CIVICUS : Pendidikan-Penelitian-Pengabdian
Pendidikan Pancasila & Kewarganegaraan
p-ISSN 2338-9680 | e-ISSN 2614-509X | Vol. 9 No. 1 Maret 2021, hal. 38-46

Desain Pola Integrasi Cyber dalam Mengurangi Kejahatan Cyberbullying

Abdul Sakban[1], Zaini Bidaya[2]

[1]Pendidikan Pancasila dan Kewarganegaraan, Universitas Muhammadiyah Mataram, sakban.elfath@yahoo.co.id
[2]Pendidikan Pancasila dan Kewarganegaraan, Universitas Muhammadiyah Mataram, zainibidaya@gmail.com

INFO ARTIKEL

Riwayat Artikel:

Diterima: 28 Februari 2021
Disetujui: 30 Maret 2021

Kata Kunci:

Pola
Intgerasi Cyber
Mengurangi
Cyberbullying

ABSTRAK

Abstrak: Dampak akibat dibully adalah depresi berat oleh si remaja korban bullying makin besar bahkan ke arah bunuh diri, menyakiti diri sendiri kepada si anak hasil bully. Tujuan penelitian ini adalah untuk menguraikan desain pola integrasi untuk mengurangi kejahatan cyberbullying. Metode yang digunakan dalam penelitian ini adalah penelitian kualitatif dengan pendekatan deskriptif analitis dan studi kasus. Sasaran subyek penelitian adalah aparat sipil negera, pegawai dan staf yang pada Kepolisian Daerah, Kemenkominfo, Telkom dan Pengadilan Negeri di Nusa Tenggara Barat metode pengumpulan data menggunakan studi kepustakaan, pengamatan, wawancara, analisis dokumen. Desain formulasi pola integrasi cyber dalam penelitian ini menggunakan desain grounded theory menurut Urguhard. Data yang terkumpul baik berupa data kepustakaan maupun data lapangan akan dianalisis dengan menggunakan deskriptif analitis untuk menguraikan data lapangan dengan studi literatur dengan pendekatan deduktif dan induktif. Hasil penelitian menunjukkan bahwa pola integrasi cyber untuk pencegahan cyberbullying menggunakan sistem siklus cyber dengan tahapan yaitu kolaborasi lembaga, pencegahan melalui penyuluhan, edukasi, kampanye dan pendampingan (PEKP), Patroli Siber, menjaga identitas, menjadi saksi ahli, mengklarifikasi berita hoax menjadi berita yang asli, dan memberikan efek jera kepada pelaku kejahatan cyberbullying.

Abstract: *The impact of being bullied is that the teenager who is bullied suffers from severe depression, even leading to suicide, hurting himself or herself to the child who is the result of being bullied. The purpose of this study is to describe the design of integration patterns to reduce cyberbullying crimes. The method used in this research is qualitative research with descriptive analytical approach and case studies. The target subjects of the study were state civil servants, employees and staff at the Regional Police, the Ministry of Communication and Informatics, Telkom and the District Court in West Nusa Tenggara. The data collection methods used were library research, observation, interviews, and document analysis. The design of the cyber integration pattern formulation in this study uses a grounded theory design according to Urguhard. The data collected in the form of library data and field data will be analyzed using analytical descriptive to describe the field data by studying literature with deductive and inductive approaches. The results show that the cyber integration pattern for cyberbullying prevention uses a cyber cycle system with stages, namely institutional collaboration, prevention through counseling, education, campaigns and mentoring (PEKP), Cyber Patrol, maintaining identity, being an expert witness, clarifying hoax news into original news. , and provide a deterrent effect to perpetrators of cyberbullying crimes.*

A. LATAR BELAKANG

Cyberbullying merupakan tindakan yang dapat dilakukan secara fisik (memukul, menendang, mendorong), verbal (menggoda, mengancam), atau relasional (pengucilan social, merusak persahabatan dan menyebarkan rumor)[1]. Kementerian Pemberdayaan Perempuan dan Perlindungan Anak melaporkan 6 persen atau sekitar 5,2 juta anak dari seluruh jumlah anak di Indonesia yang mencapai 87 juta menjadi korban kekerasan dalam berbagai aspek termasuk korban bullying. Dampak akibat dibully adalah depresi berat oleh si remaja korban bullying makin besar bahkan ke arah bunuh diri, menyakiti diri sendiri kepada si anak hasil bully[2]. KPAI melaporkan ada 37.381 pengaduan kekerasan terhadap anak, untuk bullying baik di pendidikan maupun sosial media, angkanya mencapai 2.473 laporan dan trennya terus meningkat[3].

Berbagai penelitian tentang pola integrasi cyber di media sosial, diantaranya[4] menemukan bahwa pencegahan cyberbullying dilakukan beberapa stakeholder yaitu: 1) Orangtua: perlu banyak meluangkan waktu bersama anak mereka, mengawasi

pergaulan sosial anak di media sosial, mengenali dan membantu mengembangkan minat dan bakat anak, memberikan penanaman nilai moral kepada anak dengan menjadi contoh yang baik di keluarga. 2) Pemerintah: Dirjen Rehabilitasi Sosial Anak Kemensos RI dapat mengadakan penyuluhan terhadap orangtua dan guru mengenai cara menanggulangi cyberbullying, meningkatkan peran serta kapasitas pekerja sosial dalam pendampingan korban cyberbullying, membuat panduan khusus bagi orangtua tentang cara mencegah cyberbullying, bersama instansi terkait membuat perangkat hukum/perundang-undangan terkait penanggulangan cyberbullying. 3) Guru: memberikan arahan kepada siswa cara menggunakan internet secara positif, mengoptimalkan kegiatan berbasis lingkungan, meningkatkan kinerja guru bimbingan konseling dengan memonitoring dan self-asessment terhadap siswa. Langkah pencegahan Cyberbullying yang perlu dilakukan adalah sosialisasi UU ITE dan etika berinternet yang disebut 'PIKIR' yaitu Penting, Informatif, Kebaikan, Inspiratif, dan Realitas[5]. Sementara ada tujuh bentuk perundungan siber yaitu flaming (pertengkaran daring), harassment (pelecehan), denigration (ftnah), impersonating (akun palsu), trickery (tipu daya), exclusion (pengucilan), dan cyberstalking (penguntitan siber). Di Indonesia, ditemukan tiga objek perundungan siber selain pada individu yaitu wilayah, agama, dan institusi atau profesi tertentu.

James & Yuono menjelaskan bahwa pusat pencegahan cyberbullying, sebagai wadah edukasi baru dengan penggunaan Virtual Reality, sebagai bentuk simulasi dampak cyberbullying dengan harapan terciptanya kesadaran dan partisipasi publik bagi para remaja dan orang dewasa atas bahaya Cyberbullying, untuk saling bertukar pikiran dalam bentuk Community Center[6]. Lainnya juga menjelaskan program empati yang dapat di terapkan yaitu "Media Heroes" ("Medienhelden") program ini berupa kurikulum pembelajaran yang membahas mengenai empati dan efektif dalam pengendalian empati remaja sebagai pengamat terhadap cyberbullying[7]. Kebijakan penanggulangan cyber bullying dengan hukum pidana termasuk bidang penal policy yang merupakan bagian dari criminal policy (kebijakan penanggulangan kejahatan). Dilihat dari sudut criminal policy, upaya penanggulangan tindakan cyber bullying tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistematik. Upaya penanggulangan cyber bullying juga harus ditempuh dengan pendekatan teknologi (techno prevention). Disamping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global (kerja sama internasional) [8].

Hasil studi Sakban menunjukkan bahwa etika berinternet, peran orang tua harus lebih intensif mengawasi perkembangan anaknya terhadap pengaruh media internet, aparat sipil kepolisian rutin melakukan kampanye "anti bullying" (stop bully) di sekolah, kampus/instansi dan masyarakat, dan melibatkan organisasi social untuk mengawasi peredaran kejahatan cyberbullying. Cara mencegah dan mengurangi berbagai tindakan bullying di media sosial dapat memaksimalkan sikap etika berinternet, peningkatan peran orang tua lebih intensif, pihak kepolisian rutin melakukan kegiatan sosialisasi dan penyuluhan anti bullying, dan organisasi social[9]. Hasil penelitian Sakban lainnya menunjukkan bahwa peran polisi dalam mengurangi dan mencegah kejahatan cyber-bullying di Indonesia, dapat dilakukan dengan langkah-langkah sebagai berikut: 1) sosialisasi ke institusi pendidikan, institusi, kampus dan masyarakat secara teratur, 2) etika internet, peran Orang tua harus lebih intensif mengawasi perkembangan anak terhadap pengaruh media internet, aparat kepolisian secara rutin melakukan kampanye "anti bullying" (stop bully) di sekolah, kampus / institusi dan komunitas, serta melibatkan organisasi sosial untuk memantau peredaran kejahatan cyber-bullying. Sehingga tindakan preemptive kepolisian dalam melakukan pencegahan cyber-bullying tidak bisa dilakukan sendiri (polisi) tetapi harus gotong royong dengan berbagai pihak terkait[10]. Sakban[11], menjelaskan bahwa kebijakan hukum pidana dalam menyelesaikan kejahatan cyber-bullying dapat terapkan oleh aparat penegak hukum berupa KUHP dan Undang-Undang No. 8 Tahun 2018 tentang Informasi Teknologi Elektronik dengan melihat isi penjelasan pasal demi pasal dan konten kejahatan yang dilakukan oleh pelaku.

Berbagai hasil penelitian pencegahan cyberbullying sebelumnya lebih focus pada aspek pencegahan cyberbullying pada aspek kebijakan hukum dengan melibatkan stake holders, sosialisasi, edukasi baru dengan menggunakan Virtual Reality, program empati dengan nama Media Heroes sebagai pengendali cyberbullying, pendekatan budaya/kultural, moral/edukatif, dan pendekatan global, etika berinternet, peningkatan peran orang tua lebih intensif, pihak kepolisian rutin melakukan kegiatan sosialisasi dan penyuluhan anti bullying, dan organisasi social, preventif polisi dalam pencegahan kejahatan cyber. Sementara penelitian kami lebih fikus pada aspek pola integrasi cyber untuk pencegahan kejahatan cyber bullying. Pola integrasi cyber yang dikembangkan dalam penelitian ini adalah pola integrasi cyber lembaga Negara yaitu Kepolisian, Kemenkominfo, Telkom, dan Pengadilan. Dengan harapan mendapatkan suatu kebijakan cyber security yang dalam implementasinya membutuhkan suatu badan koordinasi yang terintegrasi, kerjasama kuat dan terorganisir. Manurut Karsai dan Sztipanovits[12], menyatakan bahwa pola integrasi cyber merupakan sistem integrasi yang mencakup semua aspek komponen perangkat keras dan perangkat lunak, serta interaksinya, demikian juga Larsen[13], menyatakan bahwa model integrated cyber physical

system dapat menciptakan alat teritegrasi untuk memverifikasi data yang lebih baik dan deteksi dini dari gangguan cyber.

Terjadinya peristiwa tersebut akibat minimnya kontribusi lembaga negara dan perguruan tinggi dalam melakukan pencegahan dan pendidikan cyber. Sehubungan dengan itu, cyberbullying memiliki dampak berbahaya pada remaja, karena kemajuan teknologi, bullying melampaui batas etika komunikasi[1]. Deteksi cyberbullying mencapai 5453 tweet[14]. Di tengah pandemi Covid-19 banyak sekali informasi di media massa hoax, informasi hoax memberikan dampak negatif bagi masyarakat yang masih rendah tingkat literasinya[15]. Hasil observasi menunjukkan bahwa selain permasalahan kejahatan cyberbullying, masalah lain juga yang terjadi adalah kurangnya koordinasi, kerjasama diantara stakeholder dalam melakukan pencegahan kejahatan cyber, kurang optimalnya sistem cyber terintegrasi sebagai alat untuk pencegahan kejahatan cyber bullying di masyarakat, kurangnya sumber daya manusia dalam pencegahan digital.

B. METODE PENELITIAN

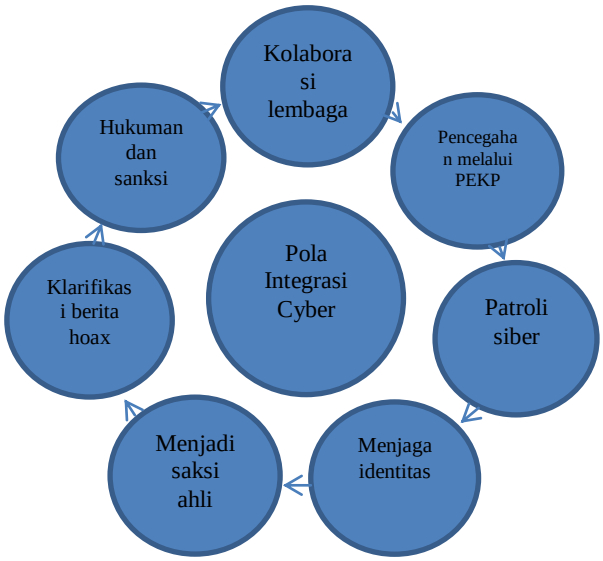
Metode penelitian ini adalah penelitian kualitatif. Pendekatan penelitian yang digunakan pendekatan deskriptif analitis, dan studi kasus. Dimana data dan informasi yang akan dikumpulkan terdiri atas interdisipliner dan multidisipliner serta lintas sektoral, kemudian dianalisis secara deskriptif mendalam. Studi kasus digunakan untuk mengkaji secara mendalam dan intensif satu kelompok sasaran subjek penelitian dengan mengacu kepada fakta materiel berupa orang, tempat, waktu dan segala yang menyertainya tentang cyberbullying.

C. HASIL DAN PEMBAHASAN

Pola integrasi cyber merupakan sistem integrasi yang mencakup semua aspek komponen perangkat keras dan perangkat lunak, serta interaksinya[12]. Model integrated cyber physical system dapat menciptakan alat teritegrasi untuk memverifikasi data yang lebih baik dan deteksi dini dari gangguan cyber[13]. Pembentukan badan tersebut akan meningkatkan kemampuan dalam pengaturan dan penataan lembaga secara terintegrasi[16]. Bagi Indonesia sendiri, kerja sama melalui wadah institusi nasional maupun internasional mengatasi permasalahan keamanan cyber adalah perwujudan dari politik bebas aktif dan menjaga perdamaian dunia[17]. Pola integrasi cyber yang ditemukan dalam penelitian ini adalah pola integrasi cyber lembaga Negara yaitu Kepolisian, Kemenkominfo, Telkom, dan Pengadilan untuk diperlukan suatu kebijakan cyber security yang dalam implementasinya membutuhkan suatu badan koordinasi.

Pola integrasi cyber untuk pencegahan cyberbullying merupakan kolaborasi beberapa lembaga Negara dalam menyelesaikan, mengawasi dan mencegah terjadinya kejahatan cyber dan isu hoax di media social. Hasil penelitian menunjukkan adanya integrasi cyber dalam mencegah kejahatan cyberbullying dapat membantu kepolisian, masyarakat dan pemerintah dalam menyelesaikan kejahatan-kejahatan di media social, pola integrasi cyber yang dibangun oleh beberapa lembaga seperti kepolisian daerah, kominfo terdekat, PT. Telkom dan pengadilan berkerjasama dalam memberikan bantuan data untuk bahan penyelidikan dalam kasus cyberbullying dan kasus Hoax-19.

Berdasarkan penjelasan Direktur Kriminal Khusus tentang penyelesaian maupun mencagah kejahatan cyberbullying, yaitu sebagai lembaga kepolisian berusaha menyelesaikan kasus kejahatan cyberbullying dengan cara menggunakan aturan yang berlaku yang diatur dalam UU ITE, KUHP yang bermuat kejahatan ITE, dalam proses penyelesaian kejahatan cyberbullying ini menurut kami termasuk kategori Delik Aduan, Delik aduan ini apabila ada yang bersangkutan baik korban maupun pelaku complain dan melaporkan ke pihak kami maka kami akan proses, jika tidak ada maka kasus ini kami tidak akan proses. Secara umum kasus yang banyak terjadi di cyber crime ini adalah kasus penipuan online, pencemaran nama baik, penghinaan, asusila, bullying, pengancaman, ujaran kebencian, berita bohong (Hoax), sementara dalam penyelesaian kasus kejahatan cyber crime baik kejahatan cyberbullying kami berkerjasama dengan mitra kami yaitu Kominfo pusat dan kominfo daerah bagian BSSN dan Cyber serta aplikasi internet dan informasi untuk mendapatkan data riil atau bukti otentik maupun rekam jejak pelaku maupun korban, serta menjadi saksi ahli IT. Mitra lainnya PT. Telkom membantu kami dalam memberikan keterangan saat persidangan untuk menjadi saksi ahli IT, kemudian mitra dengan Pengadilan negeri berfungsi sebagai tempat penyelesaian kasus kejahatan cyber crime mulai SP2HP hingga pemberian keputusan akhir. Berikut gambar pola integrasi cyber, yaitu:



Gambar 1. Dessain Pola Integrasi Cyber untuk Mengurangi Kejhatan Cyberbullying

Pola integrasi cyber untuk pencegahan cyberbullying yaitu

1. Kolaborasi lembaga

Kolaborasi lembaga merupakan suatu kerjasama berbagai lembaga Negara yang ada di pusat dan daerah

seperti Kemenkominfo pusat di Jakarta, kominfo daerah baik kota maupun kabupaten di 10 kabupaten kota yang ada di NTB yang berperan memberikan keterangan ahli maupun data otentik baik pelaku maupun korban. PT. Telkom Indonesia tbk di daerah NTB yang bertugas memberikan penjelasan ahli tentang manfaat alat telekomunikasi sebagai sarana menyampaikan informasi secara cepat, mudah dan praktis melalui keterangan ahli. Kantor Pengadilan Negeri berperan membantu kami dalam penyelesaian kasus apabila kasus tersebut sudah masuk SP2HP untuk dilakukan dalam penyelidikan, pemutusan, dan pemberian sanksi pidana atau dibebaskan.

2. Upaya Pencegahan melalui Penyuluhan, Edukasi, Kampanye dan Pendampingan (PEKP)

Upaya pencegahan melalui penyuluhan, edukasi, kampanye dan pendampingan (PEKP) kepada masyarakat baik melalui media cetak, online maupun secara pendampingan. Penyuluhan dilakukan di instansi sekolah, desa dan tempat-tempat umum dengan melibatkan OKP. Siswa, pelajar, tokoh agama, pemuda dan tokoh adat. Edukasi dilakukan pada lembaga pendidikan baik di SD, SMP, SMA dan perguruan tinggi melalui kegiatan seminar dan lokakarya. Kampanye dilakukan melalui media cetak, media social, online pada lembaga penyiaran radio, TV dan internet dengan gambar stop bullying, stop hoax covid-19. Pendampingan dilakukan kepada korban bullying maupun korban hoax covid-19 dengan memberikan bantuan hukum, social, dan psikoolgi.

3. Melakukan Patroli Siber

Patroli siber merupakan kegiatan yang dilakukan rajia online melalui system program Aplikasi Patroli Siber Polri untuk mengamati, mengawasi perkembangan media social baik facebook, twitter, email, whatshap, line, dan instagram, maupun penggunaan internet lainnya dalam waktu berkala yaitu dalam waktu 3 hari sekali, mingguan, bulanan dan tahunan. Aplikasi Patroli Siber Polri ini berkerja selama 24 jam/hari dengan tujuan mengidentifikasi berita hoax, penipuan online, pencemaran nama baik, pelecehan seksual, ujaran kebencian, bullying, ujaran kebencian yang dilakukan masyarakat baik akun pribadi maupun akun kelompok.

4. Menjaga identitas

Dalam system integrasi cyber tersebut, ada beberapa yang kami lakukan yaitu 1) bekerjasama dengan mitra lembaga Negara seperti Polda dengan Dinas Kominfo terdekat, Polda dengan PT. Telkom, Polda dengan Pengadilan negeri setempat ketiga lembaga tersebut cukup bagus dalam membantu kami dalam menyelesaikan berbagai kasus kejahatan cyberbullying dan hoax covid-19. 2) membantu memberikan informasi secara ilmiah terkait kejahatan cyber crime. 3) menjaga kerahasiaan informasi baik milik pelaku maupun korban. 4) saling memberikan informasi data sesuai dengan kebutuhan dalam proses penyelidikan suatu kasus. 5) memberikan penyuluhan kepada masyarakat baik online maupun ofline. 6) melakukan patrol dengan Aplikasi Patroli Cyber setiap hari. 7) konten kejahatan cyberbullying dan hoax covid-19 dihapus oleh kominfo pusat kemudian diganti dengan berita yang asli misalnya informasi tentang Covid-19.

5. Menjadi saksi ahli

Menjadi saksi ahli dalam persidangan, baik saksi ahli IT dan saksi ahli hukum untuk memberikan keterangan yang ilmiah sesuai permintaan majelis hakim untuk dijelaskan secara konkrit, nyata, fakta sesuai kemampuan ahli tersebut. Dalam penyelesaian suatu kasus tim ahli dilibatkan dalam proses penyelidikan hingga pemutusan denda dan sanksi pada suatu kasus kejahatan baik kejahatan penipuan online, pencemaran nama baik, asusila, ujaran kebencian, cyberbullying dan hoax Covid-19 dengan tujuan memberikan informasi yang valid yang diwakili oleh tenaga ahli sesuai bidang keilmuannya. Selain itu membantu kepolisian dalam penyelidikan kasus kejahatan cyber crime, cyber bullying, hoax maupun kejahatan dunia maya lainnya yaitu memberikan keterangan bersifat ahli dalam bidang jaringan seperti kepunyaan akun, proses akun, kapan, dimana, yang bersangkutan beraksi dengan menggunakan nomor HP dan frame akun yang bersangkutan.

6. Mengklarifikasi berita hoax menjadi berita yang asli

Mengklarifikasi berita hoax menjadi berita yang asli merupakan tugas dan tanggungjawab tim IT di bagian BSSN dan Cyber di instasi pemerintah. Sebagai lembaga pemerintahan wajib memberikan informasi yang valid kepada masyarakat tentang kebijakan pemerintah, masalah ekonomi, social, politik, kesehatan maupun data bantuan social dan kesehatan, data perkembangan Covid-19, data vaksin covid-19 dan lainnya. Untuk menghindari semakin meluasnya berita hoax terkait berita hoax covid-19 tim IT melakukan klarifikasi data dengan cara menggantinya dengan berita yang valid sesuai unsur informasi yang disebarkan di media social baik website, watshap, blogspot maupun lainnya. Adapun hal-hal yang sering dilakukan perbaikan data yang kebenarannya dapat dipertanggungjawabkan sumber keasliannya yaitu kebijakan pemerintah, data jumlah bantuan sosial, data korban covid-19, data asal muasal Covid-19, dan vaksinasi covid-19.

7. Memberikan efek jera kepada pelaku kejahatan cyberbullying dan hoax covid-19

Memberikan efek jera kepada pelaku kejahatan cyberbullying dan hoax covid-19 di media social, telah diatur dalam ketentuan hukum, undang-undang maupun KUHP berkaitan dengan kejahatan ITE. Hal tersebut diatur dalam undang-undang No 2 tahun 2002 tentang Kepolisian Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang digunakan untuk menindaklanjuti atau mengadili pelaku tindak pidana cyber crime, Undang-Undang Nomor 1 Tahun 2006 Tentang Bantuan Timbal Balik Dalam Masalah Pidana, Kitab Undang-undang Hukum Pidana, dan Undang-Undang Nomor 1 Tahun 1979 Tentang Ekstradisi.

Dasar hukum penggunaan teknologi dan informatika elektronik tercantum dalam undang-undang nomor 11 tahun 2008 pada pasal 1:

> Ayat (1)
> "Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf,

tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."

Ayat (2)
"Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya."

Ayat (3)
"Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi"

Ayat (4)
Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Ayat (5)
Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Ayat (6)
Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

Ayat (7)
Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.

Ayat (8)
Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk
melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.

Ayat (18)
Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.

Ayat (19)
Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

Pasal 5
Ayat (1)
Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Ayat (2)
Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah
sesuai dengan Hukum Acara yang berlaku di Indonesia.

Ayat (3)
Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Ayat (5)
Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Pasal yang mengatur Penyelenggaraan Sistem Elektronik termuat di Pasal 15
Ayat (1)
Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

Ayat (2)
Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

Ayat (3)
Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal yang mengatur perbuatan yang dilarang termuat di Pasal 27, 28, 29, 30, 31, 32, 33, 34, 35, 36 dan 37.
Pasal 27
Ayat (1)
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.

Ayat (3)
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 penghinaan dan/atau pencemaran nama baik.

Ayat (4)
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 pemerasan dan/atau pengancaman.

Pasal 28
Ayat (1)
Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Ayat (2)
Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Pasal 29
Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal 30
Ayat (1)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

Ayat (2)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Ayat (3)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pasal 31
Ayat (1)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

Ayat (2)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Ayat (3)
Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

Ayat (4)
Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 32
Ayat (1)
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.

Ayat (2)
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

Ayat (3)
Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Pasal 34
Ayat (1)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Ayat (2)
Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Pasal 35
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pasal 36
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Pasal 37
Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Surat Edaran Hate Speech Kepolisian Republik Indonesia Nomor : SE/6/X/2015 tentang penanganan ujaran kebencian (hate speech). Dalam surat edaran Kapolri tersebut, penjelasan terhadap kejahatan cyber bullying termuat dalam huruf (f) yang berbunyi "bahwa ujaran kebencian dapat berupa tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan ketentuan pidana lainnya di luar KUHP, yang berbentuk antara lain:

1) penghinaan;
2) pencemaran nama baik;
3) penistaan;
4) perbuatan tidak menyenangkan;
5) memprovokasi;
6) menghasut;
7) penyebaran berita bohong;

dan semua tindakan di atas memiliki tujuan atau bisa berdampak pada tindak diskriminasi, kekerasan, penghilangan nyawa, dan/atau konflik sosial; sedangkan huruf (f) bahwa ujaran kebencian sebagaimana dimaksud di atas, bertujuan untuk menghasut dan menyulut kebencian terhadap individu dan/atau kelompok masyarakat dalam berbagai komunitas yang dibedakan dari aspek:

1) suku;
2) agama;
3) aliran keagamaan;
4) keyakinan/kepercayaan;
5) ras;
6) antargolongan;
7) warna kulit;
8) etnis;
9) gender;
10) kaum difabel (cacat);
11) orientasi seksual;

Huruf (H) bahwa ujaran kebencian (hate speech) sebagaimana dimaksud di atas dapat dilakukan melalui berbagai media, antara lain:

1) pamflet;
2) media massa cetak maupun elektronik;
3) ceramah keagamaan;
4) penyampaian pendapat di muka umum (demonstrasi);
5) jejaring media sosial;
6) spanduk atau banner.

Kitab Undang-Undang Hukum Pidana (KUHP) (Pasal 156, Pasal 157) untuk menjerat pelaku dugaan ujaran kebencian

KUHP Pasal 156 berbunyi:

"Barang siapa di depan umum menyatakan perasaan permusuhan, kebencian atau merendahkan terhadap satu atau lebih suku bangsa Indonesia dihukum dengan hukuman penjara selama-Iamanya empat tahun dengan hukuman denda setinggitingginya empat ribu lima ratus rupiah,""

KUHP Pasal 157 berbunyi:

"(1) Barang siapa menyiarkan, mempertunjukkan atau menempelkan tulisan atau lukisan di muka umum, yang isinya mengandung pernyataan perasaan permusuhan, kebencian atau penghinaan di antara atau terhadap golongan-golongan rakyat Indonesia, dengan maksud supaya isinya diketahui atau lebih diketahui oleh umum, diancam dengan pidana penjara paling lama dua tahun enam bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Jika yang bersalah melakukan kejahatan tersebut pada waktu menjalankan pencariannya dan pada saat itu belum lewat lima tahun sejak pemidanaannya menjadi tetap karena kejahatan semacam itu juga, yang bersangkutan dapat dilarang menjalankan pencarian tersebut."

Pasal310 KUHP, yang berbunyi:

"(1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembiIan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(3) Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri."

Pasal 311 KUHP, yang berbunyi:
"(1) Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun.
(2) Pencabutan hak-hak berdasarkan Pasal 35 No. 1-3 dapat dijatuhkan."

Pasal 28 jis. Pasal 45 ayat (2) UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi:
Pasal 28:
"(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA)."

Pasal 45 ayat (2):
"(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,OO(satu miliar rupiah)."

Pasal 16 UU Nomor 40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis, yang berbunyi:
Pasal16:
"Setiap orang yang dengan sengaja menunjukkan kebencian atau rasa benci kepada orang lain berdasarkan diskriminasi ras dan etnis sebagaimana dimaksud dalam Pasal 4 huruf b angka 1, angka 2, atau angka 3, dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)."

Jadi dengan demikian pola integrasi cyber untuk pencegahan kejahatan cyberbullying dan hoax Covid-19 di Nusa Tenggara Barat dapat dilakukan dengan kegiatan yaitu kolaborasi lembaga, upaya pencegahan melalui penyuluhan, edukasi, kampanye dan pendampingan (PEKP), melakukan patroli siber, menjaga identitas lembaga, menjadi saksi ahli, mengklarifikasi berita hoax menjadi berita yang asli, dan memberikan efek jera kepada pelaku kejahatan cyberbullying dan hoax covid-19 mengacu pada undang-undang nomor 11 tahun 2008 pasal 1 ayat 1 – ayat 19, pasal 5 ayat 1 – ayat 5., pasal 15 ayat 1 – ayat 3, pasal 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, dan 37 masing-masing terdapat dalam ayat 1 – ayat 3. Disamping itu juga, dipergunakan juga pada Surat Edaran Hate Speech Kepolisian Republik Indonesia Nomor : SE/6/X/2015 tentang penanganan ujaran kebencian (hate speech). Dalam surat edaran Kapolri tersebut, penjelasan terhadap kejahatan cyber bullying termuat dalam huruf (f) yang berbunyi "bahwa ujaran kebencian dapat berupa tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan ketentuan pidana lainnya di luar KUHP. Kemudian KUHP pada pasal 156 dan Pasal 157.

D. SIMPULAN DAN SARAN

Pola integrasi cyber untuk pencegahan cyberbullying menggunakan sistem siklus cyber dengan tahapan yaitu kolaborasi lembaga, pencegahan melalui penyuluhan, edukasi, kampanye dan pendampingan (PEKP), Patroli Siber, menjaga identitas, menjadi saksi ahli, mengklarifikasi berita hoax menjadi berita yang asli, dan memberikan efek jera kepada pelaku kejahatan cyberbullying.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Muhammadiyah Mataram yang telah membiayai kegiatan penelitian ini, dan terima kasih kepada Direktorat Kriminal Khusus Polda NTB, Dinas Kominfo NTB, PT Telkom Mataram yang telah memberikan data penelitian, sehingga proses pelaksanaan penelitian ini berjalan dengan tepat waktu dan lancar.

DAFTAR RUJUKAN

[1] J. Chun, J. Lee, J. Kim, and S. Lee, "An international systematic review of cyberbullying measurements," *Comput. Human Behav.*, p. 106485, 2020.
[2] F. D. Wulandari, "Dampak Kekerasan Anak di Medsos Akibat Cyber Bullying," *http//lppm.unpam.ac.id/, diakses 20 Oktober 2020*, 2020.

[3] T. KPAI, "Sejumlah Kasus Bullying Sudah Warnai Catatan Masalah Anak di Awal 2020," *Artik.*, 2020.
[4] R. Syah and I. Hermawati, "Upaya pencegahan kasus cyberbullying bagi remaja pengguna media sosial di Indonesia," *J. Penelit. Kesejaht. Sos.*, vol. 17, no. 2, pp. 131–146, 2018.
[5] R. Rastati, "Bentuk Perundungan Siber di Media Sosial dan Pencegahannya Bagi Korban dan Pelaku," *J. Sosioteknologi*, vol. 15, no. 2, pp. 169–185, 2016.
[6] B. James and D. Yuono, "Pusat Pencegahan Cyberbullying: Pencegahan Cyberbullying Melalui Karya Arsitektur," *J. Sains, Teknol. Urban, Perancangan, Arsit.*, vol. 1, no. 2, pp. 1359–1372, 2020.
[7] S. Berlian, "Literature Review: Manajemen Empati Sebagai Program Pencegahan Cyberbullying Pada Remaja." Disertasi Universitas Andalas, 2020.
[8] F. L. Mufid, "Kebijakan Integral Hukum Pidana dengan Technology Prevention dalam Upaya Pencegahan Kejahatan Cyberbullying," *J. Rechtens*, vol. 7, no. 2, pp. 229–246, 2018.
[9] A. Sakban, S. Sahrul, A. Kasmawati, and H. Tahir, "The Role of Police to Reduce and Prevent Cyber-bullying Crimes in Indonesia," in *1st International Conference on Indonesian Legal Studies (ICILS 2018)*, 2018.
[10] A. Sakban, S. Sahrul, A. Kasmawati, and H. Tahir, "Tindakan Bullying di Media Sosial dan Pencegahannya," *JISIP J. Ilmu Sos. dan Pendidik.*, vol. 2, no. 3, 2018.
[11] H. Sakban, A., Sahrul, S., Kasmawati, A., & Tahir, "Police preventative against cyber-bullying crimes in indonesia," *Int. J. Sci. Technol. Res.*, vol. 8, no. 12, pp. 1532–1534, 2019.
[12] G. Karsai and J. Sztipanovits, "Model-integrated development of cyber-physical systems," in *IFIP International Workshop on Software Technolgies for Embedded and Ubiquitous Systems*, 2008, pp. 46–54.
[13] P. G. Larsen *et al.*, "Integrated tool chain for model-based design of Cyber-Physical Systems: The INTO-CPS project," in *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, 2016, pp. 1–6.
[14] V. Balakrishnan, "Actions, emotional reactions and cyberbullying – From the lens of bullies, victims, bully-victims and bystanders among Malaysian young adults," *Telemat. Informatics*, vol. 35, no. 5, pp. 1190–1200, 2018.
[15] H. Chumairoh, "Ancaman Berita Bohong di Tengah Pandemi Covid-19," *Vox Popul.*, vol. 3, no. 1, pp. 22–30, 2020.
[16] H. Zaelani, I. W. Midhio, and Y. Reksoprodjo, "Pembangunan Kapasitas Cyber Security di Negara ASEAN: Analisis Komparatif Terhadap Brunei dan Indonesia," *Peperangan Asimetris*, vol. 4, no. 1, 2018.
[17] I. Ramadhan, "Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber," *J. Sos. dan Hum.*, vol. 2, no. 4, pp. 495–508, 2017.