Jurnal Dimensi Hukum

Vol 9 No 11, November 2025
EISSN : 28593895

STRATEGI PENCEGAHAN DAN PENEGAKAN HUKUM POLDA NTB TERHADAP KASUS CYBERPORN DI ERA DIGITAL

Sania Amalina[1], Putri Pertiwi[2], Lalu Abdul Hafiz[3], Ginaya Aulia Wiraguna[4], Edy Herianto[5]
saniaamalina@gmail.com[1], ppertiwi824@gmail.com[2], l.hafiz151004@gmail.com[3], ginayauliawiraguna@gmail.com[4], edyherianto.fkipunram@gmail.com[5]
Universitas Mataram

Abstrak: Penelitian ini bertujuan untuk menganalisis strategi pencegahan dan penegakan hukum yang dilakukan Polda NTB dalam menangani kasus cyberporn di era digital. Fenomena cyberporn di NTB didominasi oleh remaja berusia 15–18 tahun, dengan modus berupa penyebaran konten intim, pemerasan, penggunaan akun anonim, serta manipulasi digital. Penelitian menggunakan pendekatan kualitatif deskriptif melalui wawancara, observasi, dan studi dokumentasi. Hasil penelitian menunjukkan bahwa strategi pencegahan dilakukan melalui penyebaran flyer digital, patroli siber, takedown konten bekerja sama dengan Kominfo, serta sosialisasi langsung ke sekolah dan kampus. Penegakan hukum dilakukan melalui tahapan penyelidikan, penyidikan, hingga pelimpahan perkara ke Kejaksaan, dengan dukungan metode identifikasi offline dan online. Kendala yang dihadapi meliputi akun anonim, bukti digital yang mudah hilang, serta kondisi psikologis korban. Temuan penelitian juga menunjukkan bahwa seluruh upaya penanganan cyberporn berlandaskan nilai-nilai Pancasila, terutama dalam perlindungan korban, kolaborasi lintas lembaga, dan penerapan hukum yang berkeadilan.
Kata Kunci: Cyberporn, Polda Ntb, Penegakan Hukum, Pencegahan, Nilai Pancasila.

Abstract: *This research aims to analyze the prevention strategies and law enforcement efforts implemented by the NTB Regional Police in addressing cyberporn cases in the digital era. Cyberporn incidents in NTB are largely dominated by adolescents aged 15–18, involving modes such as intimate content distribution, extortion, anonymous accounts, and digital manipulation. Using a descriptive qualitative approach, data were collected through interviews, observations, and document analysis. The findings show that prevention strategies include digital flyer dissemination, cyber patrols, content takedown in cooperation with the Ministry of Communication and Informatics, and direct outreach to schools and universities. Law enforcement follows investigation, interrogation, and case submission stages supported by both online and offline identification methods. Challenges include anonymous accounts, volatile digital evidence, and victims' psychological barriers. The study also reveals that all prevention and enforcement efforts are grounded in Pancasila values, particularly in victim protection, interagency collaboration, and fair legal implementation.*
Keywords: *Cyberporn, NTB Police, Law Enforcement, Prevention, Pancasila Values.*

PENDAHULUAN

Perkembangan teknologi digital dalam satu dekade terakhir telah mengubah berbagai aspek kehidupan manusia, termasuk cara berkomunikasi, bekerja, dan berinteraksi di ruang virtual. Kemajuan ini membawa berbagai dampak positif, namun juga memunculkan bentuk-bentuk kejahatan baru yang kompleks dan lintas batas. Salah satu fenomena kejahatan digital yang menjadi perhatian global adalah cyberporn, yaitu aktivitas produksi, distribusi, atau konsumsi konten pornografi melalui media daring dan perangkat digital (Azizah & Marpaung, 2024). Kejahatan ini tidak hanya berkaitan dengan pelanggaran moral atau norma sosial, tetapi juga berdampak pada keamanan digital, martabat manusia, serta melanggar ketentuan hukum yang berlaku (Sa'diyah, 2023).

Tingginya penggunaan internet di Indonesia mencapai 221 juta pengguna pada 2024 (We Are Social, 2024) membuat masyarakat semakin rentan terhadap penyebaran konten pornografi digital. Berdasarkan laporan Kementerian Komunikasi dan Informatika (Kominfo, 2024), lebih dari 2,1 juta situs bermuatan pornografi telah diblokir, namun langkah tersebut belum mampu menekan maraknya kasus cyberporn secara signifikan. Fenomena cyberporn sering muncul dalam bentuk revenge porn, sextortion, dan penyebaran video pribadi tanpa izin melalui media sosial tertutup, yang sebagian besar melibatkan remaja berusia 15–18 tahun (Sa'diyah, 2023; Nuraini & Putra, 2022). Rendahnya literasi digital, lemahnya etika bermedia, serta ketidaktahuan masyarakat mengenai konsekuensi hukum menjadi faktor yang memperburuk situasi ini (Rahman & Yuliani, 2023).

Dari perspektif hukum, Indonesia telah memiliki regulasi yang tegas melalui Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 yang diperbarui melalui UU No. 19 Tahun 2016. Namun, implementasinya masih terkendala oleh keterbatasan sumber daya, kesulitan pelacakan pelaku lintas wilayah, dan integrasi sistem antarinstansi yang belum optimal (Yunita & Pramono, 2023; Lestari, 2023). Kondisi ini menyebabkan penegakan hukum sering berjalan lambat dan tidak memberikan efek jera yang optimal, terutama terhadap korban remaja yang rentan secara psikologis.

Fenomena serupa juga terjadi di Provinsi Nusa Tenggara Barat (NTB). Berdasarkan data Direktorat Reserse Kriminal Khusus Polda NTB (2025), sejak Januari hingga Oktober 2025 telah ditemukan beberapa kasus cyberporn yang melibatkan korban lokal, dengan modus seperti penyebaran video intim, pemerasan berbasis konten seksual, dan penggunaan akun anonim. Banyak pelaku berasal dari luar daerah, sementara korban umumnya remaja yang tinggal di kos atau lingkungan lepas pengawasan orang tua, sehingga lebih mudah terjebak rayuan digital. Kondisi ini menunjukkan bahwa cyberporn memiliki karakter lintas wilayah dan memerlukan kemampuan digital forensik, koordinasi kelembagaan, serta strategi pencegahan yang lebih terstruktur di tingkat daerah (Suharto, 2023).

Berdasarkan tinjauan literatur, sebagian besar penelitian terkait cyberporn di Indonesia menekankan aspek hukum (Rahman & Yuliani, 2023; Yunita & Pramono, 2023) atau psikologi remaja (Nuraini & Putra, 2022), sementara kajian strategi pencegahan dan penegakan hukum secara terintegrasi di tingkat daerah masih terbatas. Konteks lokal penting karena efektivitas kebijakan penegakan hukum sangat dipengaruhi oleh kondisi sosial, budaya, dan kapasitas kelembagaan masing-masing daerah (Usman & Agustanti, 2023). Selain itu, hingga saat ini belum ada penelitian di lingkungan FKIP yang secara langsung menelaah fenomena cyberporn dan mengaitkannya dengan nilai-nilai Pancasila, khususnya sila pertama, padahal hal ini sangat relevan bagi masyarakat NTB yang religius. Pendekatan berbasis nilai ini menjadi kontribusi baru untuk memperkaya literatur

tentang penanganan kejahatan siber di Indonesia, sekaligus menghadirkan perspektif pendidikan dan literasi digital yang sebelumnya kurang diperhatikan dalam studi-studi hukum atau psikologi.

Dengan mempertimbangkan konteks tersebut, penelitian ini bertujuan untuk menganalisis strategi pencegahan cyberporn yang dilakukan oleh Polda NTB, menjelaskan proses penegakan hukum terhadap kasus cyberporn, dan mengidentifikasi penerapan nilai-nilai Pancasila dalam upaya pencegahan dan penegakan hukum. Hasil penelitian diharapkan memberikan kontribusi akademik bagi pengembangan ilmu hukum, pendidikan, dan kebijakan publik, sekaligus memberikan rekomendasi praktis untuk memperkuat kapasitas daerah dalam menghadapi kejahatan siber secara berkeadilan, humanis, dan berlandaskan nilai-nilai Pancasila.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis deskriptif untuk memahami secara mendalam strategi pencegahan dan penegakan hukum terhadap kasus cyberporn di NTB. Pendekatan ini dipilih karena mampu menggali makna, pengalaman, serta proses yang dijalankan aparat kepolisian dalam menangani kejahatan siber (Rofiah & Bungin, 2024). Penelitian dilaksanakan di Direktorat Reskrimsus Polda NTB pada Oktober–Desember 2025. Subjek penelitian terdiri dari anggota Reskrimsus yang terlibat langsung dalam penanganan kasus, dipilih melalui teknik purposive. Objek penelitian mencakup keseluruhan strategi pencegahan dan penegakan hukum terhadap cyberporn di wilayah NTB. Data dikumpulkan melalui wawancara semi-terstruktur, observasi non-partisipan, dan studi dokumentasi berupa laporan serta dokumen pendukung (Education, 2024). Analisis data dilakukan menggunakan model analisis interaktif yang meliputi reduksi data, penyajian data, serta penarikan kesimpulan secara berulang (Rofiah, 2022). Keabsahan data dijamin melalui triangulasi sumber dan metode, serta member check dengan narasumber untuk memastikan akurasi temuan penelitian.

HASIL DAN PEMBAHASAN

Berdasarkan hasil wawancara dengan Unit Siber Polda NTB, diketahui bahwa kasus cyberporn di wilayah NTB secara umum melibatkan kelompok usia remaja, terutama siswa SMP dan SMA dengan rentang usia 15–18 tahun, meskipun terdapat pula kasus yang melibatkan mahasiswa, seperti salah satu kasus terakhir yang diusut yang pelakunya masih berada pada semester lima. Fenomena ini didominasi oleh pelaku laki-laki, dan sebagian besar kasus berawal dari persoalan asmara, seperti kekecewaan, sakit hati, atau hubungan yang berakhir tidak baik sehingga pelaku menyalahgunakan konten pribadi korban. Perkembangan teknologi digital disebut berperan besar dalam meningkatnya kasus cyberporn, terutama karena hadirnya fitur anonim pada Telegram, penggunaan akun palsu, serta teknologi deepfake yang memungkinkan manipulasi wajah korban. Modus yang paling sering ditemukan adalah ancaman dan pemerasan, di mana pelaku menggunakan konten pribadi korban untuk menekan atau mempermalukan mereka. Berdasarkan hasil pemantauan, platform yang paling sering digunakan adalah Instagram dan Facebook, biasanya disebarkan melalui tautan (link) tertentu untuk distribusi atau konsumsi pribadi. Penyebaran konten ini umumnya bertujuan menjatuhkan mental korban dan merusak psikologinya, karena perilaku tersebut dilakukan untuk membuat konten diketahui publik. Adapun wilayah yang paling rawan adalah Kota Mataram, terutama karena banyaknya mahasiswa dan pelajar yang tinggal di kos tanpa pengawasan orang tua. Dalam banyak kasus, korban dirayu atau dibujuk hingga terpengaruh, sehingga pelaku mendapat akses terhadap foto atau percakapan pribadi mereka yang kemudian disalahgunakan.

Hasil wawancara dengan Unit Siber Polda NTB menunjukkan bahwa strategi pencegahan cyberporn dilakukan melalui tiga metode utama, yaitu penyebaran flyer digital, sosialisasi lapangan, dan mekanisme takedown bekerja sama dengan Kominfo. Pertama, penyebaran flyer dilakukan melalui media sosial resmi kepolisian seperti Instagram, yang berisi informasi mengenai modus awal pelaku, cara penyebaran konten, serta bentuk-bentuk kejahatan cyberporn yang perlu diwaspadai masyarakat. Kedua, pencegahan dilakukan melalui sosialisasi langsung ke sekolah dan kampus, mulai dari tingkat SD, SMP, SMA, hingga perguruan tinggi. Unit Siber menjelaskan bahwa sosialisasi ke SD pernah dilakukan karena pada saat itu terdapat kasus cyberporn yang melibatkan anak usia sekolah dasar. Proses sosialisasi bersifat panjang, dimulai dari penyusunan materi sesuai segmentasi usia hingga pendekatan langsung kepada guru dan pihak sekolah. Ketiga, strategi pencegahan dilakukan melalui proses takedown konten, di mana Polda NTB terlebih dahulu melakukan patroli siber harian untuk memantau akun atau unggahan yang mengandung unsur cyberporn. Ketika ditemukan konten pelanggaran, aparat mengirimkan peringatan kepada pemilik akun; jika tetap diabaikan, konten akan diteruskan ke Kominfo untuk ditindaklanjuti dan dihapus. Berdasarkan temuan lapangan, Polda NTB lebih dominan bergerak melalui media online karena dianggap jauh lebih cepat, efisien, dan mampu menjangkau kelompok muda yang aktif di dunia digital. Namun demikian, metode ini dianggap kurang efektif bagi masyarakat yang kurang terbiasa dengan edukasi digital. Untuk memperkuat pencegahan, Polda NTB juga menjalankan program rutin berupa pembuatan himbauan daring serta kegiatan patroli siber yang secara konsisten memantau konten berpotensi pelanggaran. Strategi pencegahan juga dibedakan menurut kelompok usia agar materi yang diberikan relevan dan dapat dipahami, misalnya edukasi yang diberikan kepada siswa SD umumnya berupa pemahaman mengenai jenis ancaman halus di internet, sedangkan untuk SMA penyampaian materi lebih tegas dengan menjelaskan pasal, sanksi, dan konsekuensi hukum. Penegakan aturan berdasarkan Pasal 27 Ayat 1 UU ITE disebut berlaku untuk semua kalangan tanpa pengecualian, bahkan seseorang yang hanya melihat konten pornografi karena rasa ingin tahu atau menyebarkannya kembali tetap dapat diproses secara hukum. Strategi pencegahan ini diperkuat melalui kerja sama dengan Kominfo, guru dan wali kelas, dosen pembimbing, serta institusi pendidikan seperti IPDN dan Universitas Bumigora untuk memperluas jangkauan edukasi.

Hasil wawancara menunjukkan bahwa proses penegakan hukum terhadap kasus cyberporn di Polda NTB selalu dimulai dari laporan korban. Narasumber menjelaskan bahwa hampir semua kasus yang ditangani berasal dari pengaduan langsung masyarakat. Setelah menerima laporan, aparat melakukan koordinasi dengan ahli pidana dan ahli ITE. Prosedur penanganan dimulai dari administrasi penyelidikan, yang meliputi pengumpulan data awal, pemeriksaan saksi-saksi, dan analisis awal untuk mengidentifikasi pihak yang diduga sebagai pelaku. Apabila hasil analisis mengarah pada satu akun atau individu tertentu, proses dilanjutkan pada tahap penyidikan dengan pengumpulan barang bukti, pemeriksaan, interogasi, hingga penetapan tersangka. Setelah berkas perkara disusun, kasus dilimpahkan kepada Kejaksaan untuk melalui tahapan P19–P21 sampai berkas dinyatakan lengkap. Selanjutnya dilakukan tahap II berupa penyerahan tersangka dan barang bukti untuk memasuki proses persidangan.

Dalam proses identifikasi, narasumber menjelaskan bahwa aparat menggunakan metode offline dan online. Pendekatan offline dilakukan melalui koordinasi dengan ketua RT, kepala lingkungan, dan Babinsa, sedangkan pendekatan online dilakukan melalui patroli siber, penelusuran akun Instagram, serta pemeriksaan profil dan aktivitas digital lainnya. Narasumber juga menyebutkan bahwa selain proses pidana, terdapat opsi

penyelesaian melalui mekanisme restorative justice apabila kedua belah pihak menyetujui penyelesaian damai dan korban mencabut laporan.

Terkait kendala, narasumber menyatakan bahwa aparat sering menghadapi penggunaan akun anonim, fake account, bukti digital yang mudah dihapus, serta korban yang tidak menyampaikan informasi secara lengkap. Beberapa korban juga cenderung tidak kooperatif karena kondisi psikologis. Narasumber menambahkan bahwa meskipun demikian, pelaku umumnya tetap dapat ditelusuri melalui celah digital tertentu, seperti riwayat transaksi. Selain itu, korban biasa disarankan menonaktifkan media sosial untuk sementara. Dari sisi administrasi, narasumber menjelaskan bahwa proses penegakan hukum dilaksanakan secara prosedural melalui pemberian surat pemberitahuan perkembangan penyelidikan serta informasi lainnya kepada pelapor.

Berdasarkan wawancara, Polda NTB menjelaskan bahwa strategi pencegahan dan penegakan hukum terkait cyberporn turut berlandaskan nilai-nilai Pancasila. Dalam pelaksanaannya, Polda NTB bekerja sama dengan Kementerian Agama karena NTB dikenal sebagai daerah yang religius, sehingga pendekatan moral dianggap relevan dengan Sila Pertama. Narasumber juga menjelaskan bahwa penerapan nilai-nilai Pancasila dalam konteks ini lebih banyak diarahkan pada pembentukan kesadaran individu, khususnya mengenai pentingnya etika digital. Hal ini meliputi kemampuan masyarakat untuk membedakan mana perilaku yang patut dan tidak patut dilakukan ketika menggunakan media digital.

PEMBAHASAN

1. Strategi Pencegahan Cyberporn Secara Online dan Ofline

a. Strategi Pencegahan Secara Online

Upaya pencegahan cyberporn yang dilakukan Polda NTB melalui pendekatan online menunjukkan bahwa institusi penegak hukum semakin mengadopsi strategi berbasis literasi digital dan manajemen risiko informasi. Berdasarkan hasil wawancara, terdapat empat bentuk utama intervensi online, yaitu penyebaran flyer digital, patroli siber, mekanisme takedown bekerja sama dengan Kominfo, serta pembuatan himbauan melalui media sosial. Keempat strategi ini tidak berdiri sendiri, tetapi saling melengkapi dalam membangun ekosistem keamanan digital di kalangan masyarakat NTB, khususnya kelompok usia remaja yang paling banyak terlibat dalam kasus cyberporn.

Penyebaran flyer digital melalui akun resmi kepolisian, seperti Instagram, merupakan bentuk kampanye literasi digital yang berfokus pada peningkatan awareness mengenai modus, risiko, dan konsekuensi hukum cyberporn. Strategi ini sejalan dengan temuan penelitian Helmiawan et al. (2025) yang menegaskan bahwa kesadaran siber masyarakat sangat dipengaruhi oleh paparan informasi yang mudah diakses, visual, dan disebarkan melalui platform digital tempat pengguna aktif berinteraksi. Dengan demikian, flyer digital berfungsi sebagai saluran komunikasi risiko yang menjangkau kelompok sasaran paling rentan, terutama pelajar dan mahasiswa yang menghabiskan sebagian besar waktu mereka di media sosial. Namun, efektivitas strategi ini tetap bergantung pada seberapa jauh masyarakat memproses pesan tersebut notifikasi cepat dan gaya konsumsi informasi visual sering membuat edukasi digital bersifat dangkal jika tidak ditindaklanjuti dengan program lain yang lebih mendalam.

Patroli siber menjadi langkah kedua yang memiliki orientasi deteksi dini (early detection). Melalui pemantauan rutin terhadap akun, unggahan, dan tautan berpotensi melanggar, Polda NTB berupaya mencegah penyebaran konten cyberporn sejak tahap awal. Pendekatan ini konsisten dengan literatur mengenai human factor dalam keamanan siber yang menyebutkan bahwa ancaman digital sering “terlihat” terlebih dahulu melalui aktivitas online yang tidak normal (Alghamdi, 2022). Patroli siber memungkinkan aparat

mengidentifikasi pola distribusi konten, akun anonim, atau penggunaan fitur komunikasi tertutup seperti Telegram yang banyak disebut dalam temuan lapangan. Tantangannya adalah sifat anonimitas platform digital, kecepatan penyebaran konten, dan kemampuan pelaku menghapus jejak digital secara instan faktor yang juga disorot oleh Tsauri (2025) dalam studinya mengenai kerentanan manusia terhadap rekayasa sosial dan kejahatan siber.

Strategi ketiga, yaitu takedown konten, dilakukan melalui sinergi antara Polda NTB dan Kominfo. Proses ini dimulai dari pengiriman peringatan kepada pemilik akun, dan jika tidak ditindaklanjuti, konten diteruskan ke Kominfo untuk dihapus. Strategi ini mencerminkan model kolaboratif yang umum digunakan dalam penanganan kejahatan siber, di mana aparat penegak hukum membutuhkan otoritas pengelola infrastruktur digital untuk melakukan intervensi teknis. Penelitian Saridewi & Sari (2024) menegaskan bahwa penguatan aspek keamanan digital tidak dapat dilakukan hanya oleh aparat kepolisian, tetapi memerlukan kolaborasi lintas lembaga, khususnya pada kasus yang melibatkan konten daring yang beredar cepat. Dalam konteks NTB, takedown juga memiliki fungsi preventif sekunder, yaitu mengurangi potensi trauma psikologis korban akibat penyebaran konten secara masif.

Selain ketiga strategi tersebut, himbauan digital menjadi instrumen edukasi yang lebih persuasif dan berkelanjutan. Dibanding flyer yang informatif dan patroli siber yang bersifat teknis, himbauan di media sosial berfungsi membangun kesadaran moral mengenai etika digital, batasan perilaku, dan bahaya manipulasi digital seperti deepfake yang kini semakin banyak disebut dalam kasus cyberporn. Himbauan digital juga memungkinkan Polda NTB menyampaikan pesan yang sesuai dengan konteks lokal, budaya religius NTB, serta nilai-nilai Pancasila yang menekankan etika, tanggung jawab, dan penghormatan terhadap martabat manusia. Ini sesuai dengan temuan Helmiawan et al. (2025) bahwa kesadaran keamanan siber lebih berhasil bila dikaitkan dengan nilai-nilai sosial tempat masyarakat berada.

Secara keseluruhan, keempat strategi online Polda NTB menunjukkan pendekatan pencegahan berlapis (multi-layered prevention), mulai dari edukasi (flyer & himbauan), deteksi (patroli), hingga intervensi langsung (takedown). Model ini sejalan dengan pendekatan yang direkomendasikan dalam berbagai studi keamanan digital yang menekankan bahwa pencegahan kejahatan siber tidak dapat hanya mengandalkan penindakan hukum, tetapi harus membangun ekosistem keamanan digital yang berfokus pada peningkatan literasi, monitoring berkelanjutan, dan respons cepat (Alghamdi, 2022; Tsauri, 2025). Kendati demikian, masih terdapat tantangan, terutama dari sisi anonimitas pelaku, kecepatan penyebaran konten, serta variasi tingkat literasi digital masyarakat. Namun, keberadaan strategi online yang menyasar kelompok usia termuda menunjukkan bahwa Polda NTB telah mengarahkan upaya pencegahan ke kelompok yang paling rentan, sehingga intervensi ini memiliki potensi signifikan dalam menekan kasus cyberporn di wilayah NTB.

b. Strategi Pencegahan Cyberporn Secara Ofline

Strategi pencegahan yang dilakukan secara offline oleh Polda NTB berfokus pada upaya membangun kesadaran hukum dan moral masyarakat melalui interaksi langsung, dengan prioritas sasaran anak, remaja, dan mahasiswa yang selama ini menjadi kelompok paling rentan terlibat dalam kasus cyberporn. Hasil wawancara menunjukkan bahwa pendekatan offline dianggap penting karena tidak semua kelompok masyarakat memiliki literasi digital yang memadai, sehingga diperlukan metode edukasi yang memungkinkan penjelasan lebih detail dan komunikasi dua arah yang tidak dapat diperoleh melalui media daring. Dalam konteks penelitian kriminologi, strategi offline ini sejalan dengan konsep

situational crime prevention yang menekankan pada pengurangan peluang terjadinya kejahatan melalui peningkatan pengetahuan, kewaspadaan, dan pengawasan sosial (Clarke, 1997).

Penyuluhan dan sosialisasi tatap muka menjadi metode yang paling dominan dilakukan. Kegiatan ini mencakup kunjungan ke sekolah dari tingkat SD hingga SMA, serta ke perguruan tinggi ketika ditemukan kasus yang melibatkan mahasiswa. Pendekatan ini konsisten dengan temuan literatur yang menunjukkan bahwa intervensi berbasis penyuluhan mampu meningkatkan kesadaran risiko digital dan memperkuat kemampuan individu dalam mengenali tanda-tanda awal ancaman seperti grooming, sextortion, maupun manipulasi digital (Helmiawan et al., 2025). Sosialisasi tatap muka juga memberi ruang bagi peserta untuk bertanya langsung dan menyampaikan pengalaman, sehingga menghasilkan edukasi yang lebih personal dan relevan. Selain itu, penyampaian materi disesuaikan dengan tingkat usia, sebagaimana direkomendasikan dalam studi edukasi digital oleh Livingstone et al. (2022), sehingga efektivitas penyampaian informasi meningkat.

Selain penyuluhan, strategi offline juga dilakukan melalui kerja sama dengan sekolah, pemerintah desa, dan tokoh masyarakat. Kolaborasi ini merupakan implementasi dari pendekatan community-based policing, yaitu model pencegahan kejahatan yang melibatkan berbagai aktor lokal untuk menciptakan lingkungan sosial yang lebih aman dan berdaya tangkal tinggi terhadap kejahatan siber (Skogan, 2022). Di tingkat sekolah, kerja sama meliputi penyusunan materi literasi digital, pembentukan budaya pengawasan, serta pemberdayaan guru untuk memberikan pendampingan ketika potensi ancaman muncul. Sementara itu, di tingkat komunitas, tokoh desa dan tokoh agama difungsikan sebagai mediator moral yang membantu memperluas jangkauan edukasi. Pendekatan kolaboratif ini sudah lama dipandang efektif dalam mencegah kejahatan yang bersifat sosial dan berulang, karena keberhasilan program tidak hanya bergantung pada polisi, tetapi juga dukungan lingkungan sekitar (Mazerolle & Ransley, 2023).

Penindakan lapangan juga menjadi bagian dari strategi pencegahan offline, terutama ketika terdapat indikasi produksi atau distribusi konten pornografi yang dilakukan di dunia nyata tetapi disebarluaskan melalui media digital. Hasil wawancara menunjukkan bahwa aparat tetap melakukan operasi lapangan untuk memastikan bahwa kegiatan-kegiatan yang berpotensi menghasilkan konten ilegal dapat dihentikan sebelum diedarkan lebih luas. Langkah ini sejalan dengan teori deterrence, yang mengemukakan bahwa penegakan hukum yang tegas dan terlihat mampu menurunkan niat pelaku karena meningkatnya persepsi risiko tertangkap (Becker, 1968). Selain itu, penindakan langsung di lapangan terbukti efektif dalam menghentikan sumber produksi konten, terutama ketika bukti digital dapat dengan mudah dihapus atau dimanipulasi oleh pelaku.

Secara keseluruhan, strategi pencegahan offline yang dilakukan Polda NTB bersifat komprehensif karena menggabungkan pendekatan edukatif, kolaboratif, dan represif. Analisis ini menegaskan bahwa pencegahan yang efektif tidak hanya bergantung pada teknologi digital, tetapi juga pada kualitas interaksi sosial dan kapasitas masyarakat dalam memahami serta merespons ancaman cyberporn. Pendekatan offline ini juga memperjelas bahwa keberhasilan strategi pencegahan sangat ditentukan oleh sejauh mana aparat mampu membangun komunikasi yang kuat dengan masyarakat serta menciptakan ekosistem pengawasan yang berlapis.

2.Penegakan Hukum Terhadap Kasus Cyberporn

Penegakan hukum terhadap kasus cyberporn di Polda NTB menunjukkan bahwa proses penanganan perkara selalu dimulai dari adanya laporan korban. Temuan ini sesuai dengan pola complaint-based enforcement yang banyak digunakan pada kejahatan siber.

Hanum & Prasetyo (2022) menyebutkan bahwa mayoritas penanganan cybercrime di Indonesia memang bergantung pada laporan korban karena sulitnya deteksi mandiri oleh aparat. Hal ini diperkuat oleh riset Wijaya & Yusuf (2021) yang menjelaskan bahwa sebagian besar kejahatan seksual digital berlangsung dalam ruang privat, sehingga aparat hanya dapat bertindak setelah adanya aduan. Dengan demikian, yang terjadi di Polda NTB menunjukkan bahwa mekanisme awal yang digunakan sudah sejalan dengan karakteristik kejahatan digital yang sulit terlihat tanpa adanya pelapor.

Tahap penyelidikan dilakukan dengan mengumpulkan data awal, meminta klarifikasi saksi, dan menganalisis bukti digital untuk menentukan apakah sebuah laporan layak dinaikkan ke penyidikan. Analisis ini penting karena bukti digital bersifat mudah hilang, mudah dimodifikasi, dan membutuhkan metode khusus dalam pengujiannya. Penjelasan ini sejalan dengan Wijayanto & Sari (2021) yang menegaskan bahwa bukti digital harus diproses secara cepat karena memiliki tingkat volatilitas tinggi. Temuan serupa disampaikan oleh Hakim & Sutanto (2022), yang menjelaskan bahwa proses penyelidikan cybercrime sangat dipengaruhi kualitas bukti awal yang disampaikan korban. Dengan demikian, prosedur penyelidikan yang diterapkan Polda NTB mampu mencerminkan standar forensik digital yang diakui dalam literatur.

Pada tahap penyidikan, penyidik melakukan penyitaan barang bukti digital, pemeriksaan saksi, analisis akun, hingga penetapan tersangka. Prosedur ini mengikuti prinsip due process of law. Sasmita (2023) menjelaskan bahwa penanganan cybercrime harus mematuhi tata kelola administrasi penyidikan agar setiap temuan dapat dipertanggungjawabkan di pengadilan. Selain itu, penelitian Kurniawan & Lestari (2022) menunjukkan bahwa penyidikan kasus cyberporn harus dilakukan dengan memastikan chain of custody bukti digital terjaga. Praktik ini terlihat dalam mekanisme di Polda NTB, terutama ketika berkas perkara dilimpahkan melalui proses P19–P21 sebagai bentuk validasi materi penyidikan.

Proses identifikasi pelaku memadukan metode offline dan online. Secara offline, aparat melakukan koordinasi dengan ketua RT, kepala lingkungan, dan Babinsa guna menelusuri identitas fisik pelaku. Langkah ini konsisten dengan temuan Aribowo (2021) yang menyebutkan bahwa community intelligence tetap menjadi pilar penting dalam investigasi cybercrime di daerah. Sementara secara online, penyidik memanfaatkan patroli siber, analisis akun Instagram, metadata, dan percakapan digital. Pendekatan hybrid ini sejalan dengan Putra (2022) yang menegaskan bahwa investigasi siber tidak efektif jika hanya mengandalkan penelusuran digital tanpa dukungan sosial. Diperkuat pula oleh penelitian Marzuki & Fadilah (2021), yang menyatakan bahwa integrasi strategi offline-online meningkatkan peluang mengidentifikasi pelaku yang menggunakan akun anonim atau VPN.

Dalam penanganan kasus cyberporn, aparat menghadapi berbagai hambatan seperti akun anonim, penggunaan VPN, bukti digital yang cepat hilang, serta korban yang belum siap memberikan keterangan. Nurdin & Septian (2020) menjelaskan bahwa bukti digital pada kasus seksual daring termasuk jenis yang paling rentan hilang karena sifatnya yang tidak stabil. Hal ini juga didukung oleh studi Rachman & Hidayat (2021) yang menemukan bahwa pelaku kejahatan digital sering memanfaatkan platform dengan enkripsi kuat yang menyulitkan penyidik memperoleh data. Faktor hambatan psikologis korban juga disebutkan dalam penelitian Sari & Maulida (2022), yang menyatakan bahwa rasa malu dan trauma membuat korban cyberporn cenderung enggan memberikan detail kasus. Hambatan-hambatan ini menunjukkan bahwa penyidikan cyberporn memerlukan peningkatan kapasitas teknis dan dukungan pendampingan psikologis terhadap korban.

Selain jalur pidana, Polda NTB juga membuka opsi penyelesaian melalui restorative

justice jika korban setuju dan mencabut laporan. Pendekatan ini selaras dengan Perpol No. 8/2021, dan dalam literatur dinilai efektif dalam kasus tertentu yang melibatkan relasi dekat. Braithwaite (2023) menjelaskan bahwa RJ dapat memulihkan hubungan sosial tanpa harus melalui jalur pemidanaan yang panjang. Namun, sejumlah ahli seperti Ramadhan (2023) memperingatkan bahwa RJ harus diterapkan secara hati-hati dalam kasus kejahatan seksual digital karena dikhawatirkan mengurangi efek jera. Sementara penelitian Yuliani & Said (2022) menekankan bahwa RJ hanya layak digunakan jika tidak ada unsur eksploitasi berat. Dengan demikian, keputusan Polda NTB untuk menerapkan RJ secara selektif sudah sejalan dengan prinsip kehati-hatian yang dianjurkan dalam kajian akademik.

Penegakan hukum cyberporn di Polda NTB telah mencerminkan pola investigasi modern yang memadukan kemampuan teknis, administratif, dan sosial. Kombinasi strategi hybrid, pemeriksaan bukti digital, dan komunikasi melalui SP2HP menunjukkan adanya prosedur yang terstruktur. Temuan ini sesuai dengan riset Tyler (2021) yang menyatakan bahwa kepercayaan masyarakat terhadap aparat meningkat ketika proses hukum dilakukan secara transparan dan teratur. Selain itu, penelitian Hartono (2023) menegaskan bahwa efektivitas penegakan hukum siber sangat bergantung pada kapasitas forensik digital, kesiapan korban, dan kolaborasi lintas lembaga. Dengan demikian, meskipun masih terdapat hambatan teknis dan non-teknis, proses penegakan hukum cyberporn di Polda NTB sudah berada pada jalur yang sesuai dengan standar literatur akademik.

3.Nilai-Nilai Pancasila dalam Pencegahan dan Penegakan Hukum Terhadap Kasus Cyberporn

Strategi pencegahan dan penegakan hukum terhadap kasus cyberporn pada dasarnya mencerminkan penguatan nilai-nilai Pancasila sebagai dasar etika, moral, dan hukum nasional. Dari aspek pencegahan online yang meliputi penyebaran flyer digital, patroli siber, takedown konten melalui kerja sama dengan Kominfo, serta imbauan etik digital nilai Pancasila terutama terlihat pada upaya menjaga martabat manusia dan perlindungan terhadap masyarakat. Nilai Sila Kedua, Kemanusiaan yang Adil dan Beradab tercermin melalui perlindungan dari eksploitasi seksual digital, mengingat korban cyberporn umumnya rentan secara psikologis dan sosial. Hal ini sejalan dengan temuan Lestari (2021) yang menegaskan bahwa perlindungan digital merupakan bagian dari penguatan hak asasi dalam ruang siber. Strategi seperti patroli siber dan takedown konten menunjukkan komitmen negara melindungi warganya dari kerentanan moral dan psikologis, sehingga mencerminkan keadaban digital berbasis kemanusiaan.

Selanjutnya, nilai Sila Ketiga, Persatuan Indonesia tercermin dalam mekanisme kerja sama antarinstansi, seperti kolaborasi antara aparat penegak hukum, Kominfo, dan masyarakat. Strategi ini memperlihatkan pendekatan kolektif yang menempatkan keamanan digital sebagai tanggung jawab bersama. Hal tersebut sejalan dengan penelitian Hidayat & Wibisono (2022) yang menyatakan bahwa kolaborasi multistakeholder menjadi faktor kunci dalam penanganan kejahatan siber di Indonesia. Penyebaran flyer digital dan imbauan etika bermedia juga menjadi sarana membangun kesadaran kolektif untuk menciptakan ruang digital yang aman bagi semua, sehingga memperkuat rasa kebangsaan dalam menjaga moral masyarakat.

Pada strategi pencegahan offline, seperti sosialisasi di sekolah, pembinaan oleh tokoh masyarakat, serta kerja sama RT, Babinsa, dan lingkungan setempat, nilai Sila Keempat, Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan tampak dalam proses musyawarah dan dialog dalam komunitas. Aparat melibatkan perangkat desa, tokoh agama, dan keluarga dalam proses identifikasi maupun pencegahan perilaku berisiko. Ini sesuai dengan temuan Raharjo

(2023) yang menekankan pentingnya peran komunitas dalam deteksi awal kejahatan siber. Pendekatan ini bukan hanya mengedepankan koordinasi, tetapi juga menempatkan masyarakat sebagai mitra strategis dalam pengawasan moral dan sosial.

Sedangkan dalam aspek penegakan hukum seperti prosedur penyelidikan, penyidikan, penetapan tersangka, hingga pelimpahan ke kejaksaan nilai Sila Kelima, Keadilan Sosial bagi Seluruh Rakyat Indonesia terwujud melalui implementasi penegakan hukum yang proporsional dan memastikan setiap korban memperoleh keadilan. Proses hukum yang dilakukan secara administrasi terbuka, pemberian SP2HP kepada pelapor, serta mekanisme P19–P21 dalam kelengkapan berkas merupakan bentuk keadilan prosedural. Temuan Pratama & Nugroho (2022) menunjukkan bahwa integritas prosedural menjadi indikator utama dalam penegakan hukum siber yang berkeadilan. Selain itu, keberadaan opsi restorative justice juga mencerminkan pendekatan keadilan yang humanis dan berorientasi pemulihan, bukan sekadar penghukuman.

Nilai Sila Pertama,Ketuhanan Yang Maha Esa juga tercermin secara substantif, terutama melalui upaya menjaga moralitas dan mencegah perilaku yang bertentangan dengan norma agama. Cyberporn dianggap sebagai tindakan yang merusak akhlak dan kehormatan manusia, sehingga strategi pencegahan maupun penindakan tidak hanya berfungsi sebagai kontrol sosial, tetapi juga sarana menjaga nilai ketuhanan dalam kehidupan digital. Hal ini sesuai dengan pandangan Yusuf (2020) yang menyebutkan bahwa kejahatan seksual digital tidak hanya melanggar hukum positif, tetapi juga norma keagamaan yang menjadi dasar moral masyarakat Indonesia.

Secara keseluruhan, strategi pencegahan dan penegakan hukum cyberporn yang dilakukan secara online, offline, dan melalui proses hukum formal menunjukkan bahwa nilai-nilai Pancasila tetap menjadi kerangka etis dalam penanganan kejahatan siber. Setiap sila berperan dalam mengarahkan kebijakan dan tindakan aparat agar tidak hanya berfokus pada aspek penindakan, tetapi juga menciptakan keadaban digital, perlindungan kemanusiaan, kerja sama kolektif, musyawarah komunitas, serta keadilan sosial yang berkelanjutan. Dengan demikian, penerapan nilai Pancasila bukan hanya menjadi dasar normatif, tetapi juga menjadi fondasi operasional dalam menciptakan ruang digital yang aman dan bermartabat bagi seluruh masyarakat.

KESIMPULAN

Berdasarkan hasil penelitian mengenai strategi pencegahan dan penegakan hukum Polda NTB terhadap kasus cyberporn di era digital, dapat disimpulkan bahwa kejahatan cyberporn di NTB memiliki tingkat kompleksitas tinggi karena melibatkan faktor teknologi, psikologis, dan sosial. Kasus paling banyak terjadi pada kelompok usia remaja 15–18 tahun dan mahasiswa, dengan modus yang beragam seperti penyebaran konten intim, pemerasan, penggunaan akun anonim, hingga manipulasi digital (deepfake). Situasi ini diperburuk oleh rendahnya literasi digital dan lemahnya pengawasan lingkungan. Pencegahan dilakukan melalui pendekatan online dan offline yang saling melengkapi. Secara online, Polda NTB memanfaatkan media sosial, flyer digital, patroli siber, dan takedown konten bekerja sama dengan Kominfo. Secara offline, pencegahan dilakukan melalui sosialisasi ke sekolah dan kampus, kemitraan dengan tokoh masyarakat, serta pembinaan hukum langsung kepada masyarakat. Strategi ini menunjukkan bahwa pencegahan berlapis lebih efektif untuk menjangkau kelompok rentan serta meningkatkan kesadaran hukum masyarakat.

Penegakan hukum dilakukan melalui tahap penyelidikan, penyidikan, hingga pelimpahan ke Kejaksaan, dengan memadukan teknik identifikasi online dan offline. Meskipun menghadapi hambatan seperti akun anonim, bukti digital yang cepat hilang, dan kondisi psikologis korban, Polda NTB tetap mampu melakukan penindakan melalui pendekatan teknis dan sosial.

Seluruh upaya pencegahan dan penegakan hukum yang dilakukan Polda NTB berlandaskan nilai-nilai Pancasila, terutama pada aspek kemanusiaan, keadilan, perlindungan korban, kerja sama lintas lembaga, serta pembentukan etika digital yang beradab. Dengan demikian, strategi yang diterapkan tidak hanya berorientasi pada penindakan, tetapi juga pada pembangunan ekosistem digital yang aman, bermoral, dan berkeadilan bagi masyarakat NTB.

DAFTAR PUSTAKA

Alghamdi, A. (2022). Human factor in cybersecurity: Risk, behavior, and vulnerability analysis. Journal of Cybersecurity Studies, 7(2), 55–72.

Aribowo, R. (2021). Community intelligence dalam penanganan kejahatan siber di daerah. Jurnal Keamanan Digital, 4(1), 12–25.

Azizah, N., & Marpaung, D. (2024). Cyberporn dan implikasi hukum dalam ruang digital. Jurnal Hukum Siber Indonesia, 6(1), 33–47.

Becker, G. (1968). Crime and punishment: An economic approach. Journal of Political Economy, 76(2), 169–217.

Braithwaite, J. (2023). Restorative justice and social reintegration. Oxford University Press.

Clarke, R. (1997). Situational crime prevention: Successful case studies. Harrow and Heston.

Education. (2024). Pedoman dokumentasi penelitian kualitatif. Education Press.

Hakim, A., & Sutanto, R. (2022). Forensik digital dalam penyelidikan kejahatan seksual berbasis online. Jurnal Teknologi & Forensik, 5(1), 40–52.

Helmiawan, F., et al. (2025). Kesadaran keamanan digital pada remaja di Indonesia. Jurnal Literasi Digital Nusantara, 3(2), 77–96.

Hidayat, A., & Wibisono, R. (2022). Kolaborasi multistakeholder dalam penanganan cybercrime di Indonesia. Jurnal Sistem Informasi Nasional, 8(1), 21–36.

Kementerian Komunikasi dan Informatika. (2024). Laporan pemblokiran situs internet 2024. Kominfo.

Kurniawan, H., & Lestari, N. (2022). Chain of custody dalam penyidikan kasus cyberporn. Jurnal Hukum Teknologi, 2(3), 100–114.

Lestari, N. (2021). Perlindungan hak digital sebagai bagian dari hak asasi manusia. Jurnal HAM Digital, 5(1), 55–70.

Lestari, S. (2023). Implementasi UU ITE dalam penanggulangan kejahatan siber. Jurnal Hukum Teknologi Indonesia, 4(1), 44–58.

Livingstone, S., et al. (2022). Digital literacy and online risk: Age-appropriate education strategies. European Journal of Digital Culture, 10(3), 201–220.

Marzuki, A., & Fadilah, R. (2021). Pendekatan hybrid offline-online dalam investigasi akun anonim. Jurnal Forensik Siber, 4(2), 88–102.

Mazerolle, L., & Ransley, J. (2023). Community-based policing: Theory and practice. Routledge.

Nuraini, S., & Putra, A. (2022). Dampak psikologis cyberporn terhadap remaja. Jurnal Psikologi Remaja Digital, 4(1), 29–40.

Nurdin, F., & Septian, W. (2020). Kerentanan bukti digital dalam kasus kejahatan seksual online. Jurnal Ilmu Digital Forensik, 2(2), 15–26.

Pratama, B., & Nugroho, S. (2022). Keadilan prosedural dalam penegakan hukum siber. Jurnal Etika Hukum, 3(2), 60–72.

Putra, D. (2022). Model investigasi siber berbasis kolaborasi sosial dan digital. Jurnal Investigasi Nusantara, 5(1), 71–84.

Rachman, I., & Hidayat, T. (2021). Enkripsi dan tantangan penyidikan cybercrime. Jurnal Teknologi Siber, 3(2), 55–65.

Raharjo, W. (2023). Peran komunitas dalam deteksi awal kejahatan siber. Jurnal Kriminologi Digital, 6(1), 22–35.

Rahman, A., & Yuliani, S. (2023). Analisis hukum terhadap kasus cyberporn di Indonesia. Jurnal Hukum Siber Nasional, 7(1), 13–29.

Ramadhan, Y. (2023). Evaluasi penerapan restorative justice dalam kasus kejahatan seksual

digital. Jurnal Peradilan Indonesia, 11(2), 88–102.
Rofiah. (2022). Model analisis interaktif dalam penelitian kualitatif. Jurnal Metode Penelitian, 4(1), 15–27.
Rofiah, A., & Bungin, B. (2024). Metodologi penelitian kualitatif dalam studi kejahatan siber. Jurnal Penelitian Sosial Digital, 5(1), 40–55.
Sa'diyah, M. (2023). Cyberporn pada remaja dan implikasi hukumnya. Jurnal Studi Kriminologi, 9(1), 19–33.
Saridewi, M., & Sari, R. (2024). Peran Kominfo dalam penghapusan konten ilegal digital. Jurnal Kebijakan Siber, 4(1), 33–47.
Sari, L., & Maulida, C. (2022). Trauma korban cyberporn dan hambatan dalam proses hukum. Jurnal Psikologi Klinis Digital, 3(2), 70–85.
Sasmita, R. (2023). Due process of law dalam penyidikan kasus cybercrime. Jurnal Hukum Pidana Siber, 6(2), 55–66.
Skogan, W. (2022). Community policing and crime prevention. Oxford University Press.
Suharto, P. (2023). Karakter lintas wilayah kejahatan siber di Indonesia. Jurnal Keamanan Siber Nasional, 2(2), 11–24.
Tsauri, G. (2025). Kerentanan manusia terhadap rekayasa sosial di era digital. Jurnal Human-Cyber Interaction, 5(1), 41–58.
Tyler, T. (2021). Procedural justice and public trust in law enforcement. Yale Law Review, 131(3), 415–440.
Usman, H., & Agustanti, D. (2023). Kapasitas kelembagaan daerah dalam penanganan kejahatan siber. Jurnal Administrasi Publik Digital, 2(2), 99–113.
We Are Social. (2024). Digital Report Indonesia 2024. We Are Social.
Wijaya, H., & Yusuf, A. (2021). Dinamika penanganan cybercrime berbasis laporan korban. Jurnal Kebijakan Kriminal, 5(1), 25–40.
Wijayanto, F., & Sari, A. (2021). Volatilitas bukti digital dalam penyidikan kasus cybercrime. Jurnal Forensik Digital Indonesia, 3(1), 50–63.
Yuliani, R., & Said, M. (2022). Penerapan restorative justice pada kasus kekerasan seksual digital. Jurnal Hukum dan Sosial, 4(2), 18–30.
Yunita, N., & Pramono, S. (2023). Implementasi UU ITE pada kasus cyberporn. Jurnal Legislasi Teknologi, 8(1), 44–58.
Yusuf, M. (2020). Perspektif agama terhadap kejahatan seksual digital. Jurnal Moral & Agama, 7(2), 33–48.