

Optimalisasi Pencegahan Dampak Kejahatan Digital dan Informatika Melalui Sinergi Pemerintah Daerah Dengan Kepolisian Resort Wilayah Kabupaten Labuhan Batu Selatan

Nur Ageng Sena, Hanuring Ayu Ardhani Putri², Muhammad Aziz Zaelani³

¹²³ Universitas Islam Batik Surakarta, Indonesia



agengsenase@gmail.com

Abstrak

Perkembangan teknologi digital dan informatika telah meningkatkan berbagai bentuk kejahatan digital yang berdampak pada aspek ekonomi, sosial, dan keamanan masyarakat. Kondisi tersebut menuntut adanya upaya pencegahan yang tidak hanya bersifat represif, tetapi juga preventif melalui kerja sama lintas lembaga. Penelitian ini bertujuan untuk menganalisis optimalisasi pencegahan dampak kejahatan digital dan informatika melalui sinergi antara pemerintah daerah dan Kepolisian Resor Kabupaten Labuhan Batu Selatan ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta mengidentifikasi hambatan yang dihadapi dalam pelaksanaannya. Metode penelitian yang digunakan adalah penelitian hukum empiris dengan pendekatan yuridis sosiologis. Data diperoleh melalui wawancara dengan pemerintah daerah dan kepolisian, serta didukung oleh studi kepustakaan. Analisis data dilakukan secara kualitatif. Hasil penelitian menunjukkan bahwa sinergi telah dilakukan melalui sosialisasi literasi digital, layanan pengaduan masyarakat, dan koordinasi penanganan kasus kejahatan digital. Namun, optimalisasi pencegahan masih menghadapi hambatan berupa keterbatasan sumber daya manusia, rendahnya literasi digital masyarakat, keterbatasan sarana teknologi, serta belum optimalnya koordinasi lintas sektor. Oleh karena itu, diperlukan penguatan sinergi yang berkelanjutan guna meningkatkan efektivitas pencegahan kejahatan digital di tingkat daerah.

Keywords: *Kejahatan Digital, Sinergi Pemerintah Daerah, UU ITE*

Published by

Fakultas Syariah Sekolah Tinggi Agama Islam (STAI) Al-Furqan Makassar

Website

<https://ojs.staialfurqan.ac.id/jtm/>

This is an open access article under the CC BY SA license

<https://creativecommons.org/licenses/by-sa/4.0/>



PENDAHULUAN

Perkembangan teknologi digital dalam beberapa tahun terakhir telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat. Digitalisasi yang semakin meluas membuat aktivitas komunikasi, transaksi ekonomi, hingga pelayanan publik beralih ke sistem berbasis teknologi informasi. Peningkatan penggunaan internet, telepon pintar, serta aplikasi daring telah menjadikan masyarakat semakin bergantung pada layanan digital dalam memenuhi kebutuhan sehari-hari. Namun, kemajuan ini tidak hanya memberikan manfaat positif, tetapi juga menghadirkan konsekuensi serius berupa meningkatnya ragam dan intensitas kejahatan digital. Sabrina dalam penelitiannya mengenai krisis keamanan data publik menegaskan bahwa perkembangan teknologi mendorong peningkatan ancaman digital yang tidak hanya merugikan individu, tetapi juga mengancam keamanan data, stabilitas sosial, dan kepercayaan masyarakat terhadap teknologi¹. Menurut buku *Cybercrime and Society* (edi. ke-4) yang mengidentifikasi bahwa kejahatan digital (*cybercrime*) kini berkembang menjadi berbagai bentuk seperti penipuan daring, pencurian identitas, peretasan akun media sosial, penyalahgunaan data pribadi, dan penyebaran informasi palsu².

Fenomena meningkatnya kejahatan digital tersebut didukung oleh karakter ruang siber yang tidak mengenal batas wilayah sehingga memungkinkan pelaku bertindak kapan saja dan di mana saja. Regulasi nasional sebenarnya telah berupaya memberikan payung hukum melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data

¹ Sabrina, Cindy, 'Krisis Keamanan Data Publik Dan Urgensi Kedaulatan Data Di Era Governansi Digital', *Jurnal Transformasi Administrasi*, 1 (2024), 3–6

² Majid Yar and Kevin F. Steinmetz, *Cybercrime and Society (4th Ed.)* (AGE Publications, 2023).

Pribadi (UU PDP), yang secara tegas mengatur larangan akses ilegal, manipulasi data elektronik, penipuan daring, intersepsi, maupun penyebaran konten menyesatkan. Meskipun demikian, masyarakat masih berada pada posisi rentan karena keterbatasan literasi digital dan minimnya pemahaman terhadap ancaman keamanan siber. Dampaknya tidak hanya bersifat ekonomi, tetapi juga meliputi aspek psikologis dan sosial, seperti hilangnya rasa aman, menurunnya kepercayaan terhadap layanan digital, hingga kerusakan reputasi pribadi maupun lembaga.

Di tingkat lokal, Kabupaten Labuhan Batu Selatan merupakan daerah yang sedang mengalami peningkatan pesat dalam pemanfaatan teknologi dan digitalisasi layanan publik. Akses internet yang semakin luas, tingginya penggunaan media sosial, serta meningkatnya aktivitas ekonomi digital menyebabkan masyarakat di wilayah ini semakin aktif dalam ruang siber. Namun, perkembangan tersebut juga diiringi kenaikan kasus kejahatan digital, seperti penipuan berbasis akun media sosial, investasi online ilegal, dan penyebaran konten meresahkan. Kondisi ini menunjukkan bahwa kebutuhan akan sistem pencegahan dan penanganan kejahatan digital di Kabupaten Labuhan Batu Selatan menjadi semakin mendesak. Pemerintah daerah telah melakukan berbagai upaya seperti penyuluhan keamanan informasi, penguatan regulasi lokal, dan penyediaan layanan pengaduan masyarakat. Namun, keterbatasan sumber daya manusia yang memiliki kompetensi keamanan digital, rendahnya literasi digital masyarakat, serta minimnya fasilitas pemantauan aktivitas siber masih menjadi kendala utama.

Dalam konteks penegakan hukum, Kepolisian Resort Labuhan Batu Selatan juga menghadapi tantangan dalam menangani kejahatan digital. Penanganan kasus siber memerlukan kemampuan teknis, perangkat analisis digital, serta koordinasi lintas lembaga. Mery Rohana menegaskan bahwa pembuktian digital memerlukan keahlian khusus serta kerja sama dengan pihak teknis dan penyedia layanan internet agar proses hukum berjalan efektif.³ Oleh karena itu, sinergi antara pemerintah daerah dan kepolisian menjadi kunci penting dalam membangun mekanisme pencegahan *cybercrime* yang lebih kuat dan terintegrasi. Krisna juga menunjukkan bahwa pemerintah daerah memiliki posisi strategis dalam edukasi, penyusunan kebijakan lokal, dan pemberdayaan masyarakat, tetapi peran tersebut tidak dapat berjalan efektif tanpa dukungan institusi penegak hukum.⁴

Meskipun terdapat penelitian terdahulu terkait peran pemerintah daerah, kejahatan digital maupun aspek pembuktian digital oleh kepolisian, belum ada penelitian yang secara spesifik mengkaji sinergi antara pemerintah daerah dan kepolisian dalam konteks pencegahan kejahatan digital di tingkat daerah, khususnya di Kabupaten Labuhan Batu Selatan. Penelitian yang ada sebelumnya cenderung berdiri pada fokus sectoral pmda saja atau kepolisian saja belum menyentuh bagaimana kedua lembaga berkolaborasi, hambatan yang dihadapi, dan sejauh mana tindakan bersama dapat meningkatkan efektivitas pencegahan *cybercrime*. Oleh karena itu, penelitian ini bertujuan untuk menganalisis optimalisasi pencegahan dampak kejahatan digital dan informatika melalui sinergi pemerintah daerah dengan Kepolisian Resor Kabupaten Labuhan Batu Selatan ditinjau dari UU ITE, serta mengidentifikasi hambatan yang mempengaruhi efektivitas kerja sama kedua institusi tersebut.

METODE

Penelitian ini merupakan penelitian empiris yang bertujuan menganalisis implementasi ketentuan hukum terkait pencegahan kejahatan digital melalui sinergi antara pemerintah daerah dan Kepolisian Resor Kabupaten Labuhan Batu Selatan. Lokasi penelitian ditetapkan secara purposif dengan pertimbangan meningkatnya kasus kejahatan digital dan pentingnya koordinasi antarinstansi di wilayah tersebut. Data penelitian terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara semi-terstruktur dengan pejabat Dinas Komunikasi dan Informatika, aparat kepolisian, serta pelaku usaha daring, dan dilengkapi dengan observasi non-partisipatif terhadap aktivitas instansi terkait. Data sekunder diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, khususnya Undang-Undang Informasi dan Transaksi Elektronik, serta literatur ilmiah dan dokumen pendukung yang relevan. Analisis data dilakukan

³ Mery Rohana and others, 'Penerapan Konsep Pembuktian Digital Dalam Kasus Kejahatan Teknologi Informasi Application of the Concept of Digital Evidence in Information Technology Crime Cases', *Jurnal Kolaboratif Sains*, 8.1 (2025), 390–95 <<https://doi.org/10.56338/jks.v8i1.6742>>.

⁴ Dicka Krisna and others, 'Kejahatan Cyber : Tinjauan Psikobehavioristik', *Jurnal Pengabdian Masyarakat (JPM) SENSASI*, 2.02 (2023), 256–65.

secara kualitatif menggunakan model Sigisol melalui tahapan pengumpulan, seleksi, interpretasi, dan penarikan kesimpulan dengan mengaitkan temuan lapangan pada teori dan ketentuan hukum yang berlaku. Pendekatan ini digunakan untuk memperoleh gambaran komprehensif mengenai pencegahan kejahatan digital di tingkat daerah serta memperkuat rekomendasi kebijakan.

HASIL DAN PEMBAHASAN

1. Gambaran Umum Pencegahan Kejahatan Digital di Kabupaten Labuhan Batu Selatan

Perkembangan teknologi informasi dan komunikasi di Indonesia, termasuk di Kabupaten Labuhan Batu Selatan, menunjukkan peningkatan yang signifikan seiring dengan meluasnya penggunaan internet, media sosial, serta layanan berbasis digital dalam kehidupan sehari-hari. Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), penetrasi internet di Indonesia terus meningkat dan mendorong perubahan pola interaksi sosial, ekonomi, serta pelayanan publik masyarakat⁵. Kondisi ini juga berdampak pada meningkatnya potensi kejahatan digital (*cyber crime*), seperti penipuan daring, penyalahgunaan identitas dan akun media sosial, investasi online ilegal, peretasan sistem elektronik, serta penyebaran berita bohong (*hoaks*) yang merugikan masyarakat.

Kejahatan digital didefinisikan sebagai setiap perbuatan melawan hukum yang memanfaatkan teknologi informasi dan sistem elektronik sebagai sarana utama maupun sasaran tindak pidana⁶. Widodo menegaskan bahwa karakteristik kejahatan digital bersifat lintas batas, sulit dideteksi, serta memiliki dampak luas terhadap keamanan individu dan stabilitas sosial⁷. Hal ini sejalan dengan pendapat Prasetyo yang menyatakan bahwa meningkatnya literasi digital masyarakat tidak selalu diiringi dengan pemahaman etika dan keamanan siber, sehingga membuka ruang terjadinya penyalahgunaan teknologi⁸.

Berdasarkan hasil wawancara dengan aparat pemerintah daerah dan Kepolisian Resor Kabupaten Labuhan Batu Selatan, kejahatan digital merupakan salah satu jenis tindak pidana yang paling sering dilaporkan dalam beberapa tahun terakhir. Laporan tersebut didominasi oleh kasus penipuan online melalui media sosial dan aplikasi pesan singkat, investasi bodong berbasis digital, serta penyalahgunaan data pribadi. Fenomena ini menunjukkan bahwa perkembangan teknologi digital di daerah tidak hanya membawa manfaat, tetapi juga risiko yang memerlukan upaya pencegahan dan penanganan yang sistematis. Secara normatif, upaya pencegahan kejahatan digital di Indonesia telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Undang-undang ini mengatur mengenai perbuatan yang dilarang di ruang siber, perlindungan data dan sistem elektronik, serta sanksi pidana bagi pelaku kejahatan digital. Pasal 27 sampai dengan Pasal 37 UU ITE secara khusus mengatur berbagai bentuk tindak pidana siber, mulai dari pencemaran nama baik, penyebaran konten ilegal, hingga akses ilegal terhadap sistem elektronik.

Namun demikian, sejumlah kajian menyebutkan bahwa efektivitas UU ITE dalam mencegah kejahatan digital sangat bergantung pada kapasitas aparat penegak hukum dan peran aktif pemerintah daerah. Waluyadi menyatakan bahwa pencegahan kejahatan siber tidak cukup hanya melalui pendekatan represif, tetapi harus didukung oleh upaya preventif berupa edukasi literasi digital, sosialisasi hukum, serta penguatan koordinasi antarinstansi⁹. Dalam konteks daerah, pemerintah daerah memiliki peran strategis dalam meningkatkan kesadaran masyarakat melalui program edukasi digital, sementara kepolisian berperan sebagai garda terdepan dalam penegakan hukum dan penanganan laporan kejahatan digital. Dengan demikian, pencegahan kejahatan digital di Kabupaten Labuhan Batu Selatan tidak hanya bergantung pada keberadaan regulasi seperti UU ITE, tetapi juga pada sinergi antara pemerintah daerah, kepolisian, dan masyarakat. Pendekatan yang terintegrasi antara aspek hukum, edukasi, dan penguatan kapasitas institusi menjadi kunci dalam menciptakan ruang digital yang aman, tertib, dan berkeadilan bagi masyarakat.

⁵ APJII, 'Survei Penetrasi Internet 2022–2023', *ANTARA Kantor Berita Indonesia*, 2023.

⁶ Widodo, *Aspek Hukum Pidana Kejahatan Mayantara* (Yogyakarta: Aswaja Pressindo, 2013).

⁷ Widodo.

⁸ Dimas Abimanyu Prasetyo and others, 'Pentingnya Etika Siber Pada Era Digital', *Nusantara Journal of Multidisciplinary Science*, 2.5 (2024), 1130–37.

⁹ Waluyadi Waluyadi, 'Law Enforcement Against Cyber Crimes in Indonesia : Analysis of the Role of the ITE Law in Handling Cyber Crimes', *Indonesian Cyber Law Review*, 1.2 (2024), 32–39.

2. Optimalisasi Pencegahan Dampak Kejahatan Digital Melalui Sinergi Pemerintah Daerah dan Kepolisian Ditinjau dari UU ITE

a. Bentuk Sinergi Pemerintah Daerah dan Kepolisian

Hasil penelitian menunjukkan bahwa sinergi antara pemerintah daerah dan Kepolisian Resor Kabupaten Labuhan Batu Selatan diwujudkan melalui koordinasi aktif dalam pertukaran informasi, pelaksanaan sosialisasi serta penanganan laporan masyarakat terkait kejahatan digital dan tindak pidana lainnya yang berkembang di era digital. Sinergi ini dibangun sebagai respons atas meningkatnya penggunaan teknologi informasi dalam kehidupan masyarakat yang diiringi dengan eskalasi kejahatan berbasis digital, seperti penipuan daring, penyalahgunaan data pribadi, peretasan akun, dan penyebaran konten bermuatan melanggar hukum. Kolaborasi ini menempatkan pemerintah daerah sebagai aktor utama dalam upaya preventif, sementara kepolisian berperan dominan dalam penegakan hukum dan penindakan terhadap pelaku kejahatan digital.

Dalam aspek sosialisasi literasi digital, pemerintah daerah bersama kepolisian secara aktif menyelenggarakan kegiatan edukasi kepada masyarakat mengenai pentingnya keamanan digital. Sosialisasi ini dilakukan melalui seminar, penyuluhan hukum, dan kampanye digital yang menyasar berbagai kelompok masyarakat, seperti pelajar, aparatur sipil negara, pelaku UMKM, dan masyarakat umum. Materi yang disampaikan meliputi cara mengenali modus penipuan daring, pentingnya menjaga kerahasiaan data pribadi, serta pemahaman dasar mengenai konsekuensi hukum atas penyalahgunaan teknologi informasi. Seperti yang telah dilakukan oleh pemerintah daerah bekerjasama dengan BBPSDMP Kominfo Medan dan kepolisian melaksanakan program *Digital Literacy* untuk meningkatkan pemahaman tentang penggunaan teknologi secara aman dan produktif, sekaligus meminimalisir risiko penipuan digital dan penyalahgunaan data pribadi¹⁰. Program ini termasuk pelatihan *Digital Talent Scholarship* yang terselenggara bekerja sama dengan BBPSDMP Kominfo Medan dan Pemkab Labuhan Batu Selatan, dengan tujuan memperkuat keterampilan digital warga dalam memanfaatkan teknologi secara bijak dan aman.

Bentuk lain sosialisasi literasi digital juga dilakukan melalui pemanfaatan media digital, seperti website resmi pemerintah daerah, akun media sosial Dinas Komunikasi dan Informatika, serta kanal informasi milik kepolisian. Melalui platform tersebut, masyarakat memperoleh informasi berupa infografis, video edukasi, dan imbauan terkait keamanan digital. Pendekatan ini dinilai efektif karena mampu menjangkau masyarakat secara lebih luas dan berkelanjutan, terutama generasi muda yang aktif menggunakan media sosial. Hasil penelitian menunjukkan bahwa sinergi juga diwujudkan melalui penyediaan layanan pengaduan masyarakat berbasis digital¹¹. Layanan ini dirancang untuk mempermudah masyarakat dalam melaporkan dugaan kejahatan digital tanpa harus datang langsung ke kantor pemerintah atau kepolisian. Contoh layanan digital yang digunakan antara lain aplikasi pengaduan masyarakat, layanan hotline pengaduan siber, serta kanal pelaporan daring melalui website resmi kepolisian. Layanan ini memungkinkan masyarakat menyampaikan laporan secara cepat, disertai bukti digital seperti tangkapan layar, rekaman percakapan, atau tautan yang relevan. Layanan pengaduan masyarakat tersebut berfungsi sebagai sarana deteksi dini terhadap potensi kejahatan digital. Setiap laporan yang masuk akan diverifikasi oleh petugas terkait sebelum diteruskan kepada unit yang berwenang. Pemerintah daerah, melalui perangkat teknisnya, berperan dalam membantu proses administrasi dan klasifikasi laporan, sementara kepolisian menindaklanjuti laporan tersebut melalui penyelidikan dan penyidikan sesuai dengan ketentuan hukum yang berlaku.

¹⁰ BPSDM Komdigi, 'BBPSDMP Kominfo Medan Dan Pemerintah Kabupaten Labuhan Batu Selatan Gelar Pelatihan Digital Talent Scholarship', *Badan Pengembangan Sumber Daya Manusia Komunikasi Dan Digital*, 2024 <<https://bpsdm.komdigi.go.id/upt/medan/berita-bbpsdmp-kominfo-medan-dan-pemerintah-kabupaten-labuhan-batu-selatan-gelar-p-5-148?utm=>>.

¹¹ 'Inovasi Dan Program Unggulan Di Polres Labuhan Batu Selatan', *Ditreskrim Polda Labuhan Batu Selatan*, 2025 <<https://ditreskrim.poldalabuhanbatuselatan.com/inovasi-dan-program-unggulan-di-polres-labuhan-batu-selatan/>>.

Dalam konteks koordinasi penanganan kasus kejahatan digital, sinergi antara pemerintah daerah dan kepolisian diwujudkan melalui mekanisme pertukaran data dan informasi. Koordinasi ini dilakukan melalui rapat lintas instansi, forum komunikasi keamanan daerah, serta pemanfaatan sistem informasi bersama untuk memantau perkembangan kasus. Melalui koordinasi tersebut, setiap pihak memiliki pemahaman yang sama mengenai pola kejahatan digital yang terjadi di wilayahnya serta langkah penanganan yang perlu dilakukan. Pemerintah daerah membantu proses pendataan korban dan penyediaan informasi awal, sedangkan kepolisian melakukan penelusuran jejak digital pelaku, pengamanan barang bukti elektronik, serta koordinasi dengan unit siber di tingkat yang lebih tinggi apabila kasus tersebut melibatkan lintas wilayah atau jaringan yang lebih luas.

Sinergi ini juga mencakup pemanfaatan teknologi pendukung dalam proses penanganan kasus, seperti penggunaan sistem pelaporan elektronik, basis data kriminal berbasis digital, dan pemantauan aktivitas mencurigakan melalui analisis media sosial. Pemerintah daerah berperan dalam penyediaan infrastruktur pendukung, sedangkan kepolisian memanfaatkan teknologi tersebut sebagai alat bantu dalam penegakan hukum dan pengungkapan kasus kejahatan digital.

Sinergi ini sejalan dengan Pasal 30 ayat (1) UU ITE yang menyatakan bahwa: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain"* merupakan perbuatan yang dilarang¹². Ketentuan ini menjadi dasar bagi upaya preventif pemerintah daerah dalam meningkatkan kesadaran masyarakat agar tidak melakukan maupun menjadi korban akses ilegal terhadap sistem elektronik, serta dasar represif bagi kepolisian dalam menindak pelaku peretasan dan pengambilalihan akun. Selain itu, sinergi juga terlihat dalam upaya perlindungan privasi digital masyarakat. Hal ini relevan dengan Pasal 31 ayat (1) UU ITE yang menegaskan bahwa *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik"*¹³. Pemerintah daerah berperan dalam memberikan edukasi mengenai pentingnya menjaga kerahasiaan komunikasi digital, sedangkan kepolisian memiliki kewenangan untuk melakukan penindakan terhadap praktik penyadapan ilegal. Hal ini juga sejalan dengan temuan pada penelitian yang dilakukan oleh Setyadi mengenai pentingnya edukasi keamanan siber untuk meningkatkan pemahaman masyarakat tentang ancaman digital dan perlindungan data pribadi¹⁴.

Secara keseluruhan hasil penelitian menunjukkan bahwa sinergi melalui sosialisasi literasi digital, layanan pengaduan masyarakat, dan koordinasi penanganan kasus kejahatan digital merupakan strategi yang efektif dalam menghadapi tantangan kejahatan digital di tingkat daerah. Sinergi ini tidak hanya memperkuat aspek pencegahan dan penegakan hukum, tetapi juga membangun kesadaran kolektif masyarakat mengenai pentingnya keamanan digital, sehingga tercipta lingkungan digital yang lebih aman, tertib, dan berkeadilan.

b. Optimalisasi Pencegahan Berdasarkan Ketentuan UU ITE

Upaya pencegahan kejahatan digital yang dilakukan melalui sinergi antara pemerintah daerah dan kepolisian merujuk pada ketentuan normatif dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Hasil penelitian menunjukkan bahwa Pasal 32 ayat (1) UU ITE yang melarang setiap orang *"dengan sengaja dan tanpa hak atau melawan hukum mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau menyembunyikan Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain"*¹⁵. Ini menjadi dasar hukum utama dalam penguatan pencegahan terhadap tindak perusakan, manipulasi, dan penyalahgunaan informasi elektronik. Ketentuan ini

¹² Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

¹³ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

¹⁴ Hario Jati Setyadi and others, 'Edukasi Keamanan Cyber Kepada Masyarakat Dari Ancaman Digital', *PETISI: Pengabdian Kepada Masyarakat Bidang Teknologi Informasi Dan Sistem Informasi*, 2.2 (2024), 40–47.

¹⁵ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

menjadi landasan bagi pemerintah daerah dalam memperkuat sistem keamanan data dan pengelolaan informasi publik, sekaligus menjadi acuan bagi kepolisian dalam meningkatkan kapasitas pembuktian digital dalam penanganan kasus kejahatan berbasis teknologi informasi.

Dalam konteks kejahatan ekonomi digital, sinergi antarinstansi juga diarahkan pada pencegahan penipuan daring yang diatur dalam Pasal 28 ayat (1) UU ITE, yang melarang setiap orang *Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik*¹⁶. Hasil penelitian menunjukkan bahwa pemerintah daerah berperan aktif dalam memberikan edukasi kepada masyarakat terkait perlindungan konsumen digital, termasuk peningkatan kewaspadaan terhadap modus penipuan daring dan investasi ilegal. Sementara itu, kepolisian menjalankan fungsi penegakan hukum melalui penindakan terhadap pelaku penipuan online dan investasi bodong, serta melakukan koordinasi dengan unit terkait dalam proses penyelidikan dan pembuktian.

Selain kejahatan ekonomi digital, pencegahan konflik sosial di ruang digital juga menjadi fokus sinergi antara pemerintah daerah dan kepolisian dengan mengacu pada Pasal 28 ayat (2) UU ITE, yang melarang penyebaran informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan berdasarkan suku, agama, ras, dan antargolongan (SARA)¹⁷. Dalam hal ini, pemerintah daerah berperan dalam menanamkan nilai toleransi, moderasi, dan etika bermedia melalui program literasi digital, sedangkan kepolisian bertugas menegakkan hukum secara proporsional dan profesional terhadap pelanggaran yang berpotensi mengganggu ketertiban umum dan keharmonisan sosial. Hasil penelitian juga menunjukkan bahwa koordinasi penanganan kejahatan digital tidak hanya bersifat reaktif, tetapi berkembang ke arah preventif dan antisipatif. Pemerintah daerah dan kepolisian secara bersama-sama melakukan pemetaan wilayah serta identifikasi kelompok masyarakat yang rentan terhadap kejahatan digital. Langkah ini memungkinkan dilakukannya peningkatan sosialisasi, pengawasan, dan edukasi yang lebih terarah sebagai upaya pencegahan sejak dini terhadap potensi kejahatan digital.

Sinergi yang terbangun melalui optimalisasi pencegahan berbasis UU ITE tersebut turut mendorong peningkatan kepercayaan masyarakat terhadap pemerintah daerah dan aparat penegak hukum. Keberadaan layanan pengaduan digital yang mudah diakses dan responsif memberikan rasa aman bagi masyarakat serta mendorong partisipasi aktif dalam melaporkan dugaan kejahatan digital. Partisipasi masyarakat ini menjadi elemen penting dalam menciptakan ekosistem digital yang aman, tertib, dan berkelanjutan sesuai dengan tujuan pembentukan UU ITE.

3. Hambatan Optimalisasi Pencegahan Kejahatan Digital Ditinjau dari UU ITE

a. Hambatan Internal

Hasil penelitian menunjukkan bahwa salah satu hambatan internal utama dalam optimalisasi pencegahan kejahatan digital di tingkat daerah adalah keterbatasan sumber daya manusia yang memiliki kompetensi khusus di bidang keamanan siber dan forensik digital. Penegakan ketentuan dalam Pasal 30, Pasal 31, dan Pasal 32 UU ITE yang berkaitan dengan akses ilegal, intersepsi tanpa hak, serta perusakan atau manipulasi informasi elektronik menuntut kemampuan teknis yang memadai, seperti identifikasi jejak digital, pengamanan barang bukti elektronik, serta analisis perangkat dan sistem informasi. Namun, pada praktiknya, jumlah aparatur pemerintah daerah maupun personel kepolisian yang memiliki keahlian khusus di bidang tersebut masih terbatas. Dampak dari keterbatasan ini adalah rendahnya kemampuan deteksi dini terhadap kejahatan digital, keterlambatan penanganan awal perkara, serta kurang optimalnya proses pembuktian elektronik yang berpotensi melemahkan efektivitas penegakan hukum UU ITE.

Selain keterbatasan sumber daya manusia, hambatan internal juga ditemukan pada aspek sarana dan prasarana pendukung. Hasil penelitian menunjukkan bahwa ketersediaan perangkat teknologi, perangkat lunak analisis forensik digital, serta sistem keamanan informasi yang memadai masih belum optimal di tingkat daerah. Kondisi ini menyebabkan upaya pencegahan, pemantauan, dan pengamanan sistem elektronik belum dapat dilakukan secara maksimal.

¹⁶ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

¹⁷ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Dampaknya, pemerintah daerah dan kepolisian mengalami keterbatasan dalam mengamankan data elektronik, mendeteksi serangan siber secara cepat, serta mengumpulkan alat bukti digital yang akurat dan dapat dipertanggungjawabkan secara hukum. Keterbatasan anggaran daerah untuk pengadaan dan pemeliharaan infrastruktur keamanan siber turut memperparah kondisi tersebut, sehingga pelaksanaan kebijakan pencegahan kejahatan digital belum sepenuhnya sejalan dengan pesatnya perkembangan teknologi informasi.

Hambatan internal lainnya berkaitan dengan koordinasi kelembagaan dan prosedur operasional. Meskipun sinergi antara pemerintah daerah dan kepolisian telah terbangun, hasil penelitian menunjukkan bahwa belum seluruh perangkat daerah memiliki standar operasional prosedur (SOP) yang terintegrasi dalam penanganan kejahatan digital. Dampak dari belum terintegrasinya SOP ini adalah kurang optimalnya pertukaran data dan informasi antarinstansi, potensi terjadinya tumpang tindih kewenangan, serta lambatnya pengambilan keputusan dalam penanganan awal kasus kejahatan digital, khususnya yang berkaitan dengan pengamanan sistem elektronik milik pemerintah daerah.

2. Hambatan Eksternal

Hambatan eksternal dalam optimalisasi pencegahan kejahatan digital terutama bersumber dari rendahnya tingkat literasi digital masyarakat. Hasil penelitian menunjukkan bahwa masih banyak masyarakat yang belum memiliki pemahaman memadai mengenai batasan perbuatan yang diperbolehkan dan yang dilarang di ruang digital sebagaimana diatur dalam UU ITE, khususnya terkait Pasal 28 ayat (1) mengenai penyebaran informasi bohong yang merugikan konsumen dan Pasal 28 ayat (2) mengenai penyebaran informasi yang bermuatan kebencian atau permusuhan berdasarkan suku, agama, ras, dan antargolongan (SARA). Dampak dari rendahnya literasi digital ini adalah meningkatnya kerentanan masyarakat menjadi korban kejahatan digital, sekaligus meningkatnya potensi pelanggaran hukum yang dilakukan tanpa disadari oleh pelaku.

Selain itu, hasil penelitian juga menemukan bahwa rendahnya kesadaran hukum masyarakat berdampak pada keterlambatan pelaporan kasus kejahatan digital. Banyak korban yang baru melaporkan peristiwa setelah mengalami kerugian yang signifikan, bahkan setelah bukti elektronik yang dimiliki telah terhapus atau tidak lagi dapat diakses. Dampak dari keterlambatan pelaporan ini adalah sulitnya aparat penegak hukum dalam mengumpulkan dan mengamankan alat bukti elektronik yang sah dan relevan, sehingga proses penyidikan menjadi tidak optimal dan peluang pengungkapan perkara menjadi semakin kecil.

Hambatan eksternal lainnya berkaitan dengan karakteristik kejahatan digital yang bersifat lintas wilayah dan lintas yurisdiksi. Hasil penelitian menunjukkan bahwa pelaku kejahatan digital seringkali beroperasi di luar wilayah hukum daerah, bahkan melibatkan jaringan lintas provinsi atau lintas negara. Dampak dari karakteristik ini adalah meningkatnya kompleksitas penegakan hukum UU ITE di tingkat daerah, khususnya dalam hal penelusuran pelaku, pengamanan server atau akun digital, serta koordinasi dengan aparat penegak hukum di wilayah lain. Kondisi tersebut menyebabkan proses penanganan perkara membutuhkan waktu dan sumber daya yang lebih besar, sehingga efektivitas pencegahan dan penindakan kejahatan digital menjadi terbatas.

KESIMPULAN

Hasil penelitian menunjukkan bahwa pencegahan kejahatan digital di Kabupaten Labuhan Batu Selatan telah diupayakan melalui sinergi antara pemerintah daerah dan Kepolisian Resor Labuhan Batu Selatan, yang diwujudkan dalam kegiatan literasi digital, layanan pengaduan masyarakat, serta koordinasi penanganan kasus kejahatan digital. Sinergi ini sejalan dengan ketentuan UU ITE, khususnya Pasal 30, Pasal 31, Pasal 32, dan Pasal 28, yang menekankan pentingnya perlindungan sistem elektronik, pencegahan penipuan daring, serta pengendalian konflik sosial di ruang digital. Namun demikian, optimalisasi pencegahan kejahatan digital masih menghadapi hambatan internal berupa keterbatasan sumber daya manusia, sarana prasarana, dan koordinasi kelembagaan, serta hambatan eksternal berupa rendahnya literasi digital masyarakat, keterlambatan pelaporan, dan karakteristik kejahatan digital yang bersifat lintas wilayah. Hambatan tersebut berdampak pada belum optimalnya deteksi dini dan efektivitas penegakan hukum. Oleh karena itu, diperlukan penguatan kapasitas aparatur, integrasi kebijakan lintas instansi, serta peningkatan literasi dan partisipasi masyarakat guna mewujudkan ekosistem digital yang aman dan berkelanjutan.

REFERENSI

BUKU :

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara* (Yogyakarta: Aswaja Pressindo, 2013)

Yar, Majid, and Kevin F. Steinmetz, *Cybercrime and Society (4th Ed.)* (AGE Publications, 2023)

JURNAL :

Krisna, Dicka, Kiki Septika Sari, Nurlia Anggraini, and Winda Royani, 'Kejahatan Cyber : Tinjauan Psikobehavioristik', *Jurnal Pengabdian Masyarakat (JPM) SENSASI*, 2 (2023), 256–65

Prasetyo, Dimas Abimanyu, Farhan Dwi Setiawan, Jeremiah Marvin Kapoyos, Mochamad Reyhan Gusnaldi, Wildan Hamzah Nur Fadholi, and Nurfiyah, 'Pentingnya Etika Siber Pada Era Digital', *Nusantara Journal of Multidisciplinary Science*, 2 (2024), 1130–37

Rohana, Mery, Lisbeth Sibarani, Bambang Supriadi, and Ozha Tiwa Hiawananta, 'Penerapan Konsep Pembuktian Digital Dalam Kasus Kejahatan Teknologi Informasi Application of the Concept of Digital Evidence in Information Technology Crime Cases', *Jurnal Kolaboratif Sains*, 8 (2025), 390–95 <<https://doi.org/10.56338/jks.v8i1.6742>>

Sabrina, Cindy, 'Krisis Keamanan Data Publik Dan Urgensi Kedaulatan Data Di Era Governansi Digital', *Jurnal Transformasi Administrasi*, 1 (2024), 3–6

Setyadi, Hario Jati, Amin Padmo, Azam Masa, Putut Pamilih Widagdo, Sandrina Aulia, Muhammad Hisyam Nugroho, and others, 'Edukasi Keamanan Cyber Kepada Masyarakat Dari Ancaman Digital', *PETISI: Pengabdian Kepada Masyarakat Bidang Teknologi Informasi Dan Sistem Informasi*, 2 (2024), 40–47

Waluyadi, Waluyadi, 'Law Enforcement Against Cyber Crimes in Indonesia : Analysis of the Role of the ITE Law in Handling Cyber Crimes', *Indonesian Cyber Law Review*, 1 (2024), 32–39

UNDANG-UNDANG :

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

WEB :

APJII, 'Survei Penetrasi Internet 2022–2023', *ANTARA Kantor Berita Indonesia*, 2023

BPSDM Komdigi, 'BBPSDMP Kominfo Medan Dan Pemerintah Kabupaten Labuhan Batu Selatan Gelar Pelatihan Digital Talent Scholarship', *Badan Pengembangan Sumber Daya Manusia Komunikasi Dan Digital*, 2024 <<https://bpsdm.komdigi.go.id/upt/medan/berita-bbpsdmp-kominfo-medan-dan-pemerintah-kabupaten-labuhan-batu-selatan-gelar-p-5-148?utm=>>

'Inovasi Dan Program Unggulan Di Polres Labuhan Batu Selatan', *Ditreskrimum Polda Labuhan Batu Selatan*, 2025 <<https://ditreskrimumpoldalabuhanbatuselatan.com/inovasi-dan-program-unggulan-di-polres-labuhan-batu-selatan/>>