kemudian memblokir Internet dengan dalih mencegah tersebarnya informasi palsu di Papua dan Papua Barat. Alasan serupa dilakukan terus menerus, dengan berpedoman bahwa selain informasi versi pemerintah, maka informasi versi lain bisa dicap hoaks atau berita palsu (*fake news*). Padahal tidak sesederhana itu.

Detail pemadaman Internet adalah sebagai berikut. Pertama, pemerintah melakukan pelambatan akses di beberapa wilayah Provinsi Papua Barat dan Provinsi Papua pada 19 Agustus 2019 sejak pukul 13.00 WIT sampai 20.30 WIT. Pemadaman kedua yaitu pada saat pemerintah dengan sengaja melakukan pemblokiran layanan data dan/atau pemutusan akses Internet secara menyeluruh di Provinsi Papua (29 kota/kabupaten) dan Provinsi Papua Barat (13 kota/kabupaten) tertanggal 21 Agustus sampai dengan setidaknya-tidaknya pada 4 September 2019 pukul 23.00 WIT.

Sedangkan pemadaman ketiga adalah dengan memperpanjang pemblokiran layanan data dan/atau pemutusan akses Internet di 4 kota/kabupaten di Provinsi Papua (yaitu Kota Jayapura, Kabupaten



Tabel Pemadaman Akses Internet di Indonesia Tahun 2019

No.	Lokasi	Waktu	Pelaku	Alasan & Keterangan
1	Seluruh Indonesia	22 – 24 Mei 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ <i>Bandwidth throttling</i> atau pelambatan akses Internet, pembatasan akses media sosial dan aplikasi ▪ Langkah antisipatif untuk mencegah konflik meluas ▪ Membatasi penyebaran hoaks
2	Provinsi Papua dan Papua Barat	21 Agustus 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ Alasannya adalah “..mempercepat proses pemulihan situasi keamanan..” (Sumber: Kompas.com) ▪ Akses Internet diblokir selama dua pekan. (Sumber: CNNIndonesia.com) ▪ Pemadaman Internet selama 338 jam. (Sumber: vice.com)
3	Kota Wamena dan sebagian Jayapura	23 – 29 September 2019	Kemkominfo	<ul style="list-style-type: none"> ▪ Dilakukan saat kasus kerusakan di Wamena dan sebagian kota Jayapura ▪ Alasan: meredam penyebaran hoaks, mencegah kerusakan meluas

Jayapura, Kabupaten Mimika, dan Kabupaten Jayawijaya) dan 2 kota/kabupaten di Provinsi Papua Barat (yaitu Kota Manokwari dan Kota Sorong) sejak 4 September 2019 pukul 23.00 WIT sampai dengan 9 September 2019 pukul 18.00 WIB/20.00 WIT.

Sepanjang 2019 Indonesia mengalami pemutusan Internet shutdown selama 416 jam. Total perkiraan kerugian yang didapatkan karena tindakan tersebut dilaporkan sebesar 187,7 juta USD, atau sekitar Rp 2,5 triliun⁵.

Pemadaman Internet itu menjadi masalah karena tidak dilakukan melalui mekanisme terbuka dan partisipatif. Semua dalih pemerintah hanya ditetapkan sepihak tanpa

menunjukkan prinsip-prinsip akuntabilitas. Hal inilah yang membuat SAFEnet dan organisasi jaringan memprotes tindakan tersebut, termasuk melalui petisi daring maupun gugatan hukum.

⁵ <https://www.top10vpn.com/cost-of-internet-shutdowns/>

Dominasi Cina dalam Dunia Digital Indonesia

Salah satu isu dalam pemenuhan hak-hak digital lima tahun terakhir adalah menguatnya dominasi China dalam kehidupan digital warga Indonesia, dari perangkat keras, perangkat lunak, hingga bisnis digital. Contohnya dalam hal perangkat keras, setelah sekian lama produk Korea Selatan yaitu Samsung menguasai pasar Indonesia, kini pelan-pelan China mulai menguasai, terutama jika digabungkan.

Berdasarkan data Statcounter GlobalStats, penjualan ponsel pintar di Indonesia sepanjang Mei 2019 - Mei 2020 didominasi Samsung, OPPO dan Xiaomi. Ketiganya konsisten mempertahankan *market-share* di atas 15% sepanjang satu tahun. Secara satuan, Samsung masih merajai seperempat dari total penjualan ponsel pintar di seluruh Indonesia, yaitu di angka 24,91% pada Mei 2020 dan 25,93% pada Mei 2019.

Produk asal China OPPO dan Xiaomi bersaing secara fluktuatif mendominasi peringkat kedua dan ketiga. Pada Mei 2020, OPPO berada di peringkat kedua dengan *market-share* sebesar 20,62%, naik dari 18,6% pada Mei 2019. OPPO mengalami kenaikan

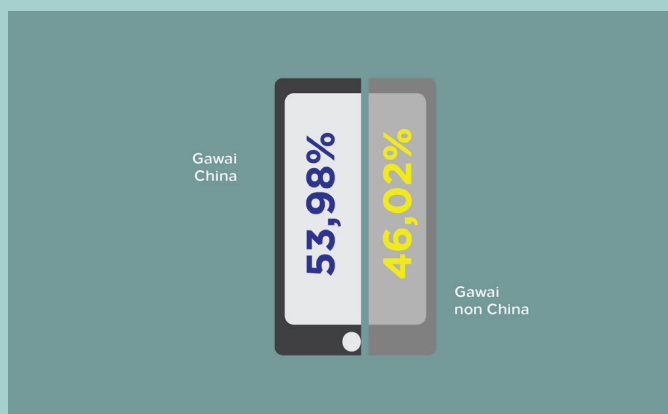
penjualan yang signifikan pada November 2019, diikuti dengan kenaikan yang stabil di bulan-bulan berikutnya sampai akhirnya pada Januari 2020 menggeser posisi Xiaomi yang dari awal menduduki peringkat kedua. Xiaomi memiliki *market-share* sebesar 19,8% pada Mei 2020, turun dari 21,07% dari Mei 2019, membuatnya menduduki peringkat ketiga pada Mei 2020.

Market Share Ponsel Pintar di Indonesia

Nama Produk	Asal Negara	Mei 2019	Mei 2020
Samsung	Korea Selatan	25.93%	24.91%
OPPO	China	18.6%	20.62%
Xiomi	China	21.07%	19.8%
Mobicel	Afrika Selatan	7%	11.4%
Apple	Amerika Serikat	5.51%	7.86%
Realme	China	0.03%	3.72%
ASUS	Taiwan	4.12%	2.97%
Tidak Diketahui	-	7.78%	2.88%
Huawei	China	1.13%	1.05%
Lenovo	China	1.87%	0.83%

Sumber: [Statcounter GlobalStats](#)

Untuk produk China dengan kategori *market-share* di bawah 15%, Realme, Huawei dan Lenovo masing-masing memiliki *market-share* sebanyak 3,72%, 1,05%, 0,83% pada Mei



2020. Dari ketiganya, Realme merupakan produk yang mengalami kenaikan pesat dalam kurun satu tahun di mana ia yang awalnya berada di urutan terbawah dengan 0,03% pada Mei 2019, naik signifikan ke angka 3,72% pada Mei 2020.

Secara umum, China menguasai hampir separuh dari *market-share* ponsel pintar di Indonesia, yakni sebesar 46,02% di Mei 2020. Angka tersebut naik sebesar 3,3% dari 42,7% pada bulan yang sama di tahun sebelumnya. Penyebab dominasi China dalam bursa pasar ponsel pintar di Indonesia ialah banyaknya varian produk yang disuguhkan kepada konsumen di Indonesia, dibandingkan negara asing lainnya.

Sumber lain menyebut *vendor smartphone* China menguasai 75% dari total pengiriman *smartphone* di Indonesia, pada kuartal III-2019.⁶ Dari lima besar *vendor smartphone* di Indonesia, empat di antaranya adalah produk Cina. Mereka adalah Oppo, Vivo, Realme, dan Xiaomi.

Tingginya pasokan ponsel *Made in China* di Indonesia sudah tergambarkan dalam perubahan nilai impor perlengkapan telekomunikasi dari negara Tirai Bambu. Pada 2007, impor produk perlengkapan telekomunikasi dari Cina melonjak tiga kali lipat dibanding tahun sebelumnya, lalu terus meledak hingga tak terkejar lagi oleh impor dari negara lain. Sebagai gambaran, dapat dilihat pada grafik di halaman berikutnya.

Aplikasi Ponsel Pintar

Tidak seperti perangkat keras, perangkat lunak asal China masih kalah saing dengan produk dari negara lain. Ini bisa dilihat dari jumlah peringkat dan penggunaan aplikasi ponsel pintar di PlayStore. Hingga Juni 2020 lalu, Indonesia masih dikuasai produk Amerika Serikat, seperti WhatsApp, Instagram, Twitter, YouTube, dan seterusnya. Aplikasi-aplikasi tersebut mendominasi tak hanya dari sisi peringkat unduh, tetapi juga penggunaan.

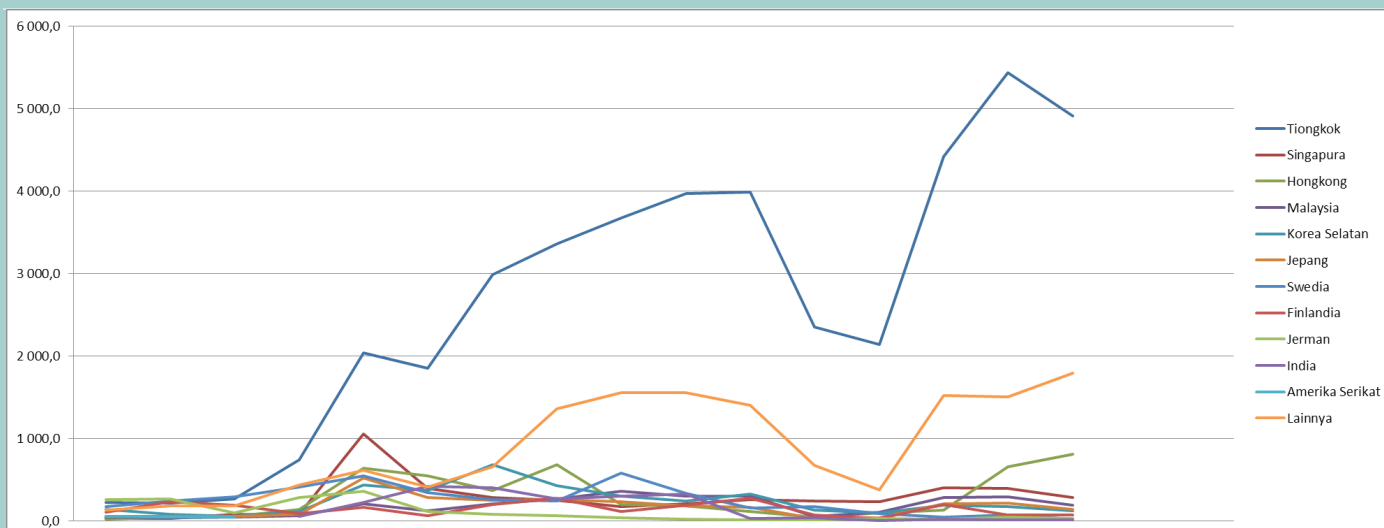
Dari sisi aplikasi, hanya ada empat aplikasi asal China yang masuk 20 besar untuk di Indonesia, yaitu TikTok (peringkat 3), SHAREit (peringkat 5), Mobile Legend (peringkat 8) dan Lazada (peringkat 18). Sementara dari segi penggunaan, hanya ada satu aplikasi asal China yang bisa masuk 20 besar yaitu UC Browser di peringkat 17.

Penetrasi perangkat lunak asal Cina perlahan-lahan mulai menjadi alternatif yang diperhitungkan di Indonesia. Pada Januari 2020 lalu, Bank Indonesia mengeluarkan izin bagi WeChat Pay untuk beroperasi di Indonesia. WeChat Pay adalah platform sistem pembayaran, yang merupakan kembangan dari aplikasi pesan instan WeChat. Mereka akhirnya bisa masuk ke Indonesia menggunakan jaringan PT Bank CIMB Niaga Tbk. Aplikasi saingannya yang juga berasal dari Cina, Alipay, kabarnya juga sedang menunggu izin untuk beroperasi di Indonesia. Alipay akan menggunakan jaringan PT Bank Central Asia Tbk.

Hal ini sesuai dengan peraturan dari negeri Cina mengenai pembatasan uang tunai yang dibawa oleh turis. Selain itu juga lebih dari 90% penduduk di kota-kota besar di Cina menggunakan WeChat Pay dan Alipay sebagai platform pembayaran utama.⁷ Maka tidak heran pangsa pasar dari kedua platform asal Cina adalah wisatawan mancanegara (wisman) dari negara mereka sendiri. Daerah-daerah yang diprediksi akan menjadi tempat transaksi yang tinggi menggunakan WeChat Pay dan Alipay ini adalah Bali, Jakarta, dan Yogyakarta.

⁶ Berita di akses pada tautan <https://tekno.kompas.com/read/2019/11/18/17080077/merek-china-kuasai-75-persen-pasar-smartphone-indonesia>

⁷ Informasi dapat dibaca di <https://katadata.co.id/berita/2020/02/12/wechat-pay-alipay-diyakini-tak-akan-rajai-pasar-dompot-digital-lokal>



Impor Perlengkapan Elektronik 2002 – 2019

Sumber: Diolah dari BPS¹

1 Data dapat dilihat di <https://www.bps.go.id/statictable/2014/09/08/1049/nilai-impor-perlengkapan-telekomunikasi-menurut-negara-asal-utama-nilai-cif-juta-us-2002-2019.html>

Isu Keamanan Data

Tingginya penggunaan aplikasi digital buatan Cina menjadi isu tersendiri, terutama bagi Amerika Serikat (AS) yang terlibat perang dagang dengan Cina. Keresahan ini muncul karena potensi risiko keamanan bagi para pengguna dan bahkan sebuah negara. Perusahaan teknologi asal Cina yang saat ini 'berperang' dengan AS adalah Huawei.

Huawei adalah perusahaan penyedia peralatan dan layanan telekomunikasi terbesar di dunia. Teknologi yang mereka gunakan berkembang sangat pesat dan saat ini sedang mempersiapkan teknologi 5G. Perkembangan teknologi Huawei ini oleh AS dianggap sebagai jalan masuk bagi intelijen Cina untuk menjalankan aksi memata-matai pemerintahan AS. Akibatnya, Huawei menjadi salah satu perusahaan yang masuk daftar hitam pemerintah AS. Presiden AS Donald Trump dikabarkan membatasi pasokan komponen untuk Huawei.

Negara barat, utamanya Amerika Serikat, menuduh perangkat 5G yang dikembangkan Huawei memiliki *backdoor* (pintu belakang) yang bisa digunakan oleh pemerintah Cina untuk melakukan *surveillance* sehingga ia bisa memata-matai kondisi negara tertentu. Meski tuduhan tersebut dibantah keras oleh Huawei dan pemerintah Cina, produk dan jasa Huawei telah ditolak di beberapa negara termasuk Amerika Serikat, Australia, Selandia Baru, Inggris, Jepang, Prancis dan

Jerman.⁸

Pada Januari 2019 Departemen Kehakiman AS dikabarkan melayangkan tuntutan pidana terhadap Huawei dan direktur keuangannya, Meng Wanzhou.⁹ AS menuntut 23 dakwaan terhadap Huawei, mulai dari kasus pencurian teknologi T-mobile hingga memperdaya AS untuk menjalin bisnis dengan Iran.

Terdapat spekulasi di ranah global bahwa produk digital asal China disebut memiliki kelemahan dari segi keamanan berdasarkan asumsi bahwa produk China diduga selalu berada di bawah bayang-bayang pemerintahan China, sehingga ia bisa dijadikan alat untuk spionase. Isu terkait yang menjadi topik perbincangan ialah infrastruktur perangkat 5G yang kini dikembangkan Huawei, sebagai pemimpin dan pemilik paten terbesar di pengembangan perangkat 5G.¹⁰

Huawei di Indonesia

Huawei memulai bisnisnya di Indonesia sejak 2000 dengan menjual alat komunikasi dan jasa konsultasi. Sebagai vendor infrastruktur digital, Huawei dengan bantuan mitranya kini melayani sekitar 500 klien dari berbagai

⁸ <https://www.thejakartapost.com/news/2018/12/18/huawei-defends-global-ambitions-amid-western-security-fears.html>

⁹ Informasi dapat dilihat di <https://www.bbc.com/indonesia/indonesia-47037816>

¹⁰ <https://www.cnbcindonesia.com/tech/20200611133719-37-164647/saat-donald-trump-tidak-berdaya-di-hadapan-huawei>



oppo vivo



sektor, termasuk pemerintah, perusahaan infrastruktur, dan lain-lain. Huawei berharap ke depannya bekerja lebih dekat dengan sektor kesehatan dan kecantikan untuk membantu mendigitalkan sistem mereka.¹¹

Selain itu, Huawei juga sudah mengantongi beberapa aplikasi asal Indonesia yang kini terdaftar di AppGallery, yakni platform yang diluncurkan Huawei sebagai alternatif dari Google Play dan App Store. Per January 2020, AppGallery sudah memiliki lebih dari 40 aplikasi buatan Indonesia baik dalam sektor perbankan (Permata Bank, BCA Mobile, Link Aja) dan e-commerce (Bibli, Tokopedia, Bukalapak). Huawei menargetkan akan ada 73 aplikasi asal Indonesia yang terdaftar di AppGallery per Maret 2020.¹²

Tak hanya dari sisi bisnis digital, Huawei juga masuk ke isu keamanan nasional di Indonesia. Pada Oktober 2019, Badan Siber dan Sandi Negara (BSSN) menggandeng Huawei dalam memperkuat keamanan siber di Indonesia melalui pengembangan sumber daya manusia pegawai BSSN.¹³ Namun, meskipun Huawei dituduh berpotensi mengancam keamanan, BSSN menyatakan tidak ada yang perlu dikhawatirkan dari kerja sama ini karena hanya terkait pengembangan SDM. BSSN menepis kerja sama ini sebagai bentuk kecondongan pada negara tertentu. Sebaliknya, ini malah mempertegas bahwa BSSN bertindak netral mengingat pada tahun sebelumnya di 2018, BSSN juga bekerja sama dengan perusahaan Amerika Serikat, Cisco.¹⁴

Terkait penerapan jaringan 5G di Indonesia, Kominfo saat ini masih mengkaji frekuensinya. Pemerintah berharap Kutai Kartanegara sebagai Ibukota baru menjadi kota pertama yang akan menggunakannya. Tidak ada kepastian kapan jaringan 5G akan diterapkan di tanah air, tetapi menurut Asosiasi Penyelenggara Jasa Telekomunikasi

Indonesia (ATSI) jaringan ini bisa diterapkan mulai tahun 2022.¹⁵

Meski jaringan 5G masih belum masuk ke Indonesia, di tahun 2020 sudah ada empat jenis ponsel pintar yang mendukung teknologi 5G beredar secara resmi di Indonesia. Semuanya merupakan ponsel asal China yaitu OPPO Find X2, OPPO Find X2 Pro, dan Huawei P40 Pro.¹⁶ Selain itu, tiga penyedia jaringan Internet di Indonesia yakni Telkomsel, XL Axiata dan Smartfren juga sudah melakukan ujicoba jaringan 5G ini.^{[17] [18]}

Melihat antusiasme Indonesia dalam menyambut jaringan 5G, penting untuk menggaris bawahi isu keamanan digital sebagaimana dituduhkan Amerika Serikat dan sekutunya. Meski belum ada bukti eksplisit dari tuduhan tersebut, setidaknya haruslah ada kewaspadaan dalam mengimplementasikan jaringan 5G ini di tanah air. Pemerintah Indonesia harus memastikan benar tidaknya isu ini serta menyusun langkah preventif jika tuduhan AS akan jaringan 5G ini benar adanya.

“

Terdapat spekulasi di ranah global bahwa produk digital asal China disebut memiliki kelemahan dari segi keamanan berdasarkan asumsi bahwa produk China diduga selalu berada di bawah bayang-bayang pemerintahan China, sehingga ia bisa dijadikan alat untuk spionase.

”

¹¹ <https://www.thejakartapost.com/adv-longform/2019/08/27/huawei-helps-create-win-win-digital-ecosystem-in-ri.html>

¹² <https://www.thejakartapost.com/news/2020/02/28/huawei-aims-to-have-73-local-indonesian-apps-in-appgallery-by-march.html>

¹³ <https://tekno.kompas.com/read/2019/10/29/15460047/bssn-dan-huawei-kerja-sama-kembangkan-sdm-untuk-keamanan-siber>

¹⁴ <https://www.cnnindonesia.com/teknologi/20191029154752-185-443825/gandeng-huawei-bssn-sebut-tak-perlu-khawatir-isu-spionase>

¹⁵ <https://katadata.co.id/berita/2020/03/09/indonesia-dianggap-siap-adopsi-5g-tahun-depan#:~:text=Mereka%20pun%20memperkirakan%2C%20nilai%20bisnis,1%2C83%20juta%20pada%202025.>

¹⁶ <https://www.suara.com/tekno/2020/05/14/155348/daftar-ponsel-5g-ini-sudah-masuk-pasar-indonesia?page=1>

¹⁷ <https://inet.detik.com/telecommunication/d-4802327/telkomsel-sukses-uji-coba-5g-di-batam>

¹⁸ <https://teknologi.bisnis.com/read/20190822/101/1139774/uji-coba-5g-smartfren-lebih-cepat-xl-axiata-lebih-menarik>



Hak untuk Berekspres

Pemidanaan Jurnalis dan Aktivist Tetap Tinggi

Pemidanaan terhadap hak kebebasan berekspres dengan menggunakan pasal-pasal karet di UU ITE masih terjadi sepanjang 2019, yang bertepatan dengan tahun politik. Data yang masuk ke SAFEnet, terjadi 24 kasus pemidanaan dengan UU ITE, menurun dibandingkan tahun 2018 yang mencapai 25 kasus.

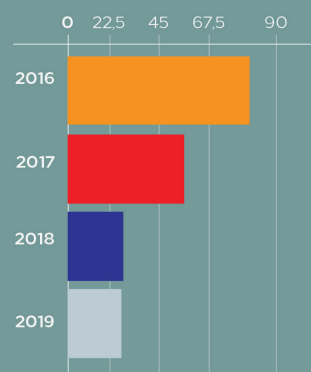
Berdasarkan profesi yang diadukan, media dan jurnalis masih menempati posisi pertama dengan 8 kasus, terdiri atas 1 media dan 7 jurnalis menjadi korban. Dalam dua tahun terakhir, jumlah media dan jurnalis yang dipidanakan cenderung lebih tinggi dibandingkan tahun-tahun sebelumnya.

Di posisi kedua, pemidanaan hak berekspres menimpa aktivis dan warga masing-masing sebanyak 5 kasus. Jumlah pemidanaan terhadap aktivis meningkat dari sebelumnya yang hanya 1 kasus.

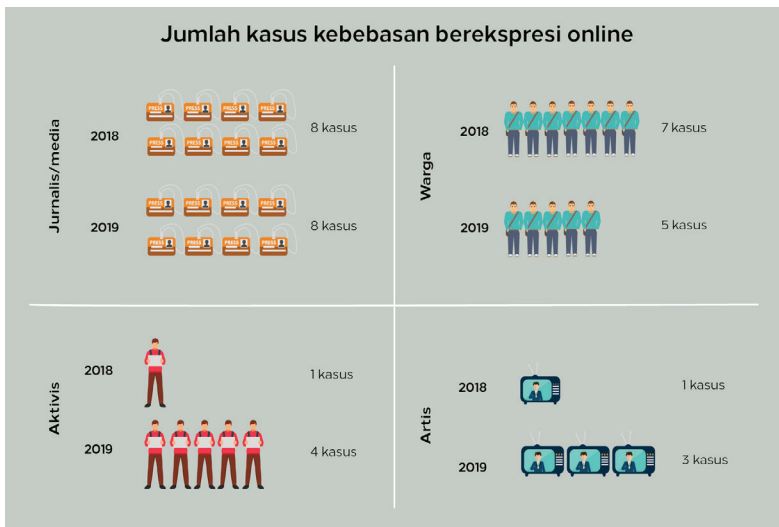
Posisi berikutnya adalah tenaga pendidik dan artis masing-masing 3 kasus.

Dari aspek pasal pemidanaan, Pasal 27 ayat 3 UU ITE (defamasi) paling banyak digunakan yakni sebanyak 10 kasus. Disusul Pasal 28 ayat 2 (kebencian) sebanyak 8 kasus. Penggunaan dua pasal sekaligus juga muncul yaitu, Pasal 27 ayat 1 (pornografi) dengan Pasal 27 ayat 3 sebanyak 3 kasus. Terakhir, penggunaan Pasal 27 ayat 1 dengan Pasal 28 ayat 2 terdapat 1 kasus.

Jumlah kasus kebebasan berekspres online



Sumber: Dokumentasi SAFEnet



Jumlah kasus yang dihimpun SAFEnet memang jauh dari angka kasus UU ITE yang direkap Polri. Data dari Direktorat Tindak pidana Siber Mabes Polri, menunjukkan bahwa jumlah penyelidikan terhadap akun media sosial selalu naik setiap tahun, yakni 1.338 kasus pada 2017, 2.552 kasus pada 2018, dan melonjak pada 2019 menjadi 3.005 kasus.

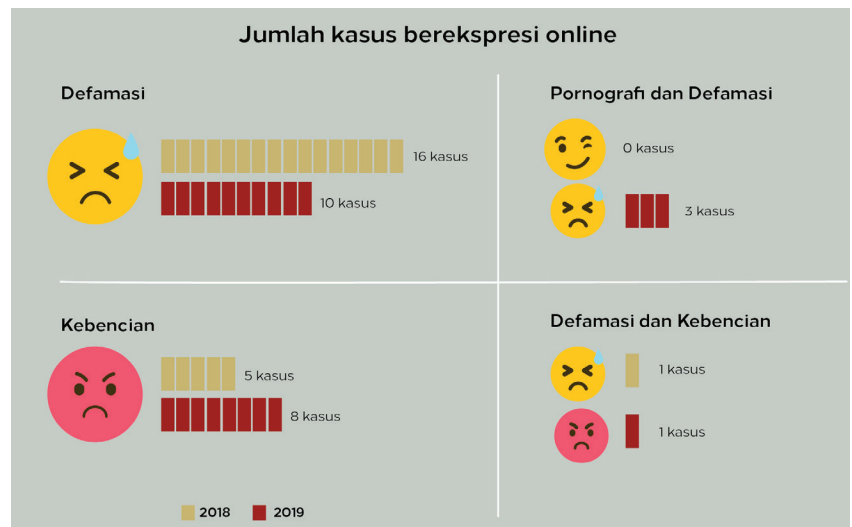
Dari jumlah itu, kasus terbanyak adalah penyelidikan menyangkut penghinaan tokoh, penguasa dan badan umum. Pada 2017 ada 679 kasus yang diselidiki terkait penghinaan, kemudian meningkat 1.177 pada 2018 dan turun pada 2019 menjadi 676 kasus. Kasus tinggi lainnya yakni mengenai dugaan provokasi dan ujaran kebencian. Tiga kasus ini kerap merujuk pada penggunaan pasal-pasal karet di UU ITE.

Pelaku Pidana

Pejabat publik dan politisi menempati posisi teratas sebagai pelaku pidana hak berekspresi daring dengan masing-masing 10 kasus. Jumlah pejabat publik seperti polisi dan aparat sipil negara sebagai pelaku memang turun dibandingkan tahun 2018 yang mencapai 11 kasus. Namun, tahun 2019 ditandai dengan banyaknya politisi sebagai pelaku pidana yang tidak dijumpai pada 2018. Selain kedua pihak itu, pelaku lainnya adalah artis (3 kasus), serta kalangan profesional seperti dosen dan dokter (2 kasus).

Dari sebaran wilayah, kasus pelanggaran kebebasan berekspresi daring yang dihimpun SAFEnet berada di 10 provinsi. DKI Jakarta menjadi provinsi dengan kasus tertinggi (10 kasus), lalu Sulawesi Tenggara (3 kasus), Aceh dan Jawa Timur (2 kasus), serta enam provinsi lain masing-masing 1 kasus.

Profil kasus pidana terhadap hak kebebasan berekspresi daring pada 2019 tidak jauh berbeda dengan tahun sebelumnya. Kasus dominan pada 2018 menimpa jurnalis dan media dengan 8 kasus. Kedua adalah masyarakat umum sebanyak 4 kasus. Aparat sipil berada di urutan ketiga dengan tiga korban. UU ITE juga menjerat tenaga pendidik (2 kasus) serta aktivis dan mahasiswa masing-masing satu kasus.



Adanya pidana sepanjang tahun 2019 tersebut menunjukkan hak kebebasan berekspresi daring di Indonesia belum terlindungi dengan baik. Pasal-pasal karet di UU ITE, terutama Pasal 27 ayat 1 dan 3 serta Pasal 28 ayat 2 masih terus dipakai untuk memberangus kebebasan berekspresi yang diperjuangkan sejak Reformasi 1998. Meskipun jaminan kebebasan berekspresi sebenarnya sudah tertera di Konstitusi dan UU Hak Asasi Manusia.

Tren peningkatan pemidanaan terhadap jurnalis dan aktivis sejak 2018 juga menjadi kekhawatiran tersendiri yang mengancam demokrasi. Munculnya aparat dan pejabat publik lain sebagai pelaku pemidanaan, menunjukkan bahwa UU ITE kian nyata telah disalahgunakan untuk membungkam suara-suara kritis terhadap kebijakan publik. Pemidanaan di ranah digital tersebut seiring dengan meningkatnya represi terhadap warga yang menyuarakan aspirasinya di tengah tahun politik dan sesudahnya.

Seperti diketahui bersama, pada 2019 berlangsung Pemilihan Legislatif (DPRD Kabupaten/Kota, DPRD Provinsi, DPR RI, dan DPD) serta Pemilihan Presiden secara serentak di seluruh kabupaten/kota. Dua kandidat yang bersaing sejak 2014, Joko Widodo dan Prabowo Subianto kembali *vis-a-vis* memperebutkan 190 juta suara warga.

Polarisasi akibat keterbelahan publik yang hanya mendukung dua kandidat sejak 2014, kembali menguat pada 2018 dan memuncak pada 2019. Polarisasi di akar rumput itu di antaranya dipengaruhi adanya pertarungan narasi politik identitas secara digital oleh dua kubu dengan memainkan sentimen agama dan rasial.

Usai kerusuhan Mei 2019, demonstrasi masyarakat sipil secara besar-besaran terjadi di Jakarta, Yogyakarta, Palembang, Makassar, dan daerah lain pada 24-26 September 2019. Mereka menolak revisi Undang-Undang Komisi Pemberantasan Korupsi (revisi UU KPK) dan Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP). Protes juga disuarakan terhadap RUU Pertanahan dan RUU Pemasaryakatan. Sejumlah RUU tersebut dianggap mengingkari amanat reformasi.¹ Polisi merespon aksi-aksi tersebut dengan represi termasuk menyebabkan 3 orang meninggal di Jakarta dan 2 mahasiswa Kendari tewas ditembak.²

Teror Negara

Situasi politik yang sangat dinamis terkait pemilu, gerakan antikorupsi, dan aksi menentang rasisme itu turut mempengaruhi kondisi pemenuhan hak-hak digital di Indonesia selama 2019 dan, menurut proyeksi kami, akan tetap berpengaruh hingga tahun-tahun selanjutnya. Menjelang pengujung 2020, SAFEnet menerbitkan proyeksi bahwa situasi kemerdekaan berekspresi di Indonesia pada 2019-2024 berada di status siaga satu. Proyeksi ini salah satunya berdasarkan meningkatnya kriminalisasi aktivis pro demokrasi dan jurnalis pada 2018-2019.

Hal ini menunjukkan bahwa Reformasi 1998 tidak cukup membawa angin perubahan dan perlindungan terhadap kerja-kerja pers di Indonesia. Meskipun terdapat UU Pers, tetapi kelemahan perlindungan pers masih terlihat dari banyaknya kekerasan terhadap jurnalis baik itu secara fisik atau non fisik. Selain kekerasan fisik, tindakan-tindakan seperti kriminalisasi jurnalis dengan UU ITE, doksing kepada jurnalis, mobilisasi untuk menghancurkan kredibilitas media dengan perundungan daring (*online harrashment*) di media sosial hingga penghancuran reputasi lewat pemberian bintang satu dan review buruk sehingga apps dihapuskan dari Google Playstore.

Penangkapan sejumlah aktivis yang melakukan kombinasi tindakan dan kampanye di media sosial atas sejumlah isu publik justru semakin banyak dan terang-terangan dilakukan, sekalipun bukti-bukti yang ada tidak memenuhi unsur hukum. Teror negara dimunculkan dengan sejumlah penangkapan ini, seperti apa yang terjadi pada aktivis Ananda Badudu dan sutradara film dokumenter Dandhy Laksono. Keduanya ditangkap meski belum dimintai keterangan polisi terkait kasus yang dituduhkan.

Labelisasi hoaks pada informasi yang diunggah aktivis juga menjadi pola baru sebelum kriminalisasi terjadi. Labelisasi terhadap unggahan Twitter pengacara HAM Veronica Koman bahkan dilakukan oleh Kementerian Komunikasi dan Informatika dan Polri. Beberapa pekan kemudian, Veronica menjadi tersangka

1 <https://nasional.kompas.com/read/2019/09/24/15440851/ramai-ramai-turun-ke-jalan-apa-yang-dituntut-mahasiswa>
2 <https://www.bbc.com/indonesia/indonesia-50217875>

dugaan menyebarkan konten provokatif dan kabar bohong. Sedangkan tuduhan hoaks terhadap unggahan Dandhy Laksono dilakukan sejumlah pendengung (*buzzer*). Beberapa hari kemudian, Dandhy menjadi tersangka ujaran kebencian melalui proses penangkapan yang janggal.

Kedua kasus tersebut terkait erat dengan isu di Papua. Apa yang dialami Veronica Koman dan Dandhy Laksono, menunjukkan negara justru mensponsori represi kebebasan berekspresi melalui media daring terhadap kelompok prodemokrasi yang memperjuangkan keadilan untuk Papua.

Kriminalisasi Media dan Jurnalis

Represi melalui media digital juga tetap terjadi pada jurnalis sepanjang 2019. Padahal, Kebebasan pers di Indonesia sejatinya telah dijamin melalui UU No 40 Tahun 1999 tentang Pers. Untuk menghindari pemidanaan terhadap karya jurnalistik, Dewan Pers dan Polri juga telah menandatangani Nota Kesepahaman pada 2012. Secara garis besar, nota kesepahaman ini berisi agar sengketa pers diselesaikan oleh Dewan Pers.

Faktanya, pemidanaan terhadap jurnalis tetap terjadi dengan menyalahgunakan sejumlah pasal karet UU ITE, utamanya Pasal 27 ayat 3 (defamasi) dan Pasal 28 ayat 2.

Kasus pertama menimpa media Jawapos yang dilaporkan oleh Manajer Persebaya ke Polresta Surabaya pada 7 Januari 2019 atas berita berjudul "Green Force Pun Terseret". Berita tersebut sebenarnya merupakan hasil investigasi jurnalis Jawa Pos atas dugaan mafia bola saat Persebaya bertanding melawan Kalteng Putra pada 12 Oktober 2017. Jawa Pos dilaporkan dengan pasal 310-311 KUHP dan pasal 27 ayat 3 UU ITE karena dianggap melakukan fitnah dan mencemarkan nama baik. Padahal berita investigasi Jawa Pos adalah bagian dari fungsi pers dalam melakukan kontrol sosial yang dilindungi dalam Pasal 3 UU No. 40 Tahun 1999. Pemberitaan Jawa Pos telah berdasarkan kaidah jurnalistik dan dilakukan demi kepentingan publik, sehingga tidak bisa dipidana dengan pasal karet UU ITE dan KUHP.

Dua jurnalis di Kendari, Sulawesi Tenggara, menjadi korban berikutnya. Fadli Aksar (Detiksultra.com) dan Wiwid Abid Abadi (okesultra.com) dilaporkan oleh Andi Tendri Awaru, calon Anggota Legislatif Partai Amanat Nasional (PAN) Dapil Kendari-Kendari Barat, ke Polda Sultra pada 8 Januari 2019. Laporan itu terjadi setelah Fadli Aksar dan Wiwid Abid Abadi memuat berita terkait laporan warga terhadap Andi Tendri Awaru ke Polda Sultra terkait dugaan tindak pidana pemalsuan surat dan administrasi kependudukan. Setelah didemo oleh kelompok jurnalis setempat, Polda Sultra akhirnya mendorong kasus ini diselesaikan ke Dewan Pers.

Masih di Sulawesi Tenggara, wartawan Liputanpersada.com di Kabupaten Buton Tengah, Mohammad Sadli Saleh, dijebloskan ke penjara setelah menyoroti pembangunan jalan dari APBD setempat. Ia dilaporkan oleh Kepala Bagian Hukum Pemkab Buton Tengah, Akhmad Sabir dan Kadis Kominfo Buteng, La Ota dengan Pasal 27 ayat 3 UU ITE (defamasi), Pasal 28 ayat 2 UU ITE (kebencian).

Kepolisian Buton Tengah mengabaikan Nota Kesepahaman antara Polri-Dewan Pers dan tetap memproses kasus ini hingga ke pengadilan. Setali tiga uang dengan polisi, pada 26 Maret 2020, majelis hakim PN Pasarwajo memvonis Sadli 2 tahun penjara.

Selain terhadap karya jurnalistik, pemidanaan juga terjadi pada konten informasi yang disampaikan jurnalis di media sosial. Ini terjadi pada jurnalis dan sutradara film dokumenter Watchdoc, Dandhy Laksono pada 23 September 2019. Dandhy ditangkap di rumahnya setelah mengunggah dua foto dan beberapa artikel berita daring sebagai berikut:

"JAYAPURA (foto 1). Mahasiswa Papua yang eksodus dari kampus-kampus di Indonesia, buka posko di Uncen. Aparat angkut mereka dari kampus ke Expo Waena. Rusuh. Ada yang tewas."

"WAMENA (foto 2). Siswa SMA protes sikap rasis guru. Dihadapi aparat. Kota rusuh. Banyak yang luka tembak," lanjut keterangannya."

Dandhy dijerat Pasal 28 ayat (2) jo Pasal 45A (ayat 2) UU ITE tentang Pasal Kebencian. Namun, sebelum Dandhy ditangkap, informasi Dandhy Laksono itu diujungi banyak komentar dan melabelinya sebagai hoaks, meski informasi yang diunggah Dandhy berdasarkan pemberitaan sejumlah media kredibel.

Penangkapan Dandhy juga sewenang-wenang. Ia ditangkap di rumahnya di Bekasi, Jawa Timur lalu dibawa ke Polda Metro Jaya pada Kamis 26 September 2019. Penangkapan itu dilakukan pada jam istirahat, yakni pada pukul 23.00 WIB, tanpa didahului surat panggilan. Dandhy dilepas dengan status sebagai tersangka, setelah pemeriksaan panjang selama sekitar tujuh jam. Kejanggalan lainnya, Dandhy ditangkap berdasarkan laporan seorang anggota polisi.³

Kriminalisasi Aktivistis

Tidak hanya menjerat jurnalis, kasus pembungkaman kebebasan berekspresi juga dialami oleh para aktivis. Kasus pertama dialami Fransiskus Olarugi Lamanepa atau biasa disapa Frank Lamanepa, aktivis Koalisi Rakyat Bersatu Flores Timur (KRBF).

Ia ditetapkan menjadi tersangka oleh penyidik Polres Flores Timur (Flotim) setelah mengkritisi Sekda Flotim Paulus Igo Geroda yang saat itu rangkap jabatan sebagai Kepala Badan Penanggulangan Bencana Daerah (BPBD) Flotim. Tulisannya dalam bentuk polling di grup Facebook Suara Flotim itu dilaporkan ke Polres Flotim oleh Sekda Flotim pada 10 Juni 2019 lalu karena dituduh mencemarkan nama baik.

Frank tetap dinyatakan bersalah, setelah sidang Putusan Praperadilan Gugatan terhadap Pihak Polres Flotim ditolak Hakim. Sementara itu kasus kriminalisasi aktivis terkait dengan kebebasan berekspresi kedua menimpa pegiat, yang juga Mantan Aktivistis Indonesia Corruption Watch (ICW), Emerson Yuntho.

Ia dilaporkan oleh bekas Ketua DPR RI, Setya Novanto ke Polda Jawa Barat terkait komentarnya di Twitter. Dalam cuitannya, Emerson mempertanyakan keberadaan Setya Novanto yang saat itu tengah menjalani hukuman lapas Sukamiskin, Bandung, Jawa Barat. Emerson kemudian dilaporkan dengan Pasal 45 ayat (3) jo Pasal 27 ayat (3) UU RI No 19 Tahun 2016 tentang perubahan atas UU RI No 11 tahun 2006 tentang ITE.

Musisi sekaligus aktivis Ananda Badudu ditangkap karena menggalang dana melalui KitaBisa untuk aksi demonstrasi mahasiswa yang menentang RKUHP dan UU KPK di depan Gedung DPR/MPR pada Selasa 24-25 September 2019. Penangkapan terhadap Ananda Badudu hanya berlangsung satu hari setelah Dandhy Laksono dan dilakukan dengan sewenang-wenang pula. Kamar kos Ananda di kawasan Tebet Barat, Jakarta Selatan digedor saat ia tertidur. Ia kemudian dibawa ke Polda Metro Jaya pada Jumat 27 September 2019 sekitar pukul 04:25 WIB.

Kriminalisasi serupa juga terjadi pada aktivis yang vokal menyuarakan isu Papua. Setelah jurnalis Dandhy Laksono, pengacara hak asasi manusia untuk Papua, Veronica Koman ditetapkan sebagai tersangka oleh Kepala Kepolisian Daerah atau Polda Jawa Timur pada 4 September 2019. Tuduhannya, Veronica diduga telah memprovokasi dan menyebarkan berita palsu di media sosialnya.

Ada tiga konten cuitan Veronica yang dituding bernada provokatif dan hoaks terkait insiden rasisme di Asrama Mahasiswa Papua Surabaya, 16 Agustus 2019. Konten pertama, *Seruan mobilisasi aksi monyet turun ke jalan untuk besok di Jayapura* (18 Agustus 2019). Konten kedua, *momen polisi tembak ke dalam asrama Papua, total 23 tembakan termasuk gas air mata, anak-anak tidak makan selama 24 jam, haus, terkurung, disuruh keluar ke lautan massa*. Dan konten ketiga, 43 mahasiswa Papua ditangkap tanpa alasan yang jelas, 5 orang terluka dan 1 terkena tembakan gas air mata.

Veronica Koman dijerat dengan empat undang-undang sekaligus, yakni UU ITE, UU KUHP 160, UU Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana, dan UU 40 tahun 2008, tentang Penghapusan Diskriminasi

³ <https://tirto.id/kasus-dandhy-laksono-ananda-badudu-lampu-kuning-untuk-demokrasi-eiUl>

Data Kriminalisasi atas Hak untuk Bereksresi



Infografis: Data Kriminalisasi atas Hak untuk Bereksresi

Ras dan Etnis. Pada 20 September 2020, Veronica Koman ditetapkan sebagai status Daftar Pencarian Orang (DPO).

Labelisasi hoaks pada Veronica Koman dan Dandhy Laksono menjadi pola baru serangan siber pada kelompok kritis. Sebelum penetapan tersangka oleh Polda Jatim, Kementerian Komunikasi dan Informatika lebih dulu memberi label hoaks pada cuitan Veronica Koman dengan artikel tertanggal 19 Agustus 2019 berjudul [Hoaks] Polres Surabaya Menculik Dua Orang Pengantar Makanan untuk Mahasiswa Papua”.

Padahal, Veronica Koman sendiri tidak menulis kata “menculik” pada cuitannya di Twitter. Cuitan asli Veronica Koman berbunyi: “2 orang pengantar makan minum untuk penghuni asrama yang belum makan minum sejak siang barusan ditangkap polisi”. Belakangan setelah kritik terhadap labelisasi hoaks dengan manipulasi konten tersebut, Kominfo memberikan klarifikasi dan mencabut artikel itu.

Kriminalisasi Akademisi

Tahun 2019 juga menandai maraknya kriminalisasi terhadap akademisi, seperti yang terjadi pada dosen Unsyiah Kuala, Saiful Mahdi dan dosen Universitas Indonesia, Ade Armando.

Saiful Mahdi dilaporkan ke polisi oleh Dekan Fakultas Teknik Unsyiah Kuala Taufik Saidi dengan tuduhan pencemaran nama baik, setelah ia memberikan pernyataan dalam WhatsApp Group (WAG) UnsyiahKita dan WAG Pusat Riset dan Pengembangan mengenai kegagalan proses penerimaan Calon Pegawai Negeri Sipil (CPNS) di Fakultas Teknik pada Maret 2019.

Pada 30 Agustus 2019 Saiful Mahdi mendapatkan panggilan sebagai Tersangka dalam perkara dugaan tindak pidana Pencemaran Nama Baik dengan menggunakan sarana elektronik sebagaimana dimaksud dalam Pasal 27 ayat (3) UU ITE. Setelah menjalani sidang pertama 17 Desember 2019, Saiful Mahdi dijatuhi vonis 3 bulan penjara dan denda Rp 10.000.000

subsider 1 bulan penjara oleh Majelis Hakim Pengadilan Negeri Banda Aceh.












Adapun kriminalisasi terhadap Ade Armando terkait dengan isu politik. Ia dilaporkan oleh politisi DPD RI Fahira Idris terkait meme Gubernur DKI Jakarta Anies Baswedan berwajah joker dengan tulisan “Gubernur Jahat Berawal dari Menteri yang Dipecat” pada 31 Oktober 2020. Fahira melaporkan Ade menggunakan Pasal 32 ayat 1 UU ITE tentang larangan mengubah terhadap bentuk dokumen elektronik dan atau informasi elektronik.

Sebelum pelaporan itu, unggahan Ade Armando tersebut menjadi viral dan memicu perisakan. Di media sosial kemudian bergema tagar #tangkapAdeArmando dan sempat menjadi trending Twitter.

Meskipun demikian, data kasus yang masuk ke SAFEnet hanya puncak gunung es. Data sesungguhnya bisa puluhan kali lipat. Sebagai perbandingan adalah data dari Mabes Polri yang bisa diakses secara terbuka di situsweb Patroli Siber. Menurut situs tersebut, kasus terkait Internet sepanjang 2019 mencapai 4.586 kasus. Kasus terkait penyebaran konten provokatif merupakan kasus terbanyak, 1.769 kasus. Merujuk pada kasus-kasus yang ditangani SAFEnet selama ini, tuduhan provokatif seringkali sumir dan multitafsir.

Dari sisi platform, media yang paling banyak digunakan pelaku yang dituduh melakukan tindak pidana terkait Internet bisa dilihat pada tabel di sebelah:

Data lain yang bisa menjadi acuan adalah jumlah kasus terkait UU ITE sebagaimana tercatat di situsweb Mahkamah Agung (MA). Pencarian dengan kata kunci “UU ITE” yang terdaftar selama 2019 menghasilkan 212 kasus. Namun, kami menyadari bahwa perlu penelusuran lebih lanjut apakah semua kasus tersebut memang murni terkait pencemaran nama baik yang sifatnya multitafsir dan dilakukan sebagai bagian dari kritik atau tidak.

Instagram		534 kasus
WhatsApp		431 kasus
Facebook		304 kasus
Telepon/SMS		198 kasus
Twitter		80 kasus
Lainnya		70 kasus
Line		55 kasus
Blogpost		32 kasus
Marketplace		30 kasus
Email		20 kasus
Telegram		9 kasus



Komite Keselamatan Jurnalis

Pada 5 April 2019, SAFEnet bersama sembilan organisasi lainnya bergabung dalam Komite Keselamatan Jurnalis (KKJ), sebuah koalisi yang digagas masyarakat pers sebagai wujud kolaborasi untuk menangani kasus kekerasan terhadap pers dan jurnalis. Inisiatif ini juga muncul sebagai antisipasi dari tren meningkatnya tindak kekerasan terhadap jurnalis pada tahun politik.

Komite telah menyusun Standar Operasional Prosedur (SOP) yang akan menjadi pedoman dalam penanganan dan pencegahan kasus kekerasan jurnalis dan pekerja media agar tidak terulang kembali.

Pada koalisi ini, SAFEnet berperan untuk membantu kampanye serta ikut mengadvokasi kasus-kasus kriminalisasi

wartawan yang menggunakan pasal karet UU ITE. Selain itu, SAFEnet mengisi kekosongan advokasi pada kasus kriminalisasi jurnalis secara personal akibat pandangan dan pendapat pribadinya.

Kasus tersebut tidak bisa ditangani secara langsung oleh KKJ karena adanya SOP yang membatasi ruang advokasi hanya pada kasus yang berhubungan dengan kerja dan karya jurnalistik.

Selain mendampingi dan memberikan bantuan hukum, KKJ juga melakukan verifikasi kasus untuk setiap kasus kekerasan yang terjadi pada wartawan. Serta membuka layanan Hotline Antikekerasan Jurnalis untuk jurnalis yang mengalami kekerasan di nomor 0812-4882-231.





Hak Atas Rasa Aman

Saat ini tubuh-tubuh kasat mata menjelma menjadi entitas-entitas digital seperti nama pengguna, alamat IP, nomor telepon, alamat surel, foto, teks, video, dan berbagai informasi dan digital yang menjadi kekhasan di ruang-ruang digital. Tidak hanya terus bertambah jumlahnya, tubuh-tubuh rentan di dunia digital juga menghadapi berbagai ancaman yang difasilitasi media-media digital.

Sub-divisi Digital At-Risks (DARK) di bawah Divisi Hak atas Rasa Aman SAFEnet mencatat tubuh-tubuh rentan di dunia digital adalah yang beridentitas sebagai anak, perempuan, LGBTQ (lesbian, gay, biseksual, transgender, dan *queer*), jurnalis, aktivis (isu HAM, anti korupsi, lingkungan, kelompok agama minoritas, dan peniup peluit (*whistleblower*)). Selama 2019, DARK mencatat berbagai kekerasan berbasis gender siber (KBGS) yang sebelumnya kami sebut sebagai kekerasan berbasis gender online (KBGO) dengan temuan dalam penjabaran-penjabaran selanjutnya.

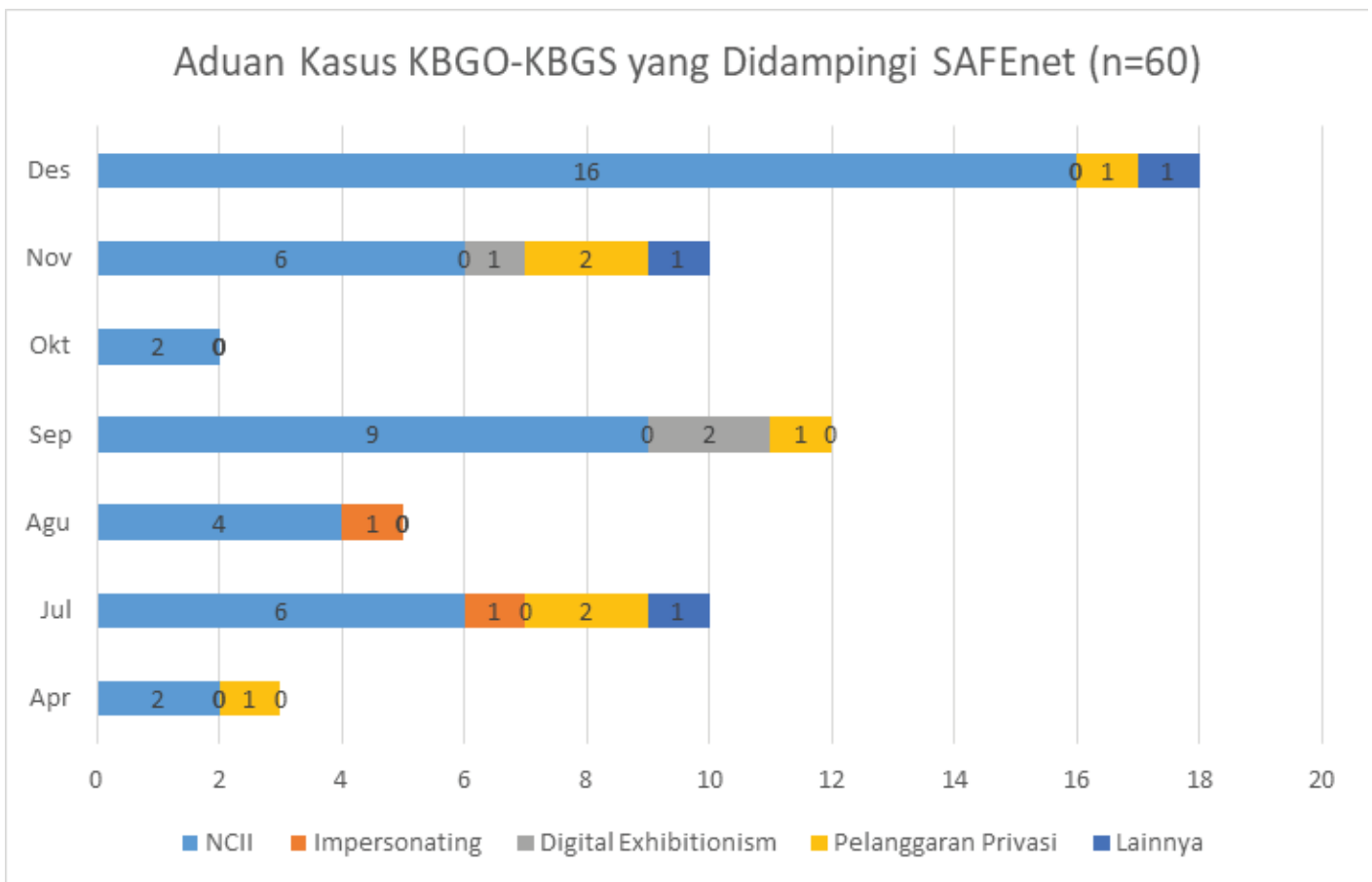
Penyebaran Konten Intim Merajalela

KBGS adalah tindakan yang membuat seseorang tidak aman atau merasa tidak

aman, menyerang atau berdampak lebih besar karena gender atau seksualitas seseorang, yang terjadi saat terhubung dengan Internet atau difasilitasi teknologi digital. Biasanya bentuk kekerasan ini berakar dari melanggar privasi dan/atau melakukan tindakan non konsensual pada satu atau banyak individu sekaligus.

Sepanjang 2019, SAFEnet menerima 60 aduan kasus KBGS. Sebanyak 44 aduan kasus adalah dari rujukan Komnas Perempuan pada SAFEnet, yang menjadi mitra resmi rujukan Komnas Perempuan sejak Juli 2019. Adapun 16 aduan lain masuk dari berbagai kanal komunikasi SAFEnet, termasuk dari yang diarahkan oleh mitra atau komunitas lain untuk membuat pengaduan di SAFEnet.

Dari jumlah tersebut, 53 korban yang mengadu adalah perempuan dan 7 lainnya tidak mengidentifikasi gendernya. Bentuk KBGS yang paling banyak dilaporkan adalah penyebaran konten intim tanpa persetujuan (*non consensual dissemination of intimate images (NCII)*) sebanyak 45 kasus, pelanggaran privasi (seperti doksing, pengawasan non konsensual, penyadapan, akses tanpa otorisasi) sebanyak 7 kasus, pembuatan akun peniru (*impersonation*) sebanyak 2 kasus, pamer alat kelamin di ruang digital secara non



Tabel 1 Aduan KBGO-KBGS berdasarkan Catatan SAFEnet

* Data 2012-2018 berdasarkan Laporan Tahunan SAFEnet 2018 "Jalan Terjal Memperjuangkan Hak-hak Digital"

konsensual (*digital exhibitionism*) sebanyak 3 kasus, dan bentuk KBGS lainnya seperti aksi memermalukan korban di ruang digital publik (*online shaming*) atau pelanggaran privasi korban di luar dari penjelasan di atas.

Angka ini tentunya belum mewakili angka kejadian KBGS secara keseluruhan di Indonesia. Catatan Tahunan Komnas Perempuan 2020 berjudul *Kekerasan Meningkat: Kebijakan Penghapusan Kekerasan Seksual untuk Membangun Ruang Aman Bagi Perempuan dan Anak Perempuan* menyebutkan setidaknya ada 281 kasus di 2019, meningkat 300% dari 97 kasus di tahun sebelumnya. Bentuk ancaman penyebaran konten foto pornografi yang paling sering dilaporkan dan mencapai 91 kasus.

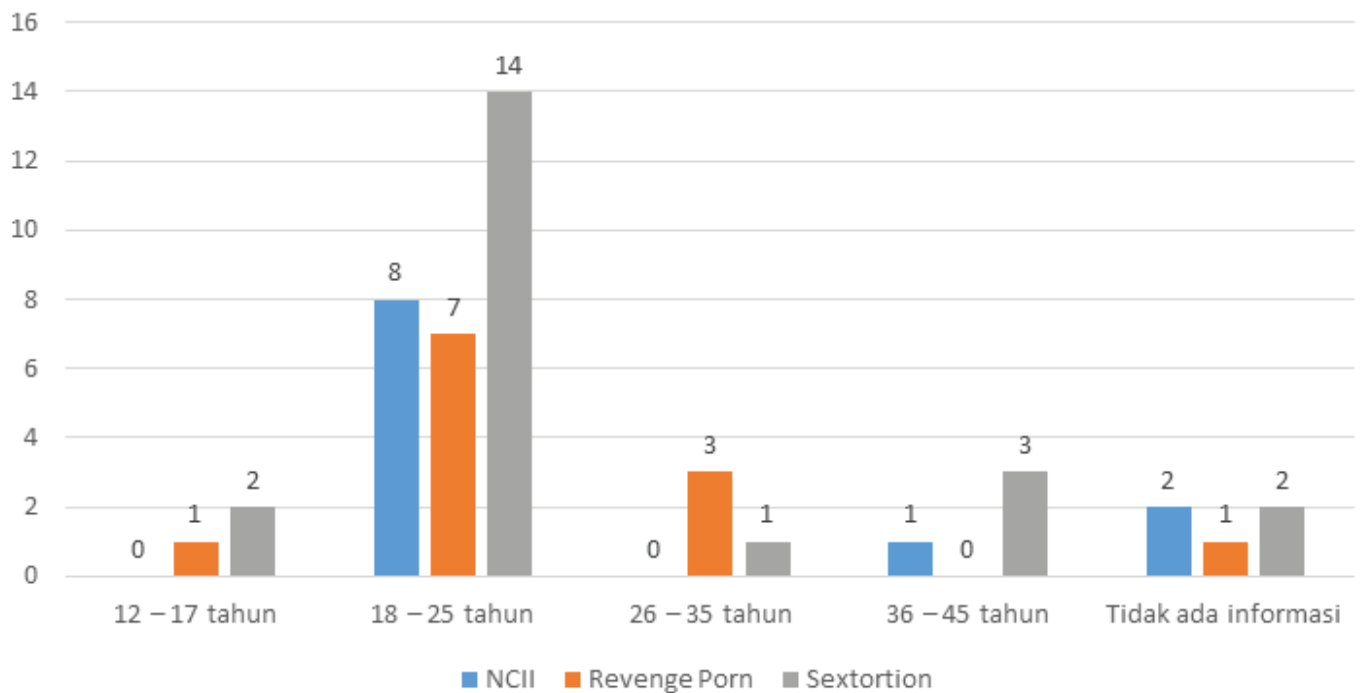
Dari 45 aduan kasus NCII, SAFEnet menemukan 22 kasus di antaranya adalah *sextortion*, atau ancaman penyebaran konten intim secara non-konsensual yang disertai pemerasan berupa permintaan uang atau

konten intim lagi. Ada pula 12 kasus *revenge porn* atau ancaman penyebaran konten intim oleh pasangan yang tidak mau putus atau berpisah ataupun mantan pasangan yang memaksa untuk berhubungan kembali. Selain itu, 11 kasus NCII lainnya tidak memiliki motif di atas atau pada saat diadakan dan selama konsultasi berlangsung motif tersebut belum terlihat.

Korban yang diancam atau sudah mengalami KBGS dalam bentuk penyebaran konten intim mayoritas berusia 18-25 tahun, terutama yang menghadapi *sextortion* sebanyak 14 orang. Hal ini bisa dipengaruhi beberapa hal, seperti bahwa usia 18-25 tahun termasuk rentang usia yang penetrasi penggunaannya Internet paling tinggi¹

¹ Laporan Survei Penetrasi dan Profil Perilaku Pengguna Internet Indonesia 2018 oleh Asosiasi Penyelenggara Internet Indonesia (APJII) yang diakses pada 18 Mei 2019 menyebutkan berdasarkan tingkat penetrasinya, rentang usia pengguna internet tertinggi pada 2018 adalah 15-19 tahun (91%), 20-24 tahun (88,5%), dan 25-29 tahun (82,7%).

Usia Korban yang Mengalami KBGO Bentuk NCII (n=45)



Tabel 2 Tabel Usia korban KBGS bentuk NCII yang didampingi SAFEnet selama 2019.

sehingga dapat mengakses bantuan atau melaporkan kasusnya ke lembaga bantuan, seperti Komnas Perempuan. Ada 36 dari total 44 aduan terkait NCII yang dirujuk dari Komnas Perempuan pada SAFEnet.

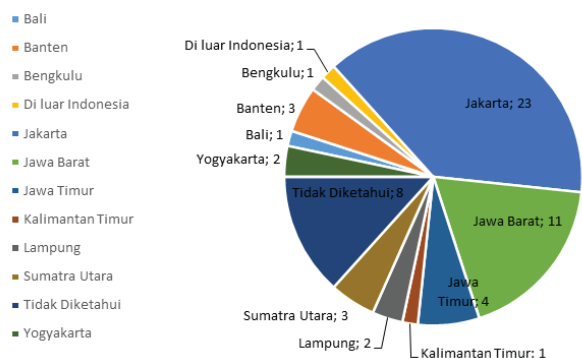
Terkait ancaman penyebaran konten intim, dua dari aduan yang masuk berdampak pada kerja korban sebagai aktivis, yang keduanya sengaja diserang ketubuhannya untuk mendelegitimasi aktivisme mereka. A² menghadapi KBGS dikarenakan pelaku memiliki motif personal dan sempat

memanipulasi korban untuk membangun relasi romantis tidak setara, sehingga ia mengalami NCII yang dikategorikan sebagai *revenge porn*. Konten intim A digunakan pelaku sebagai alat untuk mengintimidasi A dan juga diancam untuk disebarluaskan pada ruang-ruang kerja A untuk menghancurkan reputasi dan kredibilitasnya.

Beda dengan pengalaman A, B³ adalah aktivis yang mengalami KBGS bermotif politik. Pelakunya utamanya tidak diketahui, tetapi muncul sekumpulan akun yang tidak jelas identitasnya di media sosial, seperti Facebook, Twitter, dan Instagram yang bergerak seperti *buzzer* sengaja menyebarkan foto telanjang B yang dicuri dari ponsel korban yang diretas, lalu dimanipulasi dengan gubahan yang menunjukkan tubuh telanjang B disandingkan bersama mitra kerja, yang juga aktivis, dengan fitnah perselingkuhan untuk mendelegitimasi suara mereka sebagai aktivis yang sedang mengadvokasi isu revisi UU KPK saat itu.

Pengamatan SAFEnet selama menerima dan mendampingi aduan yang masuk juga menunjukkan beberapa hal, yaitu bahwa

Domisili Korban KBGO yang Didampingi SAFEnet (n=60)



2 Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

3 Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

kekerasan yang dialami korban bisa jadi tidak hanya satu bentuk seperti yang ditunjukkan oleh statistik di atas. Korban kerap kali mengalami beberapa bentuk KBGS sekaligus, seperti doksing atau penyebaran informasi data pribadi korban, seperti nama lengkap, nomor ponsel, atau akun pribadi korban, tanpa persetujuan ke dunia maya.

Aduan dari C⁴, misalnya, menyampaikan bahwa pelaku melakukan pengawasan pada dirinya dengan menggunakan teknologi digital berupa pemasangan aplikasi ponsel pintar yang memiliki fitur yang bisa mengetahui lokasi korban secara *real-time* di ponsel korban (*spyware*). Korban juga menghadapi upaya *phishing*⁵ dalam bentuk manipulasi tautan (*link manipulation*)⁶ oleh pelaku yang ingin meretas akun media sosial korban, tetapi upaya tersebut berhasil digagalkan.

Dalam kasus-kasus NCII, pelaku sering kali memanfaatkan situasi psikologis korban yang tidak ingin agar kekerasan yang dialaminya diketahui oleh orang lain, terutama orang-orang terdekat korban seperti orang tua dan keluarga. Pelaku mengintimidasi korban agar menuruti kehendak atau permintaan pelaku. Situasi psikologis korban juga terkadang dimanfaatkan pelaku untuk mendapatkan informasi pribadi korban, seperti yang dialami C. Kerentanan korban juga bertambah ketika KBGS yang dialaminya terkait dengan orientasi seksual LGB (lesbian, gay, dan biseksual) yang di Indonesia kerap kali sudah mendapatkan diskriminasi. Setidaknya ada dua kasus yang didampingi SAFEnet bersinggungan dengan orientasi seksual LGB.

SAFEnet juga menemukan bahwa kekerasan terjadi lintas dan multiplatform digital. Pelaku memanfaatkan berbagai teknologi digital untuk bisa berkomunikasi dengan korban, dari aplikasi kencan (*dating apps*), aplikasi percakapan (*chatting apps*), seperti WhatsApp, Line; aplikasi bersurat (*e-mail*); ataupun memanfaatkan fitur pesan langsung (*direct message*) di media sosial atau bahkan

aplikasi hiburan yang merangkap juga sebagai media sosial, seperti Hago.

Selama platform-platform digital tersebut memiliki fitur interaktif antar pengguna, maka dia sudah berpotensi menjadi ruang kekerasan digital.

Pemanfaatan berbagai teknologi komunikasi digital ini memungkinkan korban dan pelaku berada di lokasi berbeda dengan jarak jauh, seperti beda kota, beda provinsi, bahkan beda negara. Dalam catatan SAFEnet, ada 2 aduan KBGS dialami korban berstatus WNI yang saat kekerasan berlangsung sedang berada di luar negeri. Salah satunya dengan pelaku berada di Indonesia, dan yang lainnya dengan pelaku yang mengaku WNA dan membujuk korban untuk pergi ke luar negeri menemuinya.

Beragamnya situasi yang dihadapi korban dan kebutuhannya, membuat langkah dan tindakan yang diambil tidak berdasarkan solusi tunggal tetapi hasil pemetaan risiko. Selama proses pendampingan dan konsultasi bersama korban dan penyintas KBGS, SAFEnet mengambil tindakan berupa salah satu atau kombinasi dari memberikan saran terkait keamanan digital (58%), hanya mencatat kasus karena komunikasi tidak berlanjut (35%), membantu meningkatkan keamanan digital korban (30%), membantu proses pelaporan ke platform digital (17%), menghubungkan dengan LBH (13%) dan lembaga pendamping lain (17%), menghubungi pelaku untuk mengupayakan mediasi (5%), membantu proses pelaporan ke polisi (3%), dan memberikan saran terkait hukum (3%).

Saat mendampingi aduan kasus KBGS sepanjang 2019, SAFEnet juga melakukan konsultasi tatap muka langsung dengan korban (23%). Meskipun demikian mayoritas pendampingan dilakukan secara daring karena domisili korban ada di berbagai tempat.

Tidak semua aduan yang tercatat berujung pada pelaporan ke polisi, karena korban memilih untuk tidak sampai pada hal tersebut. Alasan-alasan yang dikemukakan termasuk tidak ingin ketahuan orang tua, proses yang panjang, ketakutan atas *victim blaming* atau dikriminalisasi dengan UU ITE, biaya, dan lain-lain. Dari kasus yang turut didampingi SAFEnet sampai di tahap pelaporan ke polisi dilakukan dengan berkoordinasi bersama lembaga bantuan hukum, seperti LBH APIK Jakarta, LBH Jakarta, dan LBH Bandung.

4 Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

5 Phishing adalah bentuk kejahatan siber ketika pelaku dengan sengaja berpura-pura menjadi atau membuat suatu identitas legal atau terpercaya untuk memancing agar korban memberikan informasi data pribadinya, yang biasanya akan digunakan untuk mendukung tindak kejahatan siber lainnya pada korban, misalnya peretasan, pengambilalihan akun, dan seterusnya.

6 Link manipulation adalah tindakan phishing dengan metode mengirimkan tautan (link) yang tampilan situs webnya dibuat sedemikian rupa mirip dengan situs web yang familiar bagi korban, biasa disertai formulir atau kolom untuk memasukkan data-data pribadi, seperti nama, kata kunci, dan lainnya.

Mesin dan Algoritma Juga Menjadi Pelaku

Salah satu aduan kasus menarik yang didampingi SAFENet adalah pelanggaran privasi yang tidak disengaja karena sistem yang tidak memahami perspektif dan dampak pada korban. Pada kasus yang dihadapi D⁷, ia mengalami KBGS karena namanya sebagai korban kekerasan seksual tidak disamarkan dalam putusan pengadilan dan muncul dalam hasil pencarian nama di Google. Dampaknya ia mengalami stigma yang kerap dialami korban kekerasan seksual.

Kasus ini menunjukkan karakteristik KBGS yang tidak selalu terkait dengan kekerasan seksual secara langsung, tetapi pada jejak digital yang menjadi dampak setelahnya. Dalam hal ini berupa putusan pengadilan yang tidak menyamarkan nama D, dan lalu diunggah di situs web Mahkamah Agung dalam format digital (pdf) dan muncul di mesin pencarian Google saat dicari dengan kata kunci berupa nama korban.

Kasus ini juga menunjukkan bahwa walaupun hampir semua kasus KBGS senantiasa terjadi di platform digital yang menyediakan fitur interaktif langsung dan dua arah antar-pengguna platform. KBGS tetap bisa terjadi bahkan ketika platform digital tersebut tidak memungkinkan adanya interaksi langsung antar pengguna, seperti mesin pencari Google. Hal ini karena yang terjadi adalah interaksi antara pengguna dan algoritma. Pelaku bisa jadi tidak melulu manusia, tetapi secara insidental berwujud teknologi digital berupa sistem algoritma mesin pencarian dan situs web sebuah institusi.

Dalam hal ini, patut disesalkan kelalaian dari pengadilan yang membuat berkas putusan pengadilan yang mengabaikan Surat Keputusan Mahkamah Agung Nomor 1-144/KMA/SK/I/2011 tentang Pedoman Pelayanan Informasi Pengadilan. Dalam SK tersebut pada Poin VI tentang Prosedur Pengaburan Sebagian Informasi Tertentu dalam Informasi yang Wajib Diumumkan dan Informasi yang Dapat Diakses Publik disebutkan untuk Petugas Informasi wajib mengaburkan nomor perkara dan identitas saksi korban dalam beberapa perkara, termasuk tindak pidana kesusilaan.

Di sisi lain, hal ini menjadi bagian kekerasan berbasis gender sendiri dikarenakan stigma di tengah masyarakat yang menghakimi

korban kekerasan seksual, sehingga dampak dari kejadian ini membuat kekerasan dan trauma baru pada korban, selain mengulang trauma lama.

Hal menarik lain dari kasus ini adalah singgungannya dengan UU ITE No. 19/2016 Pasal 26 Ayat 3 terkait hak untuk dilupakan (*right to be forgotten*) dan Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) Pasal 15 Ayat 2 terkait dengan penghapusan (*right to erasure*) dan pengeluaran dari daftar mesin pencari (*right to delisting*).

Upaya menempuh jalur hukum untuk kasus ini belum memanfaatkan peraturan-peraturan di atas berdasarkan keputusan korban. Namun, akan menarik untuk memperhatikan pasal-pasal tersebut digunakan untuk menjawab kebutuhan korban KBGS, yang kerap kali mengalami kekerasan berulang karena konten-konten yang menjadi jejak digital dari kekerasan yang dialami korban masih beredar di ruang-ruang digital di berbagai platform, baik yang bersifat publik ataupun terbatas di dalam grup-grup, alih-alih menjadi peraturan yang dimanfaatkan untuk kepentingan yang merugikan publik seperti upaya menghapus jejak korupsi.

Keadilan Semu di Ranah Hukum Bagi Korban

Ketika dihadapkan dengan mencari keadilan hukum, keberadaan UU ITE Pasal 27 Ayat 1 terkait konten bermuatan melanggar kesusilaan dan UU Pornografi kerap mengkriminalisasi atau mengintimidasi korban-korban KBGS yang terkait dengan ancaman penyebaran konten intim atau seksual, sehingga banyak yang memilih tidak meneruskan ke ranah hukum. Alih-alih merasa terlindungi, para korban justru merasa takut tidak akan dilindungi. Selain itu proses hukum yang panjang dan menguras energi, serta kekhawatiran akan biaya, juga menjadi alasan korban tidak jadi melapor ke polisi.

Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan. – UU ITE Pasal 27 Ayat 1

⁷ Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

Salah satu kasus yang KBGS yang menunjukkan situasi darurat untuk penanganan kasus KBGS adalah kasus Baiq Nuril Maknun⁸ yang mendapatkan atensi besar dari publik sejak 2018, karena keadilan yang tidak kunjung didapatnya walaupun sudah menghadapi proses hukumnya sejak 17 Maret 2015. Atensi dan desakan publik ini memang kemudian membuahkan pemberian amnesti oleh Presiden RI Joko Widodo pada 29 Juli 2019 dan membebaskan Nuril dari ancaman pidana penjara selama 6 (enam) bulan dan denda Rp500 juta subsidi 3 bulan penjara.

Banyak hal ditunjukkan dari penyelesaian kasus Nuril, yaitu terutama kegagalan perangkat hukum dengan konteks dan perspektif yang dihadapi Nuril sebagai korban pelecehan seksual verbal oleh atasannya sendiri. Ini terlihat dari Mahkamah Agung yang mengeluarkan Putusan Mahkamah Agung Nomor 574/Pid.Sus/2018 di tingkat Kasasi dan menjatuhkan pidana padanya, dan lalu menolak juga Permohonan Peninjauan Kembali Nuril selaku Terpidana berdasarkan Putusan Mahkamah Agung Nomor 83 PK/Pid.Sus/2019 di tingkat Peninjauan Kembali pada 4 Juli 2019. Keputusan-keputusan ini disayangkan Komnas Perempuan karena tidak mengindahkan Peraturan Mahkamah Agung No. 3/2017 tentang Pedoman Mengadili Perkara Perempuan Berhadapan dengan Hukum.⁹

Mirisnya lagi, dalam upaya permohonan peninjauan kembali (PK) ke Mahkamah Agung yang mensyaratkan adanya bukti baru (*novum*), Nuril yang menggugat pelaku balik di Polda Nusa Tenggara Barat dengan KUHP Pasal 294 Ayat 2 butir 1 tentang Perbuatan Cabul Dalam Sebuah Relasi Kerja dengan nomor laporan: LP/334/XI/2018/NTB/SPKT harus menelan pil pahit. Lapornya dihentikan pada 28 Januari, karena dianggap tidak memiliki cukup bukti dan tidak ada kontak fisik yang terjadi. Membuktikan bahwa payung hukum di Indonesia masih belum bisa memberikan keadilan bagi korban-korban kekerasan seksual, apalagi yang tidak memiliki bukti adanya kontak fisik.

Selain Nuril, pada 2019 lalu ada dua kasus KBGS yang turut diadvokasi SAFEnet bersama berbagai mitra yang berbuah

putusan sidang, yaitu kasus E¹⁰ dan Kennedy Jennifer Dhillon¹¹. Dua kasus ini menunjukkan hal setali tiga uang dengan kasus Nuril, bahwa dibutuhkan upaya besar dan perjalanan panjang untuk menuntut keadilan atas KBGS yang dialami.

Proses hukum yang dialami E, serupa dengan apa yang dialami oleh Nuril dari segi waktu. Bila Nuril harus melalui proses hukum sekitar 4 tahun dan 4 bulan lamanya, E mengalaminya selama 5 tahun. Ia dilaporkan pada awal 2014, sempat mengalami masa tahanan selama 8 hari di akhir 2014, lalu diputus bersalah di Pengadilan Negeri Bandung. Ia sempat diputus bebas saat banding ke Pengadilan Tinggi, walau kemudian menghadapi putusan kasasi yang memutusnya bersalah. E akhirnya diputuskan bebas dalam putusan Peninjauan Kembali oleh Mahkamah Agung pada Januari 2019.

E adalah ibu rumah tangga yang terjerat kasus UU ITE atas laporan suaminya (sekarang mantan). Kasus ini bermula dari E yang mengalami Kekerasan Dalam Rumah Tangga (KDRT) oleh suaminya sejak 1994 dan baru berani melaporkannya ke polisi pada 2013. Laporan tersebut dibalas suaminya pada 2014 dengan laporan ke polisi dengan bukti percakapan di kotak masuk (*inbox*) Facebook milik E dengan temannya yang diduga telah melakukan perbuatan asusila dan melanggar UU ITE Pasal 27 Ayat 1.

Pada kasus ini, suami E melakukan pelanggaran privasi dengan mengakses akun Facebook E secara diam-diam untuk mengambil layar tangkap (*screenshot*) percakapan tersebut, mencetak, dan menggandakannya sebagai bukti pelaporan. Fakta persidangan menemukan hal tersebut tidak benar. Berdasarkan Berita Acara Hasil Pemeriksaan Forensik dari Bareskrim Polri Direktorat Tindak Pidana Ekonomi dan Khusus yang dihadirkan di persidangan pada awal Maret 2015, disebutkan bukti yang dicetak pelaku tidak ditemukan di dalam Facebook E, atau bukti yang disampaikan pelaku tidak menunjukkan adanya tindakan asusila seperti yang dituduhkan.

Selama 4 tahun 11 bulan proses hukum dilalui E untuk bisa bebas dari tuduhan tidak terbukti oleh pelaku KDRT yang diakomodasi dengan penggunaan pasal karet UU ITE Pasal 27 Ayat 1 dan penyajian alat bukti *screenshot*

⁸ Kami mendapatkan persetujuan dari Baiq Nuril Maknun untuk pencantuman namanya di dalam laporan ini.

⁹ Amalia, S. (2019, Juli 10). Komnas Perempuan: MA Seharusnya Pakai PERMA Perkara Perempuan untuk Baiq Nuril. Diakses dari Magdalene: <https://magdalene.co/story/kasus-baiq-nuril-seharusnya-didasarkan-perma> pada 16 Juni 2020

¹⁰ Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

¹¹ Kami mendapatkan persetujuan dari Kennedy Jennifer Dhillon untuk pencantuman namanya di dalam laporan ini.

percakapan yang sudah melanggar privasi E dengan pembobolan akun Facebook miliknya.

Kennedy punya cerita berbeda dari Nuril dan E. Sebagai korban KBGS, keadilan hukum memang hadir untuk kasusnya, tetapi bukan tanpa perjuangan yang keras dari dirinya selama proses tersebut berlangsung. Ada berbagai upaya yang dilakukan F untuk mencari keadilan atas KBGS yang dialami, yaitu penyebaran nomor ponsel pribadi dengan identitas palsu di berbagai aplikasi kencan online seperti BeeTalk, WeChat, Badoo, dan lainnya.

Nomor pribadi Kennedy dipasang di akun-akun platform digital tersebut sebagai akun yang menawarkan layanan pijat dan spa beserta layanan seks. Akun-akun tersebut tidak memuat nama asli atau lengkap, ataupun memuat foto diri Kennedy, melainkan foto seksi bukan Kennedy yang dicuri pelaku dari Facebook dan Google. Akibatnya Kennedy banyak menerima pesan teks dan panggilan video di WhatsApp dan ponselnya dari para laki-laki yang menghubunginya untuk menanyakan layanan yang disebut di dalam akun-akun digital tersebut.

Gangguan ini tidak hanya dialami Kennedy. Diketahui pelaku juga melakukan KBGS serupa pada setidaknya 4 korban lain dengan motif perbedaan pandangan politik terkait kandidat Pilkada Jakarta 2017.

“Saya berharap lembaga negara juga bisa meng-upgrade dirinya untuk lebih pintar lagi melihat case yang dilaporkan sehingga bukan lagi tugas saya sebagai korban untuk mencari pelaku, mencari bukti, dan mencari tanda-tanda siapa pelakunya.”

Seruan ini terlontar oleh Kennedy di konferensi pers “Kekerasan Berbasis Gender Online (KBGO): Memahami dan Melindungi Perempuan dan Kelompok Rentan”¹² yang diselenggarakan SAFEnet. Selama menjalani proses hukum, Kennedy harus berjuang untuk mendapatkan berbagai informasi untuk bisa dijadikan bukti dan mencari petunjuk tentang pelaku, yang semestinya adalah bagian dari tugas kepolisian dalam penyelidikan dan penyidikan. Kennedy yang berinisiatif untuk mengontak platform digital BeeTalk, WeChat, dan Badoo yang memuat akun-akun palsu yang menjajakan layanan pijat dan prostitusi yang dibuat oleh pelaku. Ia juga sempat mengirimkan e-mail

ke pihak Kominfo untuk melakukan tindakan pada aplikasi-aplikasi tersebut.

Kekukuhan Kennedy dalam mengawal kasusnya dan terus mengingatkan pihak kepolisian untuk bekerja secara profesional atas kasus yang dialaminya adalah bagian dari tantangan yang dihadapi korban KBGS selama mencari keadilan melalui proses hukum.

Di sisi lain, menarik untuk memperhatikan hasil putusan dari kasus Kennedy. Hakim melalui Putusan Sidang Nomor 281/Pid. Sus/2019/PN JktPst memutuskan pelaku bersalah atas dakwaan distribusi konten bermuatan melanggar kesusilaan sesuai dengan UU ITE Pasal 27 Ayat 1, dan Pasal 93 UU Administrasi Kependudukan terkait pemalsuan dokumen kependudukan kepada instansi pelaksana. Seperti yang diketahui, UU ITE Pasal 27 Ayat 1 adalah pasal yang menjerat Nuril dan E. Hal ini menunjukkan kekaretan dari pasal tersebut, terutama dari unsur bermuatan melanggar kesusilaan.

SAFEnet menyayangkan putusan Majelis Hakim tidak turut mempertimbangkan dakwaan dengan dasar UU ITE Pasal 32 Ayat 1 terkait informasi/dokumen elektronik milik orang atau publik yang diubah, ditambahkan, atau dikurangi. Pasal ini didorong LBH Jakarta, selaku kuasa hukum Kennedy, karena KBGS yang dialami Kennedy terjadi juga karena ada upaya penyebaran nomor ponsel F dengan mengubah informasinya dengan keterangan-keterangan yang tidak benar terkait kepemilikan nomor ponsel F.

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. - UU ITE Pasal 32 Ayat 1

Tantangan lain datang dari sisi aparat penegak hukum yang belum memiliki perspektif yang mendukung korban. Alih-alih seringkali aparat penegak hukum menyalahkan korban atas KBGS yang dihadapinya. Hal ini terjadi pada F¹³ yang didampingi SAFEnet dalam proses pelaporan ke polisi terkait KBGS dalam bentuk ancaman penyebaran konten intim dengan motif pemerasan (*sextortion*). Saat proses pembuatan Berita Acara Pemeriksaan, F mendapatkan dirinya

12 Siaran langsung konferensi pers ini dapat disaksikan di Youtube melalui tautan [s.id/YTliveGBVO](https://www.youtube.com/watch?v=sid/YTliveGBVO)

13 Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

ditanya dengan hal-hal yang mengarah pada *victim blaming* sehingga membuat korban trauma dan merasa terpuruk hingga terpikir untuk bunuh diri.

Di sisi lain, saat melakukan pendampingan, SAFEnet juga menemukan alasan-alasan, seperti “SDM terbatas” dan “tidak memiliki alat” untuk digital forensik atau pelacakan ke polisi sering dikemukakan bila didesak terkait pengusutan kasus. Alasan yang juga menjadi tantangan yang dikemukakan aparat penegak hukum adalah bahwa mereka susah untuk mendapatkan informasi tentang pelaku jika meminta ke platform digital, walaupun pihak platform digital sudah memiliki kebijakan khusus terkait dengan laporan aparat penegak hukum.

Kasus lain yang mendapat perhatian publik adalah terkait dua video dengan adegan seksual lebih dari dua orang yang dijual oleh sebuah akun Twitter. Video tersebut viral dengan tagar G¹⁴ di Twitter pada Agustus 2019. G, yang berusia 19 tahun saat itu, langsung ditahan oleh pihak penyidik hingga menjadi terdakwa dalam sidang tuntutan di Pengadilan Negeri Garut dengan Jaksa Penuntut Umum mengajukan UU Pornografi Pasal 8 Jo. Pasal 34 Jo. KUHP Pasal 55 Ayat 1 untuk menjerat G.

Setiap orang dilarang dengan sengaja atau atas persetujuan dirinya menjadi objek atau model yang mengandung muatan pornografi. – UU Pornografi Pasal 8

Dipidana sebagai pelaku tindak pidana: 1. mereka yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan. – KUHP Pasal 55 Ayat 1

Diketahui pada April 2020, G diputus¹⁵ bersalah karena memenuhi unsur “turut serta dengan sengaja menjadi obyek yang mengandung muatan pornografi” dalam putusan Pengadilan Negeri Garut Nomor 289/Pid.B/2019/PN.Grt. Padahal jika menelisik lebih dalam lagi atas kasus ini, G adalah korban eksploitasi seksual oleh pelaku yang merupakan mantan suaminya.

G mengalami kekerasan seksual dimulai dari paksaan untuk berhubungan badan dengan pria selain mantan suaminya, sengaja direkam, hingga video tersebut dijual melalui lewat Internet. Dalam produksi konten video yang dicap sebagai produk pornografi ini

sendiri pun G tidak memberikan konsen atau persetujuan yang utuh karena dia berada di bawah intimidasi mantan suaminya yang memiliki perilaku seksual menyimpang. Apalagi dalam proses distribusi konten video tersebut yang dimonetisasi oleh pelaku. Perlu dicatat juga bahwa perbedaan usia keduanya adalah 14 tahun, dan pelaku menikahi G sejak ia masih berusia 16 tahun, sehingga jelas dalam hubungan keduanya sudah terdapat ketimpangan relasi kuasa.

Putusan Pengadilan Negeri Garut ini menunjukkan lagi-lagi kerentanan perempuan korban kekerasan seksual ditambah dengan KBGS saat berhadapan dengan hukum, bahkan ketika sudah ada Perma No. 3/2017 tentang Pedoman Mengadili Perkara Perempuan Berhadapan dengan Hukum dan rekomendasi untuk penghentian jeratan hukum pada G oleh Komnas Perempuan.¹⁶

Proses hukum yang panjang juga tidak menjawab karakteristik dari “online” atau “difasilitasi teknologi digital” yang cepat dalam penyebaran dan multiplikasi konten. Ada kegagapan, ketidaktanggapan, dan ketidaksiapan aparat penegak hukum untuk menyelesaikan kasus-kasus KBGS, baik dari tahapan pelaporan sampai dengan persidangan. Prosedur hukum yang memakan banyak waktu juga membuat korban berpotensi mengalami kekerasan berulang, dengan jumlah pelaku yang bisa jadi bertambah. Pada KBGS yang bentuknya penyebaran konten intim, korban harus siap menghadapi risiko besar bahwa konten tersebut dapat diunggah berulang kali oleh pelaku utama, dan oleh pelaku lain yang menemukan konten tersebut dan memanfaatkannya untuk mengintimidasi korban lebih lanjut. Hal ini berdampak pada kondisi psikologis korban dan proses pemulihan korban.

Solusi yang Belum Berujung pada Keadilan

Dalam pendampingan aduan kasus KBGS SAFEnet juga membantu proses pelaporan ke platform digital dan menghadapi tantangan tersendiri. Dalam beberapa situasi didapati bahwa korban atau penyintas memiliki pemahaman yang minim atas

¹⁴ Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

¹⁵ Putusan sedang dalam proses banding di Pengadilan Tinggi Bandung pada saat laporan ini ditulis.

¹⁶ Iqbal, M. (2019, September 20). Berbekal Surat Komnas Perempuan, Pengacara Minta Polisi Hentikan Kasus ‘Vina Garut’. Diakses dari Merdeka pada 16 Juni 2020 <https://www.merdeka.com/peristiwa/berbekal-surat-komnas-perempuan-pengacara-minta-polisi-hentikan-kasus-vina-garut.html>

prosedur pelaporan ke platform digital yang sudah disediakan oleh platform digital tersebut, sehingga membutuhkan bantuan pelaporan.

Korban, penyintas, dan SAFEnet sebagai pendamping juga mengalami saat laporan ke platform digital mendapatkan hasil yang tidak memuaskan. Seringkali laporan ditolak karena fitur pelaporan di platform digitalnya tidak tanggap dengan kejadian yang dialami korban, sehingga laporannya tidak berbuah pada penghapusan konten yang diunggah pelaku KBGS atau akun yang dibuat oleh pelaku. Alih-alih dihapus, alasan yang kerap disampaikan saat laporan ditolak adalah platform digital menemukan bahwa konten tersebut tidak melanggar panduan standar komunitas (*standard community guideline*) atau ketentuan penggunaan platform digital.

Di sisi lain, para penyedia platform digital, seperti raksasa media sosial Facebook, Instagram, Google, Twitter, memiliki sistem atau fitur yang memfasilitasi pelaku untuk bisa dengan mudah menyebarkan konten ataupun membuat belasan sampai puluhan akun palsu baru, sehingga saat korban menunggu platform digital menanggapi laporannya, ia masih rentan untuk diserang dengan unggahan konten atau akun-akun baru yang dibuat pelaku.

Fitur lain yang menyumbang kerentanan pada korban karena dapat menduplikasi konten adalah API (*application programming interface*) publik yang disediakan beberapa platform digital, seperti Instagram dan Twitter, sehingga data yang diunggah ke platform digital ini bisa dimungkinkan untuk diduplikasi pihak ketiga secara otomatis.

Terkait dengan pemanfaatan API publik yang menyumbang kerentanan pada korban KBGS ini terjadi saat SAFEnet mendampingi aduan kasus B yang menghadapi konten-konten intim dirinya muncul di hasil mesin pencarian Google dalam bentuk gambar-gambar yang terduplikasi dari postingan-postingan publik di Instagram dan Twitter ke situs web <http://pictame.biz/>, <http://saveig.org/>, dan <http://terasocial.com/>¹⁷. Ketiganya berfungsi serupa seperti ImglInn yang menjadi contoh di atas.

Dalam penanganan untuk menghapus konten ini pun bukan perihal yang mudah, bahkan setelah berkoordinasi dengan platform digital yang menerbitkan API

publik tersebut, karena terhubung dengan pihak ketiga yang menggunakan API tersebut, juga pelaporan ke Google yang memunculkan konten-konten tersebut dalam hasil pencariannya.

Penanganan pelaporan konten digital ini tidak hanya kusut di hal-hal seperti di atas, tetapi juga dalam kasus yang dihadapi Kennedy. Ia hanya berhasil mengontak satu platform digital, yaitu BeeTalk, karena memiliki kantor di Indonesia, sedang WeChat dan Badoo tidak dapat dihubungi karena tidak memiliki kantor perwakilan di Indonesia.

Monetisasi dan Normalisasi KBGS dalam Media Massa!

Berbicara tentang KBGS juga perlu membahas peran media massa online. Media massa berperan penting dalam membangun realitas sosial, mengedukasi publik, dan juga mendorong kebijakan publik. Sayangnya, SAFEnet melalui pengamatan dari 22 unggahan bertagor #WTFMedia oleh akun Instagram @magdaleneid¹⁸ selama 2019 menemukan bahwa media massa online kerap melakukan objektifikasi pada tubuh perempuan dan melanggengkan normalisasi KBGS dengan berita-berita berjudul penuh sensasi sebagai pancingan klik (*click-bait*) yang berorientasi monetisasi. Judul-judul seperti ini kerap kali tidak berperspektif ataupun sensitif dengan isu atau kelompok yang memiliki kerentanan terkait gender, seksualitas, dan kekerasan yang dialami.

Di sisi lain, pemberitaan penuh sensasi dan minim empati berpotensi menjadi KBGS baru, seperti ketika abai memperhatikan kerentanan dan privasi korban, misalnya saat mengunggah data pribadi seperti nama dan lokasi. Contohnya berbentuk *deadnaming*, atau menyebarkan kepada publik nama asli dari seorang transgender tanpa persetujuannya. Dampaknya bisa panjang terutama mengingat kerentanan transgender di Indonesia sebagai kelompok minoritas yang sering didiskriminasi.

Pelanggaran privasi dan aktivitas non-konsensual terkait data pribadi, gender, dan seksualitas seseorang adalah akar kekerasan berbasis gender. Dengan Internet dan/atau difasilitasi teknologi digital yang memiliki karakteristik tertentu, seperti cepat menyebar, konten dengan mudah diduplikasi

17 Tiga situs web tersebut sudah tidak dapat diakses lagi saat penulisan laporan ini.

18 Akun ini dikelola Magdalene, media masa online dengan klaim "Indonesian Feminist Webmagazine"

dan diproduksi, serta jejaknya yang abadi, kekerasan berbasis gender memiliki dampak-dampak yang tidak terpicirkan sebelumnya. Media massa online harusnya tidak menjadi pihak atau pelaku yang berkontribusi menambahkan kerentanan dan risiko terjadinya KBGS.

Perempuan dan Tubuh Digital yang Harus Kompromi

Berbicara tentang gender dan seksualitas, Indonesia masih menganut kuat kultur dan pola pandang patriarki, sehingga kerap kali tubuh perempuan atau non-binari yang diliyankan menjadi sasaran yang diatur oleh para penganut kultur ini. Demikian ketika, kultur dan pola pandang ini terbawa dalam perilaku di dunia digital, maka tubuh-tubuh liyan di dunia digital ini juga diatur dengan alasan yang sama. Melihat hal itu, tidak mengagetkan ketika mayoritas korban KBGS adalah perempuan dan tubuh-tubuh yang mengidentifikasi diri dengan identitas liyan, seperti non-binari.

Tidak heran pula mendengar saat muncul pernyataan dari pihak Kementerian Komunikasi dan Informatika (Kominfo) pada Juli 2019 yang menyampaikan bahwa mereka meminta platform digital Google (Alphabet) yang menaungi YouTube untuk memblokir tiga konten milik *Youtuber* dan *Gamer H*¹⁹ dengan alasan bahwa konten YouTube milik H diduga melanggar unsur kesusilaan yang tertuang dalam UU ITE Pasal 27 Ayat 1.

Awal mulanya adalah adanya laporan aduan dari masyarakat terkait konten yang diproduksi H dan diunggah ke kanal YouTube miliknya. Diketahui juga, bahwa konten milik H turut dilaporkan melalui permintaan resmi dari Ketua Komisi I DPR RI Abdul Kharis Almayahri dalam Rapat Dengar Pendapat yang berlangsung pada 18 Juli 2019. Melalui investigasi mandiri oleh Tim AIS Kominfo ditemukan 9 konten yang diduga bermuatan melanggar kesusilaan. YouTube diminta untuk melakukan pemblokiran pada 3 konten dan mengaktifkan fitur pembatasan untuk penonton berusia 18 tahun ke bawah untuk 6 video lainnya, yang kemudian dilakukan oleh platform digital tersebut.²⁰

19 Identitas sengaja disamarkan. Kasus dijabarkan sebagai bentuk edukasi beragamnya pengalaman KBGS yang dialami korban.

20 Laporan ini dapat diakses melalui tautan https://transparencyreport.google.com/government-removals/by-country/ID?country_request_amount=groupby:requestors;period:Y2019H1;authority:ID&lu=country_request_explore&country_item_amount=groupby:totals;period::authority:ID&country_request

Indonesia

Request

We received a request from the Ministry of Communication and Information Technology to remove 9 YouTube videos from a popular Indonesian YouTube creator for containing allegedly sexually provocative gaming content.

Outcome

We restricted access to 3 of the videos from YouTube in Indonesia and age-restricted the remaining 6 videos from view by users under the age of 18.

Gambar 1 Laporan Transparansi Google periode Juli 2019 – Desember 2019

Kejadian yang termasuk KBGS menunjukkan lagi kekaretan dari UU ITE Pasal 27 Ayat 1 yang kali ini digunakan untuk merepresi ekspresi dan seksualitas perempuan di dunia digital. SAFEnet melihat kultur dan pola pandang patriarki disertai dengan “*male gaze*” dalam menginterpretasikan unsur kesusilaan ini yang terus menerus akan menyempitkan ruang ekspresi perempuan dan menjadikannya tubuh-tubuh digitalnya untuk terus kompromi, bila masih ingin menggunakan ruang-ruang digital, yang pula sebenarnya sudah tidak aman bagi perempuan. Dampaknya tidak hanya pada suara atau ruang ekspresi perempuan, tetapi dapat mempengaruhi faktor ekonomi perempuan, dalam hal ini H sebagai *content creator*.

PR Besar Kolaborasi Penanganan KBGS

Bercermin pada aduan kasus KBGS yang kian meningkat penting untuk berbagai pihak pemangku kepentingan untuk duduk bersama dan berkolaborasi dalam penanganan kasus KBGS. Teknologi digital ataupun Internet bukanlah satu-satunya faktor yang berkontribusi pada KBGS. Banyak konteks dari berbagai perspektif yang membuat kekerasan ini terjadi, dan utamanya pada kekerasan berbasis gender adalah konteks struktur relasi kuasa dan patriarki yang mengakar yang berkontribusi besar menjadi penyebabnya.

Oleh karena itu, penanganan KBGS di Indonesia adalah pekerjaan rumah semua pemangku kepentingan yang terlibat dalam lingkup teknologi digital dan online itu sendiri, dari pengguna, penyedia platform digital, aparat penegak hukum, sampai para pembuat kebijakan.

Di tahun 2019, SAFEnet menginisiasi dan terlibat dalam beberapa *focus group discussion* (FGD) lintas sektor dan *multi-stakeholder*, baik dengan korban, LSM termasuk LBH dan lembaga konseling, institusi pemerintah (kementerian terkait seperti Komnas Perempuan, Kominfo, KPPPA, CCIC Polri), platform digital (media sosial seperti Google, Facebook, dan Twitter; aplikasi transportasi seperti Grab dan Go-Jek) terkait penanganan KBGS di Indonesia.

Proses dan penegakan hukum adalah kunci utama yang harus direformasi dalam penanganan KBGS. Ia harus dikembangkan agar dapat menjawab berbagai tantangan yang dihadapi korban KBGS, seperti yang sudah diangkat dalam laporan ini. Sikap aparat penegak hukum yang tidak berperspektif korban dan bertendensi menyalahkan korban (*victim blaming*), pula terkadang gagap dengan teknologi digital dan modus-modus kekerasan siber, proses hukum yang panjang dan tidak menjawab karakteristik dari kekerasan online atau yang difasilitasi teknologi digital, pengamanan alat bukti, sampai pada evaluasi pasal-pasal karet yang berpotensi mengkriminalisasi korban alih-alih melindunginya di ranah hukum, seperti UU ITE Pasal 27 Ayat 1. Dibutuhkan Undang-Undang yang memiliki perspektif korban yang baik dan diimplementasikan dengan tegas sehingga dapat mengadvokasi korban-korban yang mengalami KBGS.

Platform digital juga harus meningkatkan tanggung jawab mereka dalam bentuk kebijakan-kebijakan, fitur dan tanggapan pelaporan, serta inovasi teknologi digital yang turut mengantisipasi berbagai bentuk KBGS. Banyak platform digital yang makin terintegrasi satu sama lain, konektivitas antar aplikasi ponsel makin tinggi, fitur berbagi konten lintas dan multi platform menjadi hal semakin mudah dan mulus untuk dilakukan, tetapi fitur pelaporan konten yang digawangi masing-masing platform digital masih mengalami kegagalan dan berdampak pada jejak-jejak digital yang menghantui korban KBGS. Platform digital dengan orientasi yang makin memudahkan berbagi konten dan data, juga harus menciptakan ruang yang ramah dan mudah diakses bagi pengguna dalam hal pengaturan keamanan dan privasi, serta fitur pelaporan yang lebih tanggap dengan kebutuhan korban.

SAFEnet juga merekomendasikan peningkatan kapasitas dan wawasan terkait keamanan digital untuk para pendamping korban, misalnya dengan pelatihan berupa

lokakarya atau pelatihan keamanan digital. Selain itu juga perlu ada edukasi pada warganet, misal dengan meningkatkan pemberitaan di media massa yang berperspektif gender dan seksualitas serta mendukung praktik-praktik pemberitaan yang mengusung privasi subjek yang diberitakan, atau dengan menambahkan kurikulum terkait KBGS untuk berbagai tingkatan sekolah, dari sekolah dasar sampai dengan perguruan tinggi. Hal ini juga akan membantu pemerataan akses informasi bantuan pendampingan untuk korban KBGS.

Catatan:

SAFEnet telah mendapatkan persetujuan untuk menjabarkan pengalaman KBGS yang dialami korban dan penyintas dengan identitas yang disamarkan menjadi A, B, C, D, E, dan F sebagai bentuk edukasi pada publik. SAFEnet juga telah mendapatkan persetujuan Baiq Nuril Maknun dan Kennedy Jennifer Dhillon untuk menuliskan namanya dalam laporan ini. Mereka adalah bagian dari korban dan penyintas yang sempat dan masih didampingi SAFEnet dalam advokasi kasusnya. Penjabaran kasus G dan H adalah berdasarkan pengamatan dari berita dan berbagai sumber lain.

Mengenal KBGO

Kekerasan Berbasis Gender Online

Sepanjang 2017, setidaknya ada 8 bentuk kekerasan berbasis gender *online* yang dilaporkan kepada Komnas Perempuan, yaitu pendekatan untuk memperdaya (*cyber grooming*), pelecehan daring (*cyber harassment*), peretasan (*hacking*), konten ilegal (*illegal content*), pelanggaran privasi (*infringement of privacy*), ancaman distribusi foto/video pribadi (*malicious distribution*), pencemaran nama baik (*online defamation*), dan rekrutmen daring (*online recruitment*).

~ Komnas Perempuan.

AKTIVITAS YANG DIANGGAP SEBAGAI BAGIAN DARI KBGO

- **Pelanggaran Privasi**, seperti: mengakses, menggunakan dan menyebarkan data pribadi seseorang tanpa persetujuan si pemilik data.
- **Pengawasan dan Pemantauan**, seperti: memantau, melacak dan mengawasi kegiatan seseorang baik *online* maupun *offline*.
- **Pengawasan dan Pemantauan**, seperti: memantau, melacak dan mengawasi kegiatan seseorang baik *online* maupun *offline*.
- **Perusakan Reputasi atau Kredibilitas**, seperti: membuat akun palsu dengan tujuan merusak reputasi orang lain.
- **Pelecehan (bisa berlanjut offline)**, seperti: pelecehan berulang-ulang, perhatian berlebihan dan kadang disertai ancaman seksual.
- **Ancaman Kekerasan Langsung**, seperti: perdagangan manusia memanfaatkan teknologi, pemerasan seksual atau pencurian identitas dan peniruan (impersonifikasi) yang menyebabkan serangan fisik.
- **Serangan Kepada Komunitas Tertentu**, seperti: meretas situs komunitas, memantau aktivitas secara berlebihan, ancaman kekerasan langsung, pengempungan, pelecehan dan pengungkapan identitas tanpa persetujuan.

YANG HARUS DILAKUKAN BILA MENJADI KORBAN KBGO

- **Dokumentasikan Hal-Hal yang Terjadi**, bila memungkinkan, dokumentasikan secara detail dan buat kronologisnya sebagai bahan pelaporan.
- **Pantau Situasi**, apakah memungkinkan menghadapi pelaku sendiri? Apakah memungkinkan mendokumentasikan sendiri?
- **Menghubungi Bantuan**, cari tahu individu atau lembaga yang bisa membantu. Misalnya, LBH APIK atau Komnas Perempuan.
- **Lapor dan Blokir Pelaku**, di ranah *online* kita bisa memblokir akun pelaku dan melaporkannya ke penyedia layanan.

“Kekerasan berbasis gender online mencakup spektrum perilaku, termasuk penguntitan, pengintimidasian, pelecehan seksual, pencemaran nama baik, ujaran kebencian dan eksploitasi. KBGO juga dapat masuk ke dunia offline, di mana korban atau penyintas mengalami kombinasi penyiksaan fisik, seksual, dan psikologis, baik secara online maupun langsung di dunia nyata saat offline.”

Internet Governance Forum

Lindungi data
privasi Anda!

grafis: @dgipul | daenggassing.com

KORBAN?

SIAPA YANG JADI

- **Seseorang yang terlibat dalam hubungan intim**, bisa menyebabkan konsekuensi ekstrem seperti depresi atau bahkan bunuh diri
- **Profesional (aktivis, penulis, jurnalis, dll)**, kebebasan berekspresinya dilanggar
- **Penyintas dan Korban Penyerangan Fisik**, keselamatannya terancam dan bisa menyebabkan konsekuensi ekstrem hingga bunuh diri.

Serangan Digital Menarget Kelompok Berisiko

Serangan digital mulai menjadi persoalan serius yang harus dihadapi aktivis, jurnalis, perempuan dan kelompok berisiko di Indonesia. Bentuk serangan digital yang telah terjadi bermacam-macam, mulai dari akun peniru (*impersonator*), mengumbar identitas (*doxing*), persekusi, menggunakan *hoax* sebagai senjata (*weaponization of social media*), peretasan, hingga penyadapan ilegal (*unlawful breach and illegal surveillance*). Aktor-aktor pelaku penyerangan digital bisa berasal dari *state hackers*, kelompok berbahaya, hingga individu sebagai pelaku teror. Biasanya serangan digital yang diarahkan kepada aktivis, jurnalis, perempuan dan kelompok rentan ini terjadi pada momentum peristiwa sosial dan politik yang terjadi di Indonesia.

Selama tahun 2019, SAFEnet mendapat sejumlah laporan serangan digital yang dialami oleh akademisi, aktivis anti-korupsi, dan aktivis mahasiswa yang terlibat dalam isu Revisi UU KPK dan #ReformasiDikorupsi.

Salah satunya terjadi di Yogyakarta. Sekitar minggu pertama September 2019, dosen UGM Profesor Rimawan Pradiptyo membuat gerakan konsolidasi dan untuk koordinasi lewat grup Whatsapp UGM Berintegritas untuk menghimpun sekitar 2.000 dosen dari 34 universitas. Sekitar 4-7 hari kemudian, profesor Rimawan menerima SMS dari Pizza Hut Delivery mengirim code booking XXX. Dua menit kemudian SMS serupa dikirim dengan kode aktivasi. Kemudian masuk SMS notifikasi dari Whatsapp memberitahukan bahwa ponsel tidak lagi terhubung dengan Whatsapp. Kemudian muncul pemberitahuan bahwa nomer lain 087XXX telah mengendalikan akun Whatsapp tersebut.

Sekitar satu jam kemudian, profesor Rimawan menerima kabar bahwa akun

Whatsapp miliknya mengirimkan pesan-pesan ke seluruh Whatsapp Grup dengan tautan yang bisa diklik akan mengarah pada situs yang mendukung revisi UU KPK. Atas gangguan itu, ia meminta grup Whatsapp tersebut dibubarkan dan membentuk grup Whatsapp baru dengan mengundang anggota lama. Namun, di saat yang sama muncul WA Grup dengan nama kurang lebih sama mengundang juga anggota lain sehingga akhirnya seluruh anggota keluar dari grup tersebut.

Selain itu keesokan harinya sekitar pukul 02.30 WIB, profesor Rimawan terus menerus menerima spam/*robo calls* dari kode negara +1 (Amerika Serikat). Peristiwa yang hampir mirip juga dialami oleh dosen UGM cum aktivis anti-korupsi Oce Madril. Oce menerima semacam notifikasi lewat SMS (tidak ingat persisnya isi notifikasi tersebut) dari Whatsapp sekalipun ia tidak pernah melakukan permintaan. Kemudian Oce juga menerima telepon secara intensif, kebanyakan dengan kode negara +1 (Amerika Serikat), +61 (Australia), dan nomor-nomor dari negara Afrika.

Spam/robo call ini terjadi saat Oce sedang melakukan kegiatan konferensi pers atau jadwal lainnya terkait dengan aktivitas pengorganisasian. *Spam/robo call* ini terjadi dari pagi sampai sore tidak berhenti. Kerap kali *spam/robo call* terjadi pada saat momen-momen penting, baik konferensi pers atau demonstrasi. Seingat Oce, peristiwa ini terjadi intensif selama satu minggu. Selain di Whatsapp, di akhir September 2019 juga sempat terjadi upaya pengambilalihan akun Telegram, tetapi karena ada notifikasi dari Telegram tentang upaya masuk dari perangkat yang tidak dikenali, akhirnya hal ini bisa dimitigasi. Profesor Rimawan mengatakan bahwa serangan digital yang dialaminya berpengaruh dalam upaya konsolidasi gerakan anti-korupsi dari kalangan akademisi.

Laporan serangan digital juga terjadi di Bandung. Bigwantsa Nuary dan Luthfi Indrawan, mahasiswa Unpad jurusan Administrasi Publik sama-sama aktif di Konsolidasi Mahasiswa Unpad (KMU). Ditemani salah seorang lulusan Unpad, mereka aktif menyuarakan mosi tidak percaya dalam kaitan penolakan Revisi UU KPK dan gerakan #ReformasiDikorupsi.

Menurut Luthfi, serangan digital itu berawal dari penerimaan sejumlah permintaan One-Time Password (OTP) sekalipun ia tidak pernah kepada Whatsapp. Tercatat permintaan OTP masuk ke inbox SMS pada 15 September pukul 11.20 PM (23.20 WIB), lalu dua kali pengiriman OTP pada 16 September 2019 pukul 12.00 PM (00.00 WIB), dan sekali pengiriman OTP di hari yang sama pukul 10.55 AM (10.55 WIB). Selain itu, Luthfi juga menerima permintaan memasukkan kode 2VA pada pukul 02.50 WIB yang seingat dirinya tidak pernah ia aktifkan.

Ternyata akun Whatsapp miliknya mengirim pesan yang disebar ke sejumlah grup Whatsapp kampus dan keluarga sekitar pada pukul 02.08 WIB dengan bunyi provokatif. Selain itu, salah satu lulusan yang aktif membantu keduanya juga mengkonfirmasi bahwa akun Whatsapp miliknya telah menyebarkan pesan mirip yang terjadi pada Bigswansta.

Berdasarkan laporan-laporan yang masuk dalam kurun waktu tersebut, SAFEnet menemukan kesamaan pola yang dialami oleh akademisi, aktivis anti-korupsi, dan aktivis mahasiswa yang terlibat dalam isu Revisi UU KPK dan #ReformasiDikorupsi. Pertama, serangan digital tersebut terjadi sekitar September – Oktober 2019. Kedua, serangan digital tersebut erat kaitannya dengan keterlibatan para pelapor pada aksi protes Revisi UU KPK. Ketiga, serangan digital diarahkan karena posisi krusial mereka di dalam gerakan penolakan Revisi UU KPK. Keempat,

serangan digital digunakan untuk melemahkan konsolidasi dan gerakan yang mereka lakukan.

Opresi Teknologi pada Penanganan Isu Papua

Pada tahun 2019, Facebook mengeluarkan temuan adanya praktik *Coordinated Inauthentic Behaviour* (Koordinasi Perilaku Tak Otentik) di Indonesia. *Head of Cybersecurity Policy Facebook*, Nathaniel Gleicher, menjelaskan CIB sebagai perilaku yang dikategorikan sebagai penyalahgunaan (*abuse*). CIB adalah tindakan terkoordinasi dari sejumlah FB Pages/akun yang bekerjasama untuk memperdaya orang lain tentang siapa mereka dan apa yang mereka lakukan. Tindakan CIB bisa dilakukan karena tujuan ideologis atau karena motif ekonomi. Ia menambahkan bahwa Facebook menghapus akun-akun ini bukan karena isi kontennya, melainkan karena perilakunya yang memperdaya orang lain. Isinya bisa jadi tidak melanggar ketentuan dari Panduan Komunitas Facebook.

Kedua temuan CIB terjadi pada 31 Januari 2019 dan 3 Oktober 2019. Pada penemuan kedua, Facebook menghapus 69 akun Facebook, 42 Facebook Pages, dan 34 akun Instagram yang terlibat dalam perilaku tak otentik terkoordinasi di Indonesia. Orang-orang di belakang jaringan ini menggunakan akun palsu untuk mengelola Facebook Pages, menyebarkan konten mereka dan mengarahkan orang ke situs web di luar platform. Mereka terutama memposting dalam Bahasa Inggris dan Bahasa Indonesia tentang Papua Barat dengan beberapa Facebook Pages berbagi konten untuk mendukung gerakan kemerdekaan, sementara yang lain memposting kritik terhadapnya.

Meskipun orang-orang di balik kegiatan ini berusaha menyembunyikan identitas mereka, penyelidikan Facebook menemukan tautan ke perusahaan di Indonesia bernama InsightID. Laporan Facebook menyebutkan InsightID mengelola 69 akun Facebook, 42 Halaman, dan 34 akun Instagram. Ada sekitar 410.000 akun mengikuti satu atau lebih FB Pages ini dan sekitar 120.000 akun mengikuti setidaknya satu akun Instagram ini.

InsightID juga membelanjakan uang sekitar \$300.000 (Setara dengan Rp 4,2 miliar) yang dihabiskan untuk iklan Facebook berbayar.

Penyelidikan di ranah digital tentang InsightID telah dilakukan sejak laporan dibuat sampai hari ini dan sejauh ini dapat dikumpulkan profiling -- meskipun ada upaya luar biasa untuk menghapus semua rekam jejak digital InsightID dan orang-orang yang bekerja dibelakangnya. InsightID adalah perusahaan startup berbentuk agensi jasa konsultan individu yang dibentuk sejak Februari 2018.

Sama seperti situs perusahaan yang dihapuskan dan disamarkan, jejak digital ke situsweb yang dikelola InsightID ini juga dihapus.

Manipulasi platform juga ditemukan dalam bentuk pengerahan troll dan akun bot untuk menyerang warga yang berkomentar mengenai peristiwa di Papua. Akun bot dan troll ini bertingkah secara mekanik dan menyebarkan pesan yang sama secara berulang-ulang.

Pada 22 November 2019, SAFEnet juga menerima aduan adanya serangan DDoS terhadap kerja kolektif sejumlah pekerja HAM Papua di Jakarta, Papua, dan di luar negeri yang mengumpulkan data orang Papua yang dipenjara dalam situsweb Papuans Behind Bars beralamat URL <https://www.papuansbehindbars.org/>

Ketika dicek ke server, ditemukan bahwa target serangan DDoS masif ini adalah situsweb Papuan Behind Bars tersebut. Serangan DDoS ini dibarengi dengan upayaperetasan terhadap akun Telegram, Whatsapp dan pengambilalihan akun Gmail dari salah satu pembela HAM yang terlibat dalam situsweb tersebut.

Dalam opresi teknologi yang dilakukan terhadap aktivis, pembela HAM dan jurnalis yang bergerak di isu Papua, SAFEnet menyoroti kembali terjadinya praktik *doxing* yang sempat marak terjadi pada tahun 2017 dalam peristiwa Efek Ahok. *Doxing* adalah proses mengumpulkan informasi yang dapat diidentifikasi tentang seseorang atau sekelompok orang, dengan tujuan untuk memermalukan, menakut-nakuti, memeras, memfitnah, menggertak, atau membahayakan target.

Dalam memposting rincian pribadi seseorang secara publik sering dilakukan dengan maksud membahayakan individu yang ditargetkan, terutama jika orang tersebut adalah seorang petugas penegak hukum, seorang agen yang menyamar atau individu yang terkenal. Lebih lanjut, seorang pelaku *doxing* kemungkinan akan menyeret keluarga dan kadang-kadang teman dari target, terkadang termasuk anak-anak.

Memposting informasi pribadi secara publik dengan maksud untuk dipermalukan, mencemarkan nama baik, melecehkan atau membahayakan adalah ilegal. Ini menempatkan individu yang mengalami *doxing* dalam situasi yang berpotensi berbahaya.

Selama 2019, *doxing* terjadi pada pembela HAM dan jurnalis-jurnalis yang terkait isu sensitif Papua. Pada Oktober 2019 pukul 04.35 WIB, akun Twitter @digeembok melakukan *doxing* terhadap pembela HAM Papua, Veronica Koman

dengan memberitahu lokasi tempat tinggal kedua orang tua Veronica Koman berada. Upaya *doxing* ini disertai dengan intimidasi bahwa Veronica Koman telah dipantau oleh akun tersebut.

Selain itu, tiga orang jurnalis yang meliput isu Papua mengalami *doxing*. Pada Agustus 2019, akun Twitter @antilalat melakukan *doxing* terhadap 3 jurnalis lewat postingnya.

Kemudian pada September 2019, Febriana Firdaus, jurnalis Aljazeera, juga mengalami *doxing* karena pemberitaannya terkait jumlah korban yang meninggal dalam kerusuhan di Papua.



EPILOG: Melawan Balik Otoritarianisme Digital

Meskipun Indonesia bukan dipimpin lagi oleh figur yang bertangan besi seperti rezim Orde Baru di bawah Soeharto, namun bayang-bayang kekuatan otoriter itu masih kuat mencengkeram di kepala banyak orang. Membayangkan kembalinya dwifungsi militer, kontrol informasi yang ketat, penyeragaman di banyak dimensi demi melanggengkan kekuasaan yang korup, kolusif dan nepotis, menjadi momok tersendiri yang ikut bisa dirasakan saat ini, sekalipun Soeharto sudah ditumbangkan lebih dari 20 tahun lalu pada 1998. Pada tahun pemilihan umum, narasi anti Orde Baru hadir mengingatkan Prabowo, salah satu calon presiden yang dekat dengan lingkaran keluarga Soeharto. Sementara calon presiden lain yang kini terpilih kedua kali menjadi presiden, Joko Widodo, menarasikan dirinya sudah tidak punya beban. Namun kalangan aktivis mengkritisi siapapun yang memenangkan pemilihan umum, hampir dapat dipastikan, didukung oleh kekuatan oligarki yang masih berkelindan dengan Orde Baru. Ini yang melatari gerakan #sayagolput menjelang pemilihan umum 2019 di Indonesia.

Pemilihan umum 2019 dimenangkan kembali dengan selisih tipis oleh Joko Widodo. Masyarakat yang telah terbelah karena polarisasi dukungan, sempat mengentalkan sentimen negatif, dengan melakukan

gerakan untuk menolak hasil pemilihan umum dalam bentuk demonstrasi di depan Badan Pengawas Pemilu (Bawaslu) di Jakarta. Demonstrasi ini kemudian menjadi tidak terkendali dan berujung dengan pengendalian keras dari aparat keamanan. Suasana memanas yang bermula dari penolakan hasil pemilu, menjadi letupan-letupan kekerasan antara pendukung Prabowo dengan polisi. Kemudian, untuk pertama kalinya di Indonesia, terjadi pelambatan internet (*bandwidth throttling*) pada 23-25 Mei 2019. Alasan yang digunakan oleh pemerintah saat itu, seperti yang disampaikan dalam siaran pers Kemkominfo, adalah mencegah beredarnya hoaks terkait kerusuhan. Tentu saja peristiwa ini mengejutkan, mengingat *bandwidth throttling* adalah salah satu bentuk opresi teknologi yang dikecam oleh banyak pihak, termasuk oleh PBB karena melanggar hukum internasional terkait hak akses informasi. Kritik yang disampaikan oleh organisasi masyarakat sipil, termasuk oleh SAFEnet, tidak diperhatikan pemerintah terkait tidak adanya *due process of law* dan transparansi tindakan. Bahkan pelambatan internet ini dilakukan kembali pada bulan Agustus, dan dilanjutkan dengan pemadaman internet (*internet shutdown*) sampai bulan September 2019 di Papua dan Papua Barat.

Dalam banyak kesempatan, pemerintah Indonesia sesumbar bahwa apa yang mereka lakukan dipuji oleh banyak negara karena dianggap mampu menyeimbangkan antara kemerdekaan berekspresi dan keamanan nasional.

Usai pemilihan umum 2019, pemerintah Joko Widodo didukung oleh oligarki dan melakukan konsolidasi dengan lawan politiknya dengan memberi porsi jabatan Menteri dan jabatan strategis lainnya. Pemerintah Indonesia memfokuskan diri pada investasi dan peningkatan Sumber Daya Manusia/SDM, seperti yang disampaikan dalam pidato kepresidenan, dan tidak menyinggung sama sekali tentang perbaikan hak asasi manusia/HAM. Untuk mendukung keperluan investasi tersebut, presiden mengerahkan segala upaya termasuk aparat keamanan dan intelejen untuk memuluskan jalan, terutama melancarkan upayanya melakukan pengesahan Omnibus Law. Selain itu, pemerintah juga mengusulkan revisi UU KPK, yang salah satu poin meminta agar ada Dewan Pengawas KPK yang mengawasi kinerja lembaga anti-rasuah tersebut. Kedua kebijakan ini dinilai kritis oleh organisasi masyarakat sipil dan akademisi sebagai upaya melemahkan kekuatan Negara dalam melawan korupsi dan oligarki. Karenanya terjadi demonstrasi besar-besaran terkait penolakan revisi UU KPK dan juga Omnibus Law di banyak kota. Demonstrasi yang mayoritas dilakukan oleh mahasiswa, akademisi, dan aktivis ini dihadapi dengan aksi kekerasan di sejumlah kota. Tercatat ratusan korban luka-luka akibat benturan dengan aparat, bahkan juga ada korban meninggal dunia. Kekerasan fisik dengan terjadi semakin diperparah dengan laporan kekerasan digital yang dialami oleh mahasiswa, akademisi dan aktivis. Selain itu, dengan memanasnya konflik di Papua akibat tindakan rasial kepada mahasiswa Papua di Malang dan Surabaya, kekerasan fisik dan kekerasan digital juga terjadi pada mereka yang mengadvokasi isu Papua, dilanjut dengan peristiwa pelambatan internet dan pemadaman internet.

Berbagai peristiwa peretasan aktivis dan akademisi, intimidasi dalam bentuk doxing kepada aktivis dan jurnalis, pengerahan *cyber army* yang dipimpin *key opinion leader* untuk menggeruduk para penolak kebijakan pemerintah, juga kepada media yang kritis, merupakan penanda bagaimana teknologi digunakan untuk melakukan represi terhadap kemerdekaan berekspresi dan kemerdekaan untuk berkumpul di Indonesia.

Catatan lengkap mengenai seluruh kejadian ini telah dipantau dan dimuat dalam laporan tahun ini kondisi hak digital di Indonesia untuk dibaca. Sebagai organisasi yang memerjuangkan hak digital di kawasan Asia Tenggara, termasuk di antaranya Indonesia, SAFE-net betul-betul khawatir bahwa Indonesia akan segera menyusul banyak negara di kawasan yang kini mempraktikkan Otoritarianisme Digital.

Sejak pengungkapan Edward Snowden pada 2013 tentang program-program pengawasan massa yang dijalankan oleh badan-badan intelijen di negara-negara demokrasi Barat menyoroti fakta bahwa praktik-praktik otoritarianisme digital bukan semata-mata terjadi pada rezim otoriter. Hal semacam ini bisa terjadi bahkan di negara demokratis. Manipulasi teknologi digital dan penyalahgunaan media sosial dan feed berita yang dikuratori dengan algoritma dapat digunakan untuk melemahkan nilai-nilai demokrasi suatu negara. Yang akan terjadi sebagaimana bisa dilihat pada rezim otoriter adalah bagaimana teknologi komunikasi digital digunakan untuk melakukan penyaringan dan sensor untuk mengendalikan arus informasi di dan keluar negara tersebut. Mereka menggunakan penyadapan, serangan siber, dan disinformasi untuk mengkonsolidasikan kekuatan. Selain itu, antara sesama rezim otoriter mereka bertukar alat dan keahlian dalam melakukan kontrol Internet dan mempromosikan ide-ide tentang bagaimana mengatur teknologi digital di tingkat internasional, sebagaimana disebut profesor Diebert sebagai *Network Authoritarianism* seperti yang telah terjadi di China selama ini.

Mengadopsi sistem kebencanaan yang telah digunakan selama ini dalam penyusunan laporan kondisi hak-hak digital, SAFE-net menetapkan Indonesia kini berada dalam siaga satu menghadapi Otoritarianisme Digital. Menyadari atas situasi kebangkitan Otoritarianisme Digital ini, tidak ada cara lain yang dapat kami rekomendasikan, selain melakukan perlawanan balik untuk memukul mundur kemunculan otoritarianisme digital di Indonesia, lewat jalur hukum, melakukan kritik secara terbuka, melakukan konsolidasi masyarakat sipil di tingkat nasional, sembari menjalin dukungan dari kawasan dan internasional untuk mencegah hal terburuk di masa depan.



SOUTHEAST ASIA FREEDOM OF EXPRESSION NETWORK

2020