BAB II

Online Gender Based Violence (OGBV) di Asia Tenggara

2.1. Pelanggaran Hak Digital di Asia Tenggara

Maraknya adopsi teknologi digital dan internet telah mentransformasi ruang publik di Asia Tenggara, namun pada saat yang sama, telah menciptakan arena baru bagi praktik kekerasan berbasis gender yang dikenal sebagai Online Gender-Based Violence (OGBV). OGBV, yang mencakup cyber-harassment, dimana penyebaran disinformasi berbasis gender, doxing, hingga penyebaran gambar intim non-konsensual, telah menjadi salah satu bentuk kekerasan berbasis gender dengan pertumbuhan tercepat di kawasan Asia Tenggara (ASEAN & UNFPA, 2025). Hal ini berdasarkan studi yang menunjukkan bahwa antara 16% hingga 58% wanita di Asia Tenggara pernah mengalami kekerasan online, dan sekitar 85% telah menyaksikan bentuk kekerasan tersebut (Asean & Unfpa, 2025; Eria, 2022). Percepatan digitalisasi yang didorong oleh respons terhadap Pandemi COVID-19—di mana ketergantungan pada ruang online untuk bekerja, belajar, dan bersosialisasi meningkat tajam—sehingga secara signifikan memperluas vektor ancaman OGBV, membuat perempuan dan kelompok gender rentan semakin terekspos (Un Women, 2021).

OGBV tidak hanya mencerminkan ketidaksetaraan gender yang sudah ada di dunia offline, tetapi juga menimbulkan dampak psikologis, sosial, dan ekonomi yang berkepanjangan, serta mengikis partisipasi perempuan dan kelompok gender rentan di ruang digital atau di berbagai sektor kehidupan masyarakat. (UNFPA, 2025). Yang kemudian kondisi ini diperparah oleh adanya kesenjangan regulasi dan keterbatasan mekanisme pelaporan yang responsif negara ASEAN (Eria, 2022; Women's Rights Online, n.d.). Dimana hal ini juga merujuk pada periode setelah krisis global akibat COVID-19, yakni setelah gelombang awal pembatasan sosial selama pandemi yang mendorong masyarakat untuk beradaptasi dengan layanan berbasis teknologi. Fenomena ini tidak berhenti setelah pandemi mereda, melainkan berkembang menjadi pola baru kehidupan sosial berbasis digital. Ruang digital menjadi arena utama interaksi sosial, ekonomi, dan politik bagi masyarakat di Asia Tenggara yang memperoleh lebih dari 70 juta pengguna digital baru sejak 2020, menjadikan kawasan

ini salah satu wilayah dengan pertumbuhan digital tercepat di dunia (Google Temasek Bain, 2022).

Era digital di Asia Tenggara telah membawa transformasi besar, internet, smartphone, dan layanan daring menjadi bagian dari kehidupan sehari-hari. Akses informasi, media sosial, serta platform komunikasi memungkinkan orang untuk mendapat informasi, berkomunikasi, berorganisasi, atau menyuarakan pendapat secara lebih luas. Namun, transformasi ini tidak hanya soal kemajuan teknologi atau ekonomi namun ruang digital juga menjadi medan penting bagi ekspresi sosial-politik dan partisipasi publik. Perkembangan ini secara khusus terlihat pada pesatnya penggunaan internet dan perangkat seluler di Asia Tenggara. Laporan menunjukkan bahwa Asia Tenggara ini memiliki lebih dari 335 juta pengguna smartphone, dan sekitar 66% lalu lintas internet berasal dari perangkat mobile (Tech for Good Institute, 2023).

Tetapi, perluasan akses dan dominasi ruang digital ini juga membuka pintu bagi risiko pelanggaran hak digital. Fakta di Indonesia, yang mewakili bagian dari Asia Tenggara, menggambarkan bagaimana tantangan itu muncul. Laporan SAFEnet menegaskan bahwa pelanggaran hak-hak digital, termasuk akses internet, kebebasan berekspresi, keamanan digital, dan kekerasan berbasis gender online terus terjadi lantaran campur tangan negara maupun aktor non-negara. Dalam periode jelang Pemilu 2024, SAFEnet mencatat sebanyak 323 serangan digital, termasuk peretasan situs pemerintah maupun swasta, kebocoran data pemilih, serta serangan terhadap jurnalis, akademisi, dan aktivis (Freedom House, 2024, 168). Lebih lanjut, sepanjang triwulan I 2025, SAFEnet melaporkan 12 gangguan infrastruktur internet dan puluhan kasus kriminalisasi ekspresi daring serta kekerasan berbasis gender online menjadi bukti bahwa pelanggaran hak digital bukan fenomena sesaat, melainkan bagian dari pola berkelanjutan (SAFEnet, 2025).

Lebih luas lagi, di kawasan Asia Pasifik, tren global ketidakbebasan internet tercermin melalui praktik sensor, blokir situs, pembatasan konten, dan represi digital (Freedom House, 2024). Pemblokiran layanan daring, pengawasan, penghentian koneksi internet saat krisis politik atau demonstrasi, serta regulasi yang memungkinkan pembatasan konten, menjadi bagian dari strategi kontrol yang menurunkan ruang kebebasan digital. Data dari Safeguarding Digital Rights in Southeast Asia Report oleh SAFEnet (2023) menunjukkan bahwa aduan pelanggaran hak digital di Indonesia dan beberapa negara ASEAN meningkat setiap tahun,

terutama dalam kategori serangan digital (digital attacks), kriminalisasi ekspresi, gangguan akses, dan kekerasan berbasis gender online. Laporan tersebut juga menegaskan bahwa perempuan mendominasi korban kekerasan digital, meski laki-laki juga mengalami risiko serupa. Pola ini memperlihatkan keterkaitan langsung antara pelanggaran hak digital dan bentuk-bentuk OGBV, di mana teknologi digunakan untuk memperkuat kekerasan berbasis gender melalui penyebaran konten, manipulasi digital, hingga ancaman dan intimidasi.

Di Indonesia, salah satunya, Menurut Laporan Situasi Hak Digital di Indonesia Tahun 2023, terdapat sejumlah pelanggaran hak digital yang signifikan, termasuk pelanggaran terkait kekerasan berbasis gender online (OGBV) dan kebocoran data pribadi, terutama terkait dengan Pemilu 2024 di Indonesia (SAFEnet, 2023, 5-6). Laporan tersebut merinci beberapa kasus kebocoran data pribadi, seperti kebocoran yang melibatkan informasi pribadi jutaan warga, termasuk nomor identifikasi pribadi, rekam medis, dan data keuangan. Laporan ini juga membahas bagaimana gangguan akses internet, yang mempengaruhi kemampuan warga untuk terlibat dalam proses pemilu, semakin diperburuk selama periode pemilu. Setidaknya 63 kasus masalah akses internet dilaporkan pada 2023, termasuk gangguan berbasis kebijakan dan gangguan layanan. Selain itu, laporan ini menyoroti insiden sensor politik, dengan motif politik di balik banyaknya kriminalisasi ekspresi online, terutama yang terkait dengan penggunaan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Dengan demikian, meskipun digitalisasi sesungguhnya membawa banyak potensi bagi akses informasi dan partisipasi publik, kenyataan di Asia Tenggara menunjukkan bahwa tanpa perlindungan hak digital yang kokoh, perluasan ruang digital dapat berubah menjadi alat represi. Pelanggaran hak-hak seperti kebebasan berekspresi, akses internet, privasi, dan keamanan digital terjadi nyata, baik melalui regulasi, sensor, kriminalisasi, maupun serangan siber. Oleh karena itu, terutama dalam konteks Hubungan Internasional, fenomena OGBV di Asia Tenggara, khususnya pada periode pasca-pandemi yang ditandai dengan intensifikasi ruang digital, menjadi isu penting yang membutuhkan respon kolektif dan transnasional, yang melibatkan aktor negara maupun non-negara, termasuk di dalamnya adalah Peran Civil Society Organizations Berbasis Digital dalam melakukan advokasi terhadap isu ini.

2.1.1. Karakter Online Gender Based Violence

Perkembangan teknologi digital tidak hanya membuka ruang baru untuk berinteraksi dan berekspresi, tetapi juga memunculkan bentuk-bentuk kekerasan berbasis gender yang berlangsung melalui daring. Online Gender- Based Violence (OGBV) merujuk pada kekerasan berbasis gender yang dilakukan melalui perangkat dan platform digital, berupa tindakan yang menyerang identitas, tubuh, keamanan, atau privasi perempuan dan kelompok rentan. Komnas Perempuan telah menegaskan bahwa sejak 2015 ruang digital di Indonesia membuka peluang munculnya kekerasan baru seperti pelecehan, doxxing, penyebaran konten seksual tanpa persetujuan, ancaman kekerasan, hingga peretasan akun. SAFEnet juga mengidentifikasi bahwa OGBV adalah bagian dari pelanggaran hak digital karena menyerang hak atas privasi, kebebasan berekspresi, serta keamanan digital korban (Manohara, 2023, 103).

Online Gender-Based Violence (OGBV) bukanlah perpanjangan sederhana dari kekerasan offline, melainkan memiliki karakteristik unik, seperti jangkauan global, anonimitas pelaku yang tinggi, potensi penyebaran konten yang cepat dan permanen, serta dampaknya yang sering kali membatasi partisipasi politik dan ruang berekspresi korban di ranah publik digital (Keller & Ringrose, 2019). Dalam konteks Asia Tenggara, proliferasi internet dan media sosial telah meningkatkan insiden OGBV, yang diperburuk oleh lemahnya kerangka hukum siber, norma budaya patriarkal yang meresap, dan celah digital (digital divide), Online Gender-Based Violence (OGBV) merupakan isu keamanan non-tradisional yang mengancam partisipasi digital dan hak asasi manusia perempuan, didefinisikan sebagai kekerasan berbasis gender yang difasilitasi oleh teknologi informasi dan komunikasi [(Wood, 2020)]. Bentuk-bentuk OGBV sangat beragam dan meliputi, namun tidak terbatas pada pelecehan dan trolling (serangan verbal berulang), penyebaran informasi atau gambar intim non-konsensual (non-consensual sharing of intimate images atau revenge porn), ancaman kekerasan (cyber-threats), pencurian identitas dan doxing (publikasi data pribadi tanpa izin), dan penguntitan siber (cyberstalking) (Keller & Ringrose, 2019).

Sehingga dalam konteks Asia Tenggara, proliferasi platform digital telah memperparah insiden ini, menjadikannya masalah lintas batas (transnasional) yang membatasi ruang sipil dan politik perempuan secara daring, terutama bagi mereka yang aktif dalam advokasi atau politik. Oleh karena itu, OGBV menyoroti kegagalan

tata kelola siber regional, sehingga menggarisbawahi peran krusial Civil Society Organizations (CSO) berbasis digital dalam melakukan advokasi reformasi kebijakan, menyediakan bantuan hukum, dan membangun mekanisme respon bagi korban yang terintegrasi secara regional (Phan & Grewal, 2021). yang semuanya menyoroti peran penting Civil Society Organizations (CSO) berbasis digital dalam advokasi, respon, dan upaya reformasi kebijakan untuk mengatasi fenomena transnasional dan multidimensi ini (Phan & Grewal, 2021).

Pernyataan tersebut juga didukung oleh adanya temuan Komnas Perempuan yang mengidentifikasi bentuk kekerasan seksual berbasis teknologi dan mengelompokkannya ke dalam sembilan kategori GBV, yaitu: (1) Cyber Hacking, penggunaan teknologi secara ilegal untuk memperoleh informasi pribadi atau merusak reputasi korban; (2) Cyber Harassment, penggunaan teknologi untuk menghubungi, mengancam, atau menakut-nakuti korban; (3) Impersonation, penggunaan teknologi untuk mengambil identitas orang lain guna mengakses informasi pribadi, mempermalukan, atau membuat dokumen palsu; (4) Cyber Recruitment, penggunaan teknologi untuk memanipulasi korban hingga masuk ke situasi berbahaya; (5) Cyberstalking, penggunaan teknologi untuk mengawasi perilaku atau pergerakan korban melalui pengamatan langsung atau penelusuran jejak digital; (6) Malicious Distribution, penggunaan teknologi untuk menyebarkan konten yang merusak reputasi korban; (7) Revenge Porn, penyebaran foto atau video intim tanpa persetujuan sebagai bentuk balas dendam; (8) Sexting, pengiriman gambar atau video bermuatan pornografi kepada korban tanpa permintaan; (9) Morphing, pengubahan foto atau video untuk merusak reputasi atau martabat korban (Manohara, 2023; Komnas Perempuan, 2021). Sementara itu, SAFEnet mengelompokkan delapan bentuk kekerasan berbasis gender online yang umum terjadi, meliputi: (1) Cyber Grooming, pendekatan manipulatif untuk tujuan seksual; (2) Cyber Harassment; (3) Hacking; (4) Illegal Content, penyebaran konten ilegal yang melanggar hukum atau norma kesusilaan; (5) Infringement of Privacy, pelanggaran atas data dan ruang privat korban; (6) Malicious Distribution (7) Online Defamation, pencemaran nama baik melalui platform daring; (8) Online Recruitment, perekrutan korban secara daring untuk tujuan eksploitasi (Manohara, 2023; SAFEnet, 2019).

SAFENet mengelompokkan berbagai bentuk OGBV kedalam kategori, yaitu Pelanggaran privasi, Pengawasan dan pemantauan, Perusakan reputasi/kredibilitas,

Pelecehan, Ancaman dan kekerasan langsung, serta Serangan yang ditargetkan secara langsung. (SAFEnet, 2019).

No	Kategori	Definisi	Contoh Diskriminasi	Sumber
1	*Pelanggaran Privasi*	Mencakup tindakan yang melanggar hak personal dan ruang privat korban, seperti peretasan, pelanggaran privasi, impersonation, hingga perekrutan daring yang memanipulasi korban ke situasi berbahaya.	Penyebaran Foto/Video Intim Tanpa Izin (*Non- Consensual Intimate Image/NCII*) atau penyebaran data pribadi korban yang sensitif. (Ranah diskriminasi: pekerjaan & karir). Penyebaran *Chat* Pribadi yang telah dimanipulasi atau *sextortion* yang gagal dan pelakunya	(SAFEnet, 2019).
2	*Pengawasan dan Pemantauan*	Meliputi bentuk-bentuk pengawasan dan pelacakan aktivitas korban melalui teknologi, termasuk *cyber stalking* dan pemantauan jejak digital tanpa persetujuan.	Pemantauan Media Sosial / Sosial Media Monitoring. (Ranah diskriminasi sosial privasi).	(SAFEnet, 2019).
3	*Perusakan Reputasi*	Merujuk pada tindakan yang merusak nama baik dan citra korban, seperti *malicious distribution*, pencemaran nama baik daring, morphing, serta penyebaran konten intim tanpa persetujuan ketika ditujukan untuk menjatuhkan reputasi.	Kampanyem *Smear* Daring Berbasis Gender/Seksualitas terhadap perempuan profesional. (Ranah diskriminasi sosial & komunitas).	(SAFEnet, 2019).
4	*Pelecehan*	Mencakup berbagai bentuk pelecehan dan intimidasi daring, termasuk *cyber harassment*, pengiriman konten seksual tanpa izin, hingga grooming yang memanfaatkan pendekatan manipulatif untuk tujuan seksual.	Pelecehan Seksual Berulang di tempat kerja (misalnya, komentar cabul, sentuhan yang tidak diinginkan, atau permintaan seksual). (Ranah diskrimanasi *Constructive Dismissal*) Pelecehan Rasial/Etnis (misalnya, panggilan yang merendahkan, lelucon etnis yang menghina, atau intimidasi) . (Ranah diskriminasi sosial & komunitas).	(SAFEnet, 2019).
5	*Ancaman dan*	mengacu pada pemerasan, dapat secara seksual, materi seperti uang, properti,	Ancaman Pembunuhan atau Penyiksaan Fisik (Ranah	(SAFEnet, 2019).

	Kekerasan Langsung	atau identitas, perdagangan manusia atau perempuan melalui penggunaan teknologi dengan persiapan (kekerasan seksual terencana) , peniruan identitas atau impersonasi yang mengakibatkan serangan fisik	diskriminasi politik dan kebebasan berpendapat).	
6	*Serangan yang ditargetkan ke komunitas tertentu*	merajuk pada peretasan situs web, media sosial, atau email organisasi atau komunitas dengan niat jahat, pemantauan dan ancaman pada anggota komunitas/organisasi, Pengepungan (mobbing), khususnya ketika memilih target untuk intimidasi atau pelecehan oleh sekelompok orang, daripada individu.	Kampanye Pelecehan dan Ancaman Massal. Serangan Siber (Hack and Leak).	(SAFEnet, 2019).

Kategori OGBV/KBGO yang ditetapkan SAFEnet secara jelas menggarisbawahi bahwa kekerasan digital adalah titik awal yang terstruktur yang mengarah pada diskriminasi multispektrum (dari pemecatan, pengucilan, hingga penghambatan politik). Oleh karena itu, penanganan OGBV/KBGO harus diintegrasikan dengan upaya anti-diskriminasi dan perlindungan hak asasi manusia di ranah digital dan non-digital.

2.2. Fenomena Online Gender Based Violence di Asia Tenggara

Fenomena OGBV di Asia Tenggara menunjukkan peningkatan signifikan selama dan setelah pandemi COVID-19 seiring dengan meningkatnya penggunaan internet, media sosial, dan layanan berbasis aplikasi. Data nasional dari Indonesia menunjukkan pola ini dengan jelas: laporan mengenai penyebaran konten intim non-konsensual (NCII), pelecehan seksual digital, peretasan akun pribadi, dan doxxing meningkat sejak 2020 menurut SAFEnet (SAFEnet, 2021; SAFEnet, 2023). Hal ini sejalan dengan temuan Komnas Perempuan, yang mencatat tren kenaikan kekerasan berbasis siber dalam laporan tahunan mereka, terutama pada periode 2020–2023, akibat meningkatnya intensitas aktivitas digital masyarakat (Komnas Perempuan,

2022). Data regional juga mendukung hal ini, misalnya laporan UN Women Asia-Pacific yang menemukan bahwa lebih dari separuh perempuan muda di kawasan tersebut pernah mengalami bentuk pelecehan atau kekerasan berbasis gender di ruang digital (UN Women, 2022).

Selain peningkatan jumlah kasus, modus OGBV juga mengalami diversifikasi. Bentuk-bentuk seperti NCII, cyber-harassment, cyber-stalking, pemerasan seksual digital (sextortion), deepfake, dan doxxing menjadi semakin umum. Studi lokal di Indonesia menunjukkan bahwa kelompok perempuan muda, khususnya Gen-Z, merupakan kelompok yang paling sering terpapar bentuk-bentuk kekerasan digital tersebut (Manuhoro, 2023). Pola serupa juga ditemukan di Malaysia; laporan Women's Aid Organisation (WAO) mencatat peningkatan aduan mengenai pelecehan seksual digital, termasuk pengintaian digital dan pengiriman konten seksual tanpa izin, sepanjang 2020–2022 (WAO, 2022). Konsistensi pola lintas negara ini menunjukkan bahwa meningkatnya interaksi digital pasca-pandemi berkontribusi langsung terhadap perluasan risiko OGBV di kawasan.

Kemudian fenomena OGBV di Asia Tenggara pasca-pandemi COVID-19 terutama di periode 2020-2024 juga ditandai oleh tiga tren utama yang kompleks, yang menuntut respons transnasional dan peran aktif Civil Society Organizations (CSO) dimana ketiga tren tersebut yaitu: Peningkatan Akselerasi dan Intensitas Kasus ; Tren ini paling signifikan yakni karena akselerasi dramatis jumlah kasus, yang menunjukkan pergeseran lingkungan kekerasan dari offline ke online sebagai dampak dari masifnya digitalisasi selama pandemi. Dimana data empiris dari Indonesia menunjukkan lonjakan kekerasan siber yang dilaporkan mencapai lebih dari 300% pada tahun 2020 dibandingkan tahun sebelumnya (Komnas Perempuan, 2021).

Dengan organisasi regional seperti SAFEnet mencatat lebih dari 620 kasus OGBV sepanjang 2020 di kawasan tersebut (SAFEnet, 2021). Peningkatan ini mengindikasikan bahwa infrastruktur digital yang berkembang pesat tidak diimbangi dengan perlindungan yang memadai, menciptakan celah keamanan siber yang eksploitatif bagi perempuan (Phan & Grewal, 2021). Selanjutnya dominasi Konten Intim Non-Konsensual (NCII) dan Pemerasan, bentuk OGBV yang paling mendominasi adalah penyebaran Konten Intim Non-Konsensual (NCII), atau yang dikenal sebagai revenge porn, seringkali disertai dengan ancaman sextortion (pemerasan seksual). Fenomena ini menjadi isu transnasional karena pelaku dapat beroperasi lintas batas, mengeksploitasi anonimitas dan kesulitan yurisdiksi hukum.

Studi oleh Plan International (2020). di Asia Tenggara menegaskan prevalensi tinggi, menemukan bahwa hampir 75% perempuan muda pernah mengalami kekerasan atau pelecehan online, dengan NCII menjadi salah satu bentuk yang paling merusak secara psikologis (Plan International, 2020).

Kemudian selanjutnya yaitu penargetan terorganisir terhadap partisipasi sipil perempuan, dimana fenomena krusial dalam konteks Hubungan Internasional adalah penggunaan OGBV sebagai senjata politik yang terorganisir (coordinated harassment) untuk membungkam partisipasi perempuan dalam ruang publik digital. OGBV secara sistematis menargetkan jurnalis perempuan, aktivis hak asasi manusia, dan politisi perempuan, bertujuan merusak kredibilitas dan memaksa mereka menarik diri dari wacana publik [(UN Women, 2021)]. Tren ini menunjukkan bahwa OGBV bukan hanya masalah individu, melainkan isu keamanan digital kolektif yang mengancam demokrasi digital dan hak berekspresi di Asia Tenggara (Loh, 2023).

Tren kenaikan ini juga diikuti oleh berkembangnya kerangka normatif internasional yang mengakui kekerasan berbasis gender di ruang digital sebagai isu yang membutuhkan respons negara. CEDAW melalui General Recommendation No. 35 menegaskan bahwa kekerasan berbasis gender yang terjadi di ruang yang dimediasi teknologi merupakan bentuk diskriminasi yang wajib dicegah dan ditangani oleh negara pihak (CEDAW, 2017). Di tingkat global, Dewan HAM PBB menerbitkan resolusi khusus mengenai kekerasan berbasis teknologi terhadap perempuan dan anak perempuan yang menyoroti ancaman seperti cyber-harassment, doxxing, dan penyebaran konten intim tanpa persetujuan (UN Human Rights Council, 2024). UN Women juga telah mengembangkan kerangka konseptual komprehensif mengenai technology-facilitated gender-based violence sebagai acuan global bagi negara dan organisasi masyarakat sipil untuk memahami pola, risiko, serta kebutuhan kebijakan dalam menangani OGBV (UN Women, 2025).

Pada tingkat regional, ASEAN melalui ASEAN Declaration on the Elimination of Violence Against Women and Children dan ASEAN Regional Plan of Action on EVAW menunjukkan adanya komitmen kawasan untuk memperkuat perlindungan perempuan dari bentuk-bentuk kekerasan, termasuk yang muncul akibat perkembangan teknologi (ASEAN, 2013; ASEAN, 2015). Kehadiran berbagai instrumen ini menegaskan bahwa OGBV telah memperoleh pengakuan internasional sebagai fenomena yang menuntut tanggung jawab negara dan kerja sama lintas batas.

Namun, kerangka kebijakan di tingkat ASEAN belum mampu mengimbangi peningkatan risiko tersebut. ASEAN Declaration on the Elimination of Violence Against Women and Children (2013) memang mengakui bahwa teknologi dapat melahirkan bentuk-bentuk kekerasan baru, tetapi sifatnya yang non-binding menjadikan implementasi sangat bergantung pada masing-masing negara (ASEAN, 2013). Demikian pula, ASEAN Digital Masterplan 2025 menekankan pentingnya keamanan digital tetapi tidak mengatur OGBV secara spesifik (ASEAN, 2021). Laporan UNFPA Asia-Pacific menyebutkan bahwa ketiadaan standar regional yang mengikat membuat negara-negara di Asia Tenggara menghadapi tantangan besar dalam menangani OGBV yang bersifat lintas batas dan sulit dilacak (UNFPA, 2025).

Pada tingkat nasional, negara-negara Asia Tenggara menunjukkan variasi besar dalam kualitas regulasi. Filipina termasuk yang paling maju melalui Safe Spaces Act (RA 11313), yang secara eksplisit mengatur pelecehan berbasis gender di internet dan menyediakan mekanisme penghapusan konten serta perlindungan bagi korban (Philippine Commission on Women, 2021). Singapura memiliki Protection from Harassment Act (POHA) yang memungkinkan korban mengajukan protection order terhadap pelaku pelecehan daring (Singapore Government, 2022). Indonesia mengandalkan UU ITE, UU TPKS, dan UU Perlindungan Data Pribadi (PDP), tetapi belum memiliki regulasi khusus OGBV yang komprehensif (Kemenkominfo, 2022; DPR RI, 2022). Malaysia dan Thailand memiliki Undang-Undang Perlindungan Data Pribadi (PDPA), tetapi fokus utamanya masih pada keamanan data, bukan kekerasan berbasis gender digital (Malaysia PDPA, 2010; Thailand PDPA, 2019).

Tantangan implementasi regulasi terlihat dari minimnya mekanisme dukungan korban. Laporan UNDP dan UN Women menunjukkan bahwa kurang dari sepertiga perempuan korban kekerasan digital di kawasan Asia-Pasifik melaporkan kasusnya kepada aparat formal karena rendahnya kepercayaan, ketakutan akan stigma, dan kerumitan pembuktian (UNDP, 2021; UN Women, 2022). Temuan SAFEnet dan WAO juga menunjukkan bahwa korban sering kesulitan mendapatkan keadilan, terutama ketika pelaku anonim atau berada di negara lain, sehingga penanganannya terbentur yurisdiksi yang berbeda (SAFEnet, 2023; WAO, 2022).

Dalam situasi ketika negara belum mampu menyediakan perlindungan yang memadai, organisasi masyarakat sipil memainkan peran yang sangat penting. Di Indonesia, SAFEnet berperan dalam pendampingan korban, advokasi kebijakan, dan edukasi literasi digital. Di Malaysia, WAO menjalankan fungsi serupa melalui hotline

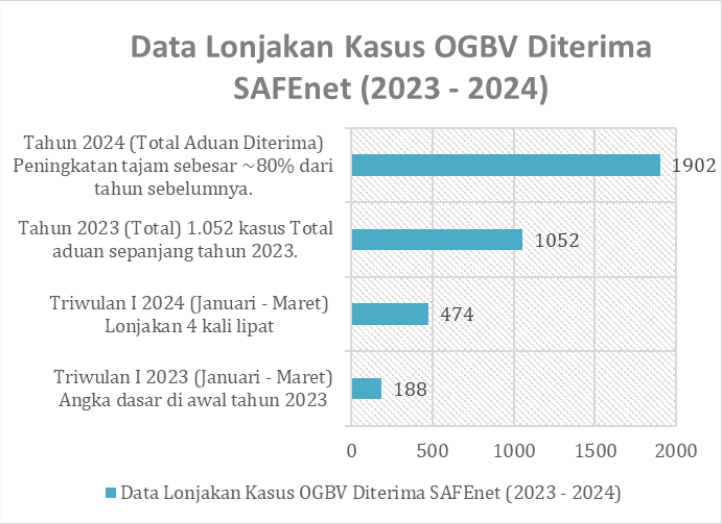
dan kampanye kesadaran publik (WAO, 2022). Kolaborasi antara negara dan CSO menjadi kunci untuk membangun ekosistem digital yang lebih aman dan responsif terhadap kebutuhan korban OGBV di Asia Tenggara.

2.3. SAFEnet terhadap OGBV di Asia Tenggara

SAFEnet (Southeast Asia Freedom of Expression Network) merupakan organisasi masyarakat sipil yang berfokus pada isu kebebasan berekspresi, hak digital, dan keamanan pengguna internet di Indonesia serta kawasan Asia Tenggara. Sejak berdiri, SAFEnet menempatkan pemantauan, advokasi kebijakan, peningkatan kapasitas digital, serta perlindungan bagi kelompok rentan sebagai mandat utamanya, sebagaimana dijelaskan dalam laporan organisasi dan berbagai publikasi resmi (SAFEnet, 2020). Dalam kerangka tersebut, SAFEnet memandang pelanggaran hak digital bukan hanya sebagai tindakan teknis yang mengganggu akses internet, melainkan sebagai persoalan hak asasi yang berkaitan dengan pembatasan kebebasan berekspresi, kriminalisasi berbasis UU ITE, sensor digital, manipulasi informasi, serta runtuhnya rasa aman pengguna di ruang daring. Laporan situasi digital tahunan SAFEnet secara konsisten menekankan bahwa empat indikator utama—akses, kebebasan berekspresi, keamanan pengguna, dan keberpihakan terhadap kelompok rentan—harus hadir secara simultan agar hak digital dapat dipenuhi (SAFEnet, 2021).

Dalam konteks OGBV (Online Gender-Based Violence), SAFEnet memandang fenomena ini sebagai bentuk pelanggaran hak digital yang bersifat struktural dan semakin meningkat seiring intensifikasi penggunaan teknologi, termasuk pada masa pandemi. SAFEnet menekankan bahwa OGBV tidak dapat dipandang sebagai insiden individu semata karena karakteristiknya yang sistemik, berkelindan dengan ketimpangan gender, serta dipengaruhi oleh mekanisme digital yang memungkinkan penyebaran cepat, anonimitas pelaku, dan kerentanan terhadap doxing, pelecehan seksual daring, maupun penyebaran konten intim non-konsensual (SAFEnet, 2021). Pandangan ini diperkuat melalui kolaborasi pemantauan bersama Komnas Perempuan, yang menunjukkan tren berulang dan konsisten terkait kekerasan berbasis gender online sejak 2019 (Komnas Perempuan, 2022). Dalam beberapa rilis pers dan laporan situasi kasus, SAFEnet juga mencatat bahwa laporan yang masuk ke layanan pendampingan menunjukkan pola ancaman yang semakin kompleks,

termasuk pemerasan, pengawasan digital, penyalahgunaan data pribadi, serta tindakan intimidatif berbasis politisasi gender (SAFEnet, 2022). Pernyataan di atas tersebut diperkuat kembali oleh data lonjakan aduan terkait OBGV yang diterima oleh SAFEnet pada tahun 2023 sampai dengan 2024, melalui grafik data berikut:



Gambar 2.1 Data Lonjakan Kasus isu OGBV SAFEnet

Sumber : Data aduan yang diterima SAFEnet (2023-2024)

Berdasarkan grafik data diatas tersebut, SAFEnet (Southeast Asia Freedom of Expression Network) memandang Kekerasan Berbasis Gender Online (OGBV) di Asia Tenggara sebagai ancaman serius terhadap hak-hak digital, khususnya bagi perempuan dan kelompok rentan, dan mencatat lonjakan kasus yang memprihatinkan. Organisasi ini secara aktif memantau dan mendokumentasikan kasus OGBV yang terjadi, seringkali menunjukkan peningkatan tajam dari tahun ke tahun misalnya, adanya peningkatan signifikan aduan dari 1.052 kasus pada 2023 menjadi 1.902 aduan pada 2024, mengindikasikan grafik yang terus menanjak tajam. Jenis-jenis OGBV yang didata SAFEnet meliputi berbagai bentuk, dengan beberapa kasus terbanyak adalah ancaman penyebaran konten intim, sextortion (pemerasan seksual), dan penyebaran konten intim tanpa izin (NCII), selain juga mencakup doxing, flaming, dan impersonasi akun. Peningkatan ini memperlihatkan bahwa ranah digital di Asia Tenggara masih jauh dari aman dan membutuhkan advokasi kebijakan serta dukungan bagi korban yang berkelanjutan.

SAFEnet juga berperan melalui inisiatif praktis seperti kampanye “Awas KBGO!”, layanan pendampingan korban, pelatihan keamanan digital, serta advokasi

untuk reformasi kebijakan yang lebih efektif dalam menangani OGBV. Kampanye tersebut menegaskan pentingnya pendekatan yang menggabungkan perlindungan data pribadi, keamanan digital, dan dukungan psikososial bagi korban, serta dorongan menuju peningkatan kapasitas aparat penegak hukum agar respons terhadap kasus-kasus OGBV tidak reviktimisasi (SAFEnet, 2021). Sejumlah laporan SAFEnet selama 2020–2023 juga menempatkan OGBV sebagai isu prioritas yang mempengaruhi kualitas demokrasi digital, karena meningkatnya kekerasan daring terhadap perempuan berkontribusi pada menurunnya partisipasi publik dan kebebasan berekspresi kelompok rentan di dunia maya (SAFEnet, 2023).

Sehingga secara keseluruhan, posisi SAFEnet terhadap OGBV di Asia Tenggara memperlihatkan peran ganda: sebagai lembaga yang memproduksi data, memetakan tren kasus, serta mengangkat bahaya OGBV ke dalam wacana kebijakan; dan sebagai aktor yang menyediakan dukungan langsung melalui pendampingan dan edukasi publik. Melalui publikasi, laporan advokasi, dan kolaborasi dengan lembaga nasional maupun regional, SAFEnet menempatkan OGBV sebagai komponen integral dari pelanggaran hak digital yang harus ditangani secara holistik melalui pendekatan struktural, kebijakan, dan penguatan kapasitas komunitas (SAFEnet, 2023).